OPTIMAL QUOTIENTS AND SURJECTIONS OF
MORDELL–WEIL GROUPS

EVERETT W. HOWE

Abstract. Answering a question of Ed Schaefer, we show that if $J$ is the
Jacobian of a curve $C$ over a number field, if $s$ is an automorphism of $J$
coming from an automorphism of $C$, and if $u$ lies in $\mathbb{Z}[s] \subseteq \text{End} J$ and has
connected kernel, then it is not necessarily the case that $u$ gives a surjective
map from the Mordell–Weil group of $J$ to the Mordell–Weil group of its image.

1. Introduction

Let $J$ be the Jacobian of a curve $C$ over a number field. If the automorphism
group $G$ of $J$ is nontrivial, one can use idempotents of the group algebra $\mathbb{Q}[G]$ to
decompose $J$ (up to isogeny) as a direct sum of abelian subvarieties. This
decomposition can be useful, for example, if one would like to compute the rational
points on $C$, because one of the subvarieties may satisfy the conditions necessary
for Chabauty’s method even when $J$ itself does not.

In this context, Ed Schaefer asked the following question in an online discussion:

Question 1. Let $C$ be a curve over a number field $k$, let $\sigma$ be a nontrivial auto-
morphism of $C$, let $s$ be the associated automorphism of the Jacobian $J$ of $C$, and
let $u$ be an element of $\mathbb{Z}[s] \subseteq \text{End} J$. Let $A \subseteq J$ be the image of $u$, and suppose
the kernel of $u$ is connected. Is it always true that map of Mordell–Weil groups
$J(k) \rightarrow A(k)$ induced by $u$ is surjective?

An optimal quotient of an abelian variety $A$ is a surjective morphism $A \rightarrow A'$ of
abelian varieties whose kernel is connected (see [1, §3]), so Schaefer’s question asks
whether an optimal quotient of a curve’s Jacobian “coming from” an automorphism
of the curve necessarily induces a surjection on Mordell–Weil groups.

The purpose of this paper is to show by explicit example that the answer to
Schaefer’s question is no. In Section 2 we show that if $\varphi : C \rightarrow E$ is a degree-2
map from a genus-2 curve to an elliptic curve, and if $\sigma$ is the involution of $C$ that
fixes $E$, then the endomorphism $1 + s$ of $J$ has connected kernel and its image is
isomorphic to $E$. In fact, the map $J \rightarrow E$ determined by $1 + s$ is isomorphic to
the push-forward $\varphi_* : J \rightarrow E$. To show that the answer to Question 1 is no, it
therefore suffices to find a double cover $\varphi : C \rightarrow E$ of an elliptic curve by a genus-2
curve such that $\varphi_*$ is not surjective on Mordell–Weil groups. We provide one such
example in Section 3, and show in Section 4 that there are in fact infinitely many
examples.
2. GENUS-2 DOUBLE COVERS OF ELLIPTIC CURVES

In this section we review some facts about genus-2 double covers of elliptic curves over an arbitrary field of characteristic not 2. In Section 3 we will return to the case where the base field is a number field.

The general theory of degree-$n$ maps from genus-2 curves to elliptic curves is explained by Frey and Kani [2]. Over the complex numbers, the complete two-parameter family of genus-2 double covers of elliptic curves was given in 1832 by Jacobi ([4, pp. 416–417], [5, pp. 380–382]) as a postscript to his review of Legendre’s *Traité des fonctions elliptiques* [6]; Legendre had himself given a one-parameter family of genus-2 double covers of elliptic curves (see Remark 3, below). In [3, §3.2], Jacobi’s construction is modified so that it works rationally over any base field of characteristic not 2, as follows:

Let $k$ be an arbitrary field of characteristic not 2 and let $K$ be a separable closure of $k$. Suppose we are given equations $y^2 = f$ and $y^2 = g$ for two elliptic curves $E$ and $F$ over $k$, where $f$ and $g$ are separable cubics in $k[x]$, and suppose further that we are given an isomorphism $\psi: E[2](K) \to F[2](K)$ of Galois modules such that $\psi$ is not the restriction to $E[2]$ of a geometric isomorphism $E_K \to F_K$. Then [3, Proposition 4, p. 324] gives an explicit equation for a genus-2 curve $C/k$ such that the Jacobian $J$ of $C$ is isomorphic to the quotient of $E \times F$ by the graph $\Gamma$ of $\psi$. (We say that $C$ is the curve obtained by gluing $E$ and $F$ together along their 2-torsion using $\psi$.) Let $\omega$ be the quotient map from $E \times F$ to $J$. The construction from [3] also shows that if $\lambda: J \to \hat{J}$ is the canonical principal polarization on $J$, then there is a diagram

\[
\begin{array}{ccc}
E \times F & \overset{(2:2)}{\longrightarrow} & E \times F \\
\omega \downarrow & & \omega \downarrow \\
J & \longrightarrow & J \\
& \lambda & \\
\end{array}
\]

The automorphism $(1, -1)$ of $E \times F$ fixes $\Gamma$ and respects the product polarization on $E \times F$, so it descends to give an automorphism $s$ of the polarized variety $(J, \lambda)$. By Torelli’s theorem [8, Theorem 12.1, p. 202], the automorphism $s$ comes from an automorphism $\sigma$ of $C$. Clearly $\sigma$ has order 2, and the quotient of $C$ by the order-2 group $\langle \sigma \rangle$ is isomorphic to $E$. Let $\varphi: C \to E$ be the associated double cover.

Let $u = 1 + s \in \text{End } J$. Then we have a diagram

\[
\begin{array}{ccc}
E \times F & \overset{(2,0)}{\longrightarrow} & E \times F \\
\omega \downarrow & & \omega \downarrow \\
J & \longrightarrow & J \\
& u & \\
\end{array}
\]

We claim that the kernel of $u$ is connected. To see this, note that the kernel of $\omega \circ (2, 0)$ is simply $E[2] \times F$. The image of $E[2] \times F$ in $J$ (under the map $\omega$) is equal to the image of $0 \times F$ in $J$ because every element of $E[2] \times 0$ is congruent modulo $\Gamma$ to an element of $0 \times F[2]$. Also, since $\Gamma$ intersects $0 \times F$ only in the identity, the image of $F$ in $J$ is isomorphic to $F$, so the kernel of $u$ is isomorphic to $F$.

On the other hand, we see from diagram (2) that the image of $u$ is equal to the image of $E \times 0$ in $J$. Since $\Gamma$ has trivial intersection with $E \times 0$, the image of $u$ is isomorphic to $E$. The induced map $J \to E$ is nothing other than $\varphi_*$. 
Likewise, the involution \(-s\) on \(J\) corresponds to an involution \(\sigma'\) of \(C\). The quotient of \(C\) by the group \((\sigma')\) is isomorphic to \(F\), and gives us a double cover \(\varphi' : C \to F\). If we set \(v = 1 - s\), then \(v\) has kernel isomorphic to \(E\) and image isomorphic to \(F\), and the map \(J \to F\) induced by \(v\) is \(\varphi'_*\).

**Remark 2.** Frey and Kani prove a more general result: Given two elliptic curves \(E\) and \(F\) over an algebraically closed field \(k\), an integer \(n > 1\), and an isomorphism \(\psi : E[n] \to F[n]\) of group schemes that is an anti-isometry with respect to the Weil pairings on \(E[n]\) and \(F[n]\), there is a possibly-singular curve \(C\) over \(k\) of arithmetic genus 2 whose polarized Jacobian \((J, \lambda)\) fits into a diagram analogous to (1), but with the 2's on the top arrow replaced with \(n\)'s. The curve \(C\) has degree-\(n\) maps to both \(E\) and \(F\), and arguments like the one given above show that the corresponding push-forward maps from \(J\) to \(E\) and from \(J\) to \(F\) are optimal.

**Remark 3.** Legendre’s family of genus-2 curves with split Jacobians [6, Troisième Supplément, §XII, pp. 333–359] is the family over \(C\) obtained from the construction above by taking \(F = E\) and by taking \(\psi : E[2](C) \to E[2](C)\) so that it fixes one point of order 2 and swaps the other two.

In Sections 3 and 4, we will use the construction that we have just described to produce genus-2 curves with involutions that we can use to show that the answer to Question 1 is no. As part of our analyses, we will need to know how to tell whether a point of \((E \times F)(k)\) lies in the image of \(J(k)\) under the map \((\varphi_*, \varphi'_*) : J \to E \times F\). Such a criterion is given in Proposition 12 (p. 338) of [3]. For the reader’s convenience, we review that criterion here. We continue to use the notation set earlier in the section: \(E\) and \(F\) are elliptic curves given by equations \(y^2 = f\) and \(y^2 = g\), respectively; \(\psi : E[2](K) \to F[2](K)\) is an isomorphism of Galois modules; and \(C\) is a genus-2 curve whose Jacobian \(J\) is isomorphic the quotient of \(E \times F\) by the graph of \(\psi\). The curve \(C\) comes provided with covering maps \(\varphi : C \to E\) and \(\varphi' : C \to F\) of degree 2, and the quotient map \(E \times F \to J\) followed by \((\varphi_*, \varphi'_*)\) is multiplication-by-2 on \(E \times F\).

Let \(L\) be the 3-dimensional \(k\)-algebra \(k[x]/(f)\) and let \(X\) be the image of \(x\) in \(L\). Note that \(L\) is a product of fields, one for each Galois orbit of 2-torsion points in \(E(K)\). The norm from \(L\) to \(k\) induces a map from \(L^*/L^{*2}\) to \(k^*/k^{*2}\) that we continue to call the norm, and we let \(\hat{L}\) be the kernel of the norm \(L^*/L^{*2} \to k^*/k^{*2}\).

There is a homomorphism \(\iota : E(k)/2E(k) \to \hat{L}\) defined as follows: If \(P \in E(k)\) is a rational non-2-torsion point with \(x\)-coordinate \(x_P\), then \(\iota\) sends the class of \(P\) modulo \(2E(k)\) to the class of \(x_P - X\) modulo \(L^{*2}\). If \(P \in E(k)\) is a rational point of order 2, then \(x_P - X\) is nonzero in each component of \(L\) other than the one corresponding to \(P\); the value of \(\iota\) on the class of \(P\) is then the unique element of \(\hat{L}\) that agrees with \(x_P - X\) on the components where it is nonzero.

Similarly, we define a \(k\)-algebra \(L' = k[x]/(g)\) and a homomorphism \(\iota'\) from \(E(k)/2E(k)\) to \(\hat{L}'\). We note that the map \(\psi\) induces an isomorphism \(\psi^* : \hat{L}' \to \hat{L}\).

**Proposition 4.** A point \((P, Q) \in (E \times F)(k)\) lies in the image of \(J(k)\) under the map \((\varphi_*, \varphi'_*)\) if and only if the isomorphism \(\psi^*\) takes \(\iota'(Q)\) to \(\iota(P)\).

**Proof.** This follows immediately from [3, Proposition 12, p. 338].
3. A SMALL EXAMPLE

Let $E$ and $F$ be the elliptic curves over $\mathbb{Q}$ defined by $y^2 = f$ and $y^2 = g$, respectively, where

$$f = x^3 + 5x^2 + 6x + 1 \quad \text{and} \quad g = x^3 - 6x^2 + 5x - 1.$$ 

Let $K$ be the number field defined by the irreducible polynomial $f$. Let $r$ be a root of $f$ in $K$; then $-r^2 - 4r - 4$ and $r^2 + 3r - 1$ are also roots of $f$. Set $\alpha_1 = r, \quad \alpha_2 = -r^2 - 4r - 4, \quad \alpha_3 = r^2 + 3r - 1,$

and note that if we set $\beta_i = 1/\alpha_i$ then the $\beta_i$’s are the three roots of $g$.

Let $\psi: E[2](K) \rightarrow E[2](K)$ be the isomorphism that sends $(\alpha_i, 0)$ to $(\beta_i, 0)$, for $i = 1, 2, 3$. Using the formulas from [3, Proposition 4, p. 324], we see that the curve $C$ over $\mathbb{Q}$ defined by $y^2 = 7^8g(x^2)$ has Jacobian $J$ isomorphic to the quotient of $E \times F$ by the graph of $\psi$. Rescaling $y$, we find that $C$ has a model

$$y^2 = x^6 - 6x^4 + 5x^2 - 1.$$ 

The double cover $\varphi: C \rightarrow E$ is given by $(x, y) \mapsto (-1/x^2, y/x^3)$, and the double cover $\varphi': C \rightarrow F$ by $(x, y) \mapsto (x^2, y)$.

The curve $E$ is isomorphic to the curve 196A1 from Cremona’s database; its Mordell–Weil group is generated by the point $P = (-2,1)$ of infinite order. The curve $F$ is isomorphic to the curve 784F1 from Cremona’s database, and its Mordell–Weil group is trivial.

Let $\sigma$ be the involution $(x, y) \mapsto (-x, -y)$ of $C$, so that $\sigma$ generates the Galois group of the cover $C \rightarrow E$, and let $s$ be the corresponding involution of $J$. We know from Section 2 that the endomorphism $u = 1 + s$ of $J$ has connected kernel and has image isomorphic to $E$, and that the associated optimal cover $J \rightarrow E$ is simply $\varphi_*$. We claim that the point $P$ is not in the image under $\varphi_*$ of the Mordell–Weil group of $J$.

We prove this claim by contradiction. Suppose there were a point $R$ of $J(\mathbb{Q})$ with $\varphi_*(R) = P$. The only possible image for $R$ in $F(\mathbb{Q})$ is the identity element $O$, so we must have $(\varphi_*, \varphi'_*)(R) = (P, O)$. Now we apply Proposition 4. We see that the $\mathbb{Q}$-algebra $L$ from the proposition is simply the field $K$, the group $\bar{L}$ is the quotient of the subgroup of elements of $K^*$ with square norm by the subgroup $K^{r,2}$, and the map $\iota: E(\mathbb{Q})/2E(\mathbb{Q}) \rightarrow \bar{L}$ sends the class of a nonzero point $(x, y) \in E(\mathbb{Q})$ to the class in $\bar{L}$ of the element $x - r \in K^*$. (Note that $x - r$ does lie in the subgroup of $K^*$ of elements whose norms are squares, because the norm of $x - r$ is equal to $y^2$.)

Since $(P, O)$ lies in the image of $J(\mathbb{Q})$, Proposition 4 says $\iota(P)$ must be the trivial element of $\bar{L}$; that is, $-2 - r$ must be a square in $K$. But $-2 - r$ is not a square in $K$; this can be seen, for example, by looking modulo 13. Therefore $P$ is not in the image of under $\varphi_*$ of the Mordell–Weil group of $J$.

4. INFINITELY MANY EXAMPLES

The specific example given in Section 3 was chosen because the equations for the curves and the maps worked out to have small integer coefficients. In this section we present a method for producing infinitely many examples, without concerning ourselves about the simplicity of the equations we obtain.

Let $E$ and $F$ be two elliptic curves over $\mathbb{Q}$ defined by equations $y^2 = f$ and $y^2 = g$, respectively, where $f$ and $g$ are monic cubic polynomials in $\mathbb{Q}[x]$ that split
completely over \( \mathbb{Q} \). Let \( P_1, P_2, P_3 \) be the points of order 2 in \( E(\mathbb{Q}) \) and let \( Q_1, Q_2, Q_3 \) be the points of order 2 in \( F(\mathbb{Q}) \). Let \( C \) be the genus-2 curve over \( \mathbb{Q} \) produced by gluing \( E \) and \( F \) together along their 2-torsion subgroups using the isomorphism \( \psi: E[2](K) \rightarrow F[2](K) \) that takes \( P_i \) to \( Q_i \), for \( i = 1, 2, 3 \). Let \( \varphi: C \rightarrow E \) and \( \varphi': C \rightarrow F \) be the degree-2 maps associated to this data and let \( J \) be the Jacobian of \( C \). Suppose \( P \) is a rational point on \( E \). We know that \( P \) is in the image of \( J(\mathbb{Q}) \) under \( \varphi_* \) if and only if there is a point \( Q \) of \( F(\mathbb{Q}) \) such that \( (P, Q) \) is in the image of \( J(\mathbb{Q}) \) under the map \( (\varphi_*, \varphi'_*) \).

Again Proposition 4 tells us whether such a \( Q \) exists. In this case, because the 2-torsion points of \( E \) and \( F \) are all rational, the answer takes a slightly different shape than it did in the preceding section. Let \( Z \) be the subgroup of \( (\mathbb{Q}^* / \mathbb{Q}^{*2})^3 \) consisting of those triples \((r, s, t)\) whose product is equal to the trivial element of \( \mathbb{Q}^*/\mathbb{Q}^{*2} \). Then the group \( \hat{L} \) from Proposition 4 is isomorphic to \( Z \), and the isomorphism can be chosen so that the homomorphism \( \iota \) sends a non-2-torsion point \( P \) of \( E(\mathbb{Q}) \) to the class in \( Z \) of the triple

\[
(x(P) - x(P_1), x(P) - x(P_2), x(P) - x(P_3)).
\]

Likewise, \( \hat{L}' \) is isomorphic to \( Z \), and the isomorphism can be chosen so that the homomorphism \( \iota' \) sends a non-2-torsion point \( Q \) of \( F(\mathbb{Q}) \) to the class of

\[
(x(Q) - x(Q_1), x(Q) - x(Q_2), x(Q) - x(Q_3)).
\]

Under these identifications, the isomorphism \( \psi_* \) is nothing other than the identity on \( Z \). Thus, Proposition 4 says that a point \( (P, Q) \) in \( (E \times F)(\mathbb{Q}) \) is in the image of \( (\varphi_*, \varphi'_*) \) if and only if \( \iota(P) = \iota'(Q) \).

Suppose we are given an arbitrary elliptic curve \( E/\mathbb{Q} \) with rational points \( Q_1, Q_2, Q_3 \) of order 2. We will show that there are infinitely many geographically distinct choices for \( E/\mathbb{Q} \) with rational points \( P_1, P_2, P_3 \) of order 2 such that if \( \varphi: C \rightarrow E \) is constructed as above, then there is a point of infinite order in \( E(\mathbb{Q}) \) that is not contained in the subgroup of \( E(\mathbb{Q}) \) generated by the torsion elements and the image of \( J(\mathbb{Q}) \) under \( \varphi_* \).

If \( z \) is an element of \( (\mathbb{Q}^*/\mathbb{Q}^{*2})^3 \), we say that a prime \( p \) occurs in \( z \) if one of the components of \( z \) has odd valuation at \( p \). If \( E \) is an elliptic curve over \( \mathbb{Q} \) with all of its 2-torsion rational over \( \mathbb{Q} \), we say that a prime \( p \) occurs in \( E(\mathbb{Q}) \) if it occurs in some element of \( \iota(E(\mathbb{Q})) \); note that only finitely many primes occur in \( E(\mathbb{Q}) \) because \( E(\mathbb{Q}) \) is a finitely-generated group. Let \( \ell_1 \) and \( \ell_2 \) be two distinct odd primes that do not occur in \( F(\mathbb{Q}) \) and that are congruent to \( \ell_1 + 1 \) modulo \( \ell_1^2 \) and to \( \ell_2 - 1 \) modulo \( \ell_2^2 \), and let \( E_p \) be the elliptic curve

\[
y^2 = x(x + p + 1)(x - p + 1).
\]

Let \( P_1, P_2, \) and \( P_3 \) be the 2-torsion points on \( E_p \) with \( x \)-coordinates \( 0, -p - 1, \) and \( p - 1 \), respectively, and let \( P = (-1, p) \in E_p(\mathbb{Q}) \). We compute that the images of these points in \( Z \subset (\mathbb{Q}^*/\mathbb{Q}^{*2})^3 \) are as follows:

\[
\begin{align*}
\iota(P) &= (-1, p, -p) \\
\iota(P_1) &= (-p^2 + 1, p + 1, -p + 1) \\
\iota(P_2) &= (-p - 1, 2p(p + 1), -2p) \\
\iota(P_3) &= (p - 1, 2p, 2p(p - 1)).
\end{align*}
\]
We see that \( p \) occurs in \( \iota(P) \), that \( p \) occurs in \( \iota(P + P_1) \), that \( \ell_2 \) occurs in \( P + P_2 \), and that \( \ell_1 \) occurs in \( P + P_3 \).

Note that \( \iota(P_1) \), \( \iota(P_2) \), and \( \iota(P_3) \) are nontrivial, because either \( \ell_1 \) or \( \ell_2 \) occurs in each of them. This shows that none of the points \( P_1 \), \( P_2 \), and \( P_3 \) is the double of a rational point. Since we know the possible torsion structures of elliptic curves over \( \mathbb{Q} \) [7, Theorem 8, p. 35], we see that \( E_p \) has torsion subgroup isomorphic to either \( \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \) or \( \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \). If there is a rational 3-torsion point \( T \) on \( E \), then \( \iota(T) = (1, 1, 1) \), because \( T \) is twice \(-T\). Combining this with what we have already shown, we find that \( \iota(P) \) is not contained in the group generated by \( \iota'(F(\mathbb{Q})) \) and the image under \( \iota \) of the torsion subgroup of \( E(\mathbb{Q}) \). From this, we see that \( P \) is not contained in the subgroup of \( E(\mathbb{Q}) \) generated by the torsion elements and the image of \( J(\mathbb{Q}) \) under \( \varphi_\ast \).

Finally, we note that the \( j \)-invariant of \( E_p \) is given by

\[
\begin{align*}
j(E_p) &= \frac{64(3p + 1)^3}{p^2(p - 1)^2(p + 1)^2},
\end{align*}
\]

so that, since \( p \) is odd, it is the largest prime for which \( j(E_p) \) has negative valuation. Therefore distinct odd primes \( p \) and \( q \) give geometrically nonisomorphic curves \( E_p \) and \( E_q \), so there are infinitely many curves \( E_p \) that we can glue to \( F \) as above to get examples showing that the answer to Schaefer’s question is no.

References

[1] Brian Conrad and William A. Stein, Component groups of purely toric quotients, Math. Res. Lett. 8 (2001), no. 5-6, 745–766.
[2] Gerhard Frey and Ernst Kani, Curves of genus 2 covering elliptic curves and an arithmetical application, Arithmetic algebraic geometry (Texel, 1989), Progr. Math., vol. 89, Birkhäuser Boston, Boston, MA, 1991, pp. 153-176.
[3] Everett W. Howe, Franck Leprévost, and Bjorn Poonen, Large torsion subgroups of split Jacobians of curves of genus two or three, Forum Math. 12 (2000), no. 3, 315–364.
[4] C. G. J Jacobi, Review of Legendre’s Traité des fonctions elliptiques, troisième supplément, J. Reine Angew. Math. 8 (1832), 413–417.
[5] C. G. J. Jacobi, Gesammelte Werke. Erster Band, Herausgegeben auf Veranlassung der Königlich Preussischen Akademie der Wissenschaften, Verlag von G. Reimer, Berlin, 1881.
[6] A. M. Legendre, Traité des fonctions elliptiques et des intégrales Eulériennes, Tome troisième, Huzard–Courcier, Paris, 1828.
[7] B. Mazur, Modular curves and the Eisenstein ideal, Inst. Hautes Études Sci. Publ. Math. 47 (1977), 33–186.
[8] J. S. Milne, Jacobian varieties, Arithmetic geometry (Storrs, Conn., 1984) (G. Cornell and J.H. Silverman, eds.), Springer, New York, 1986, pp. 167–212.

Center for Communications Research, 4320 Westerra Court, San Diego, CA 92121-1967, USA.

E-mail address: however@alumni.caltech.edu
URL: http://www.alumni.caltech.edu/~however/