Supplement to:
Covering Collections and a Challenge Problem of Serre

E. Victor Flynn*, Mathematical Institute, University of Oxford

Joseph L. Wetherell†, Department of Mathematics, University of Southern California

§0. Introduction

In the article *Covering Collections and a Challenge Problem of Serre* [9], we showed that the problem of finding $\mathcal{D}(\mathbb{Q})$ for:

$$\mathcal{D} : x^4 + y^4 = 17$$

can be reduced to that of showing $\mathcal{C}(\mathbb{Q})$ has no affine points, where:

$$\mathcal{C} : y^2 = (9x^2 - 28x + 18)(x^2 + 12x + 2)(x^2 - 2),$$

which in turn can to showing that the following curve has no affine $(x, v) \in \mathcal{F}(\mathbb{Q}(\sqrt{2}, \sqrt{34}))$ with $x \in \mathbb{Q}$, where:

$$\mathcal{F} : v^2 = (9x^2 - 28x + 18)(x - (-6 + \sqrt{34}))(x - \sqrt{2}). \tag{2.8}$$

In this supplement, we give an alternative way of showing how finding $\mathcal{C}(\mathbb{Q})$ can be reduced to that of finding all $(x, v) \in \mathcal{F}(\mathbb{Q}(\sqrt{2}, \sqrt{34}))$ with $x \in \mathbb{Q}$.

§1. Covering Collections Induced by $J(K)/2J(K)$

Suppose we have a hyperelliptic curve defined over a number field K, with a known K-rational point mapped to infinity

$$\begin{aligned} \mathcal{C} : y^2 = F(x) &= f_n x^n + \ldots + f_1 x + f_0, \text{ with } f_n \in (K^*)^2,\ 4 \not| \, n, \\ &= F_1(x) \ldots F_k(x), \end{aligned} \tag{1.1}$$

* The author thanks the Nuffield Foundation (Grant SCI/180/96/71/G) for financial support.

† The author thanks the National Science Foundation (Grant DMS-9705959) for financial support.

where $F_1(x), \ldots, F_k(x)$ are irreducible factors of $F(X)$ over K. For each i, let α_i be a root of $F_i(x)$, and $L_i = K(\alpha_i)$. When n is even, we let $\infty^+, \infty^- \in \mathcal{C}(K)$ denote the points on the non-singular curve that lie over the point at infinity on $\mathcal{C}$; when n is odd, there is one such point, which we denote $\infty^+ \in \mathcal{C}(K)$. Our simplifying condition $4 \not| n$ guarantees that any 2-torsion member of $J(K)$ can be represented by a K-rational set of Weierstrass points on $\mathcal{C}$. Define a map q (as in [2] p.48) on $J(\mathbb{Q})$ by

$$\begin{aligned} q : J(\mathbb{Q}) &\to \Big(L_1^*/(L_1^*)^2 \times \ldots \times L_k^*/(L_k^*)^2\Big)/\sim \\ &: [\sum_{j=1}^{\ell} n_j(x_j, y_j)] \mapsto [\prod_{j=1}^{\ell}(x_j - \alpha_1)^{n_j}, \ldots, \prod_{j=1}^{\ell}(x_j - \alpha_k)^{n_j}], \end{aligned} \tag{1.2}$$

where the equivalence relation $\sim$ is defined by

$$\begin{aligned} &n \text{ even. } [a_1, \ldots, a_k] \sim [b_1, \ldots, b_k] \iff a_1 = wb_1, \ldots, a_k = wb_k, \text{ for some } w \in K^*. \\ &n \text{ odd. } [a_1, \ldots, a_k] \sim [b_1, \ldots, b_k] \iff a_1 = b_1, \ldots, a_k = b_k. \end{aligned} \tag{1.3}$$

In other words, when n is odd, one is not required to include the quotient by $\sim$ in (1.2). In the above definition, $x_j - \alpha_i$ should be taken to be 1 when (x_j, y_j) is any point at infinity. When n is odd, $2J(K)$ is the kernel of q. When n is even, $2J(K)$ is either the kernel of q or has index 2 in the kernel of q (see [10],[14]). The square brackets in the left hand side of (1.2) denote an equivalence class of divisors modulo linear equivalence, whereas those on the right hand side merely enclose an ordered list of elements.

Now suppose that $G(x)|F(x)$ and that $2|\deg(G(x))\deg\big(F(x)/G(x)\big)$. Then there is an induced map

$$q_G : J(K) \to L_G^*/(L_G^*)^2 : [\sum_{j=1}^{\ell} n_j(x_j, y_j)] \mapsto \prod_{j=1}^{\ell} G(x_j)^{n_j}, \tag{1.4}$$

where L_G denotes the smallest field containing K over which $G(x)$ is defined. The condition $2|\deg(G(x))\deg\big(F(x)/G(x)\big)$ is just a way of saying $\deg\big(F(x)\big)$ even $\Rightarrow \deg\big(G(x)\big)$ even, which allows the relation $\sim$ to be absorbed.

We now suppose that we have performed a 2-descent which has successfully found $J(K)/2J(K)$. There are several descriptions in the literature of the methodology ([2],[7],[10],[11]). It is then straightforward to deduce $J(K)/\ker(q)$, which we list as

$$J(K)/\ker(q) = \{D_1, \ldots, D_r\}. \tag{1.5}$$

Let $P = (x, y) \in \mathcal{C}(K)$ so that $[P - \infty^+] \in J(K)$. Then, for some $i \in \{1, \dots, r\}$, we must have $q([(x, y) - \infty^+]) = q(D_i)$, giving that $q_G([P - \infty^+]) = q_G(D_i)$ for all $G(x)|F(x)$ with $2|\deg(G(x))\deg\big(F(x)/G(x)\big)$. That is

$$q_G(D_i)G(x) \in (L_G^*)^2 \text{ for all } G(x)|F(x) \text{ with } 2|\deg(G(x))\deg\big(F(x)/G(x)\big). \tag{1.6}$$

Each choice of G therefore gives a hyperelliptic curve defined over L_G on which there must be an L_G-rational point with K-rational x-coordinate. We let $\mathcal{B}_i$ denote the curve defined by all of these equations:

$$\mathcal{B}_i : \{v_{i,G}^2 = q_G(D_i)G(x) : \; G(x)|F(x), \; 2|\deg(G(x))\deg\big(F(x)/G(x)\big)\}. \tag{1.7}$$

In order to determine all points $P \in \mathcal{C}(K)$ it is therefore sufficient, for each $i \in \{1, \dots r\}$, to find all points on $\mathcal{B}_i$ with $x \in K$ and each $v_{i,G} \in L_G^*$. It may be that these can be reduced to a finite set by local arguments directly applied to the curves $v_{i,G}^2 = q_G(D_i)G(x)$. When $G(x)$ has degree 3 or 4, it may be that $v_{i,G}^2 = q_G(D_i)G(x)$ turns out to be an elliptic curve whose rank over L_G is less than $[L_G : K]$. In such cases, Chabauty techniques as in [1] and [8] can be applied, as will be illustrated in Section 3. We note that the idea of using hyperelliptic curves resulting from factors of $F(X)$ is also discussed in [1] and [3] (see also [15] for related ideas); the new idea in our applications is that we are using information from $J(K)/\ker(q)$ to assist in the process.

§2. Application to Serre's Curve

Recall the genus 2 curve of (0.9)

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

where

$$\begin{aligned}
&G_1(x) = 9x^2 - 28x + 18 = (x - \alpha_1)(x - \beta_1), \; \alpha_1 = 14/9 + 1/9\sqrt{34}, \; \beta_1 = 14/9 - 1/9\sqrt{34},\\
&G_2(x) = x^2 + 12x + 2 = (x - \alpha_2)(x - \beta_2), \; \alpha_2 = -6 + \sqrt{34}, \; \beta_2 = -6 - \sqrt{34},\\
&G_3(x) = x^2 - 2 = (x - \alpha_3)(x - \beta_3), \; \alpha_3 = \sqrt{2}, \beta_3 = -\sqrt{2}.
\end{aligned} \tag{2.2}$$

We note in passing that $\mu = (5x-4)/(2x-5)$ is an involution which swaps roots of $F(x)$: $\alpha_1 \leftrightarrow \beta_2$, $\alpha_2 \leftrightarrow \beta_1$, and $\alpha_3 \leftrightarrow \beta_3$, and so $s = (x+\mu)/2 = (x^2-2)/(2x-5)$ is invariant under this involution. Then $(x,y) \mapsto ((x^2-2)/(2x-5), y(x-(5+\sqrt{17})/2)/(2x-5)^2)$ is a map from $\mathcal{C}$ to the elliptic curve

$$t^2 = s(s-(5+\sqrt{17})/2)(9s^2+40s-16). \tag{2.3}$$

This shows that the Jacobian J of $\mathcal{C}$ is bielliptic and indeed the above map induces a 4-isogeny over $\mathbb{Q}$ to the Weil restriction of scalars over $\mathbb{Q}$ of (2.3). A consequence is that the rank of $J(\mathbb{Q})$ is the same as the rank over $\mathbb{Q}(\sqrt{17})$ of the elliptic curve in (2.3). This gives us two ways of computing the rank of $J(\mathbb{Q})$: either directly on $\mathcal{C}$ as in [7], or by performing a descent via isogeny on the elliptic curve (2.3) as in [4,5,12,13]. Indeed, since $\mathbb{Q}(\sqrt{17})$ is a real field of class number 1, this can be performed by the program SIMATH, which can be found at

http://emmy.math.uni-sb.de/~simath/

This confirmed the rank of (2.3) over $\mathbb{Q}(\sqrt{17})$ (and hence the rank of $J(\mathbb{Q})$) to be 2, independently of our own computations. We shall not need to make any further use of the fact that J is bielliptic, and the rest of our argument follows the outline of Section 1.

Note that the map q of (1.2) specialises to

$$\begin{aligned} q : J(\mathbb{Q}) &\to \Big(\mathbb{Q}(\sqrt{34})^*/(\mathbb{Q}(\sqrt{34})^*)^2 \times \mathbb{Q}(\sqrt{34})^*/(\mathbb{Q}(\sqrt{34})^*)^2 \times \mathbb{Q}(\sqrt{2})^*/(\mathbb{Q}(\sqrt{2})^*)^2\Big)/\sim \\ : [\sum_{j=1}^{\ell} n_j(x_j,y_j)] &\mapsto [\prod_{j=1}^{\ell}(x_j-\alpha_1)^{n_j}, \prod_{j=1}^{\ell}(x_j-\alpha_2)^{n_j}, \prod_{j=1}^{\ell}(x_j-\alpha_3)^{n_j}] \\ &= [\prod_{j=1}^{\ell}(x_j-(14/9+1/9\sqrt{34}))^{n_j}, \prod_{j=1}^{\ell}(x_j-(-6+\sqrt{34}))^{n_j}, \prod_{j=1}^{\ell}(x_j-\sqrt{2})^{n_j}]. \end{aligned} \tag{2.4}$$

On computing the reduction of the Jacobian modulo 3, the resulting group is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, into which the torsion group of $J(\mathbb{Q})$ must inject. Therefore, the 2-torsion of $J(\mathbb{Q})$ gives the whole of the torsion group of $J(\mathbb{Q})$. The 2-torsion of $J(\mathbb{Q})$, and therefore the whole torsion group, is easily seen to be generated by $[(\alpha_1,0)-(\beta_1,0)]$ and $[(\alpha_2,0)-(\beta_2,0)]$. Therefore $[\infty^+ - \infty^-] \in J(\mathbb{Q})$ is of infinite order, and is in the kernel of q. Recall also from [7] that if, for some $d \in \mathbb{Q}$, we let $\theta_1, \ldots, \theta_6$ be the roots of

$H(X) = F(X+d)$, and find that $h(X) = \prod(X - \theta_i\theta_j\theta_k - \theta_\ell\theta_m\theta_n)$ is square free and has no $\mathbb{Q}$-rational root, then $[\infty^+ - \infty^-] \notin 2J(\mathbb{Q})$. The product in the definition of $h(X)$ is taken over the ten unordered partitions of the six roots $\theta_1, \ldots, \theta_6$ of $H(X)$ into two sets of three. Applying this to $H(X) = F(X+1)$ gives $h(X)$ of degree 10 with factors irreducible over $\mathbb{Q}$:

$$27x^2 - 420x + 908,\ 9x^2 - 276x - 2236,\ 81x^2 - 36x - 1084,$$
$$27x^2 - 420x - 1268,\ 81x^2 + 2412x - 19036,$$

and so $[\infty^+ - \infty^-] \notin 2J(\mathbb{Q})$. We know (see [2] and [10]) that $2J(\mathbb{Q})$ has index at most 2 in the kernel of q, so we have established that $[\infty^+ - \infty^-]$ is not in $2J(\mathbb{Q})$, and that the kernel of q is the group generated by $2J(\mathbb{Q})$ and $[\infty^+ - \infty^-]$. We are missing one further infinite generator of $J(\mathbb{Q})$. A short search finds

$$\begin{aligned}&[(x_1, y_1) + (x_2, y_2) - \infty^+ - \infty^-] \in J(\mathbb{Q}),\ \text{where}\\ &x_1, x_2 \text{ are the roots of } 5x^2 - 18x + 17,\ \text{and } y_j = 3(-603x_j + 1187)/50,\ j = 1, 2.\end{aligned} \tag{2.5}$$

It is easily checked that $[(\alpha_1, 0) - (\beta_1, 0)]$, $[(\alpha_2, 0) - (\beta_2, 0)]$ and $[(x_1, y_1) + (x_2, y_2) - \infty^+ - \infty^-]$ all map to independent images under q of (2.4). In summary, since $J(\mathbb{Q})$ has rank 2, it must be that $[\infty^+ - \infty^-]$, $[(\alpha_1, 0) - (\beta_1, 0)]$, $[(\alpha_2, 0) - (\beta_2, 0)]$ and $[(x_1, y_1) + (x_2, y_2) - \infty^+ - \infty^-]$ are a set of generators for $J(\mathbb{Q})/2J(\mathbb{Q})$, with the latter 3 being generators for $J(\mathbb{Q})/\ker(q)$. We summarise what we need in the following Lemma.

Lemma 2.1. *Let $\mathcal{C}$ be the curve of genus 2 in (2.1), and let J be the Jacobian of $\mathcal{C}$. Then $J(\mathbb{Q})/\ker(q) = \{D_1, \ldots D_8\}$, where*

$$D_1 = \textit{identity},\ D_2 = [(\alpha_1, 0) - (\beta_1, 0)],\ D_3 = [(\alpha_2, 0) - (\beta_2, 0)], D_4 = [(\alpha_3, 0) - (\beta_3, 0)],$$
$$D_5 = [(x_1, y_1) + (x_2, y_2) - \infty^+ - \infty^-],\ D_6 = D_5 + D_2,\ D_7 = D_5 + D_3,\ D_8 = D_5 + D_4,$$

with $(x_1, y_1), (x_2, y_2)$ as in (2.5). □

Now suppose that $(x, y) \in \mathcal{C}(\mathbb{Q})$. Then $[(x, y) - \infty^+] \in J(\mathbb{Q})$ and so $[(x, y) - \infty^+] = D_i$ in $J(\mathbb{Q})/\ker(q)$ for some $i \in \{1, \ldots 8\}$.

We first consider the case $i = 2$. Note that, since $F(X)$ has even degree, the condition $2|\deg(G(x))\deg\big(F(x)/G(x)\big)$ means we must restrict ourselves to $G(X)$ of even degree with $G(X)|F(X)$. We compute $q_{G_2}(D_2) = 2$ and $q_{G_3}(D_2) = -17$ in $\mathbb{Q}^*/(\mathbb{Q}^*)^2$, so that if $[(x,y) - \infty^+] = D_2$ then

$$\begin{aligned} v_{2,G_2}^2 &= q_{G_2}(D_2)G_2(x) = 2(x^2 + 12x + 2), \\ v_{2,G_3}^2 &= q_{G_3}(D_2)G_3(x) = -17(x^2 - 2), \end{aligned} \tag{2.6}$$

for some $v_{2,G_2}, v_{2,G_3} \in \mathbb{Q}$ (since $G_2(x)$ and $G_3(x)$ are defined over $\mathbb{Q}$). The second equation forces x to be a 2-adic unit, but then the right hand side of the first equation has odd 2-adic valuation, and so cannot be a square. Therefore, (2.6) has no solutions in $\mathbb{Q}_2$ and therefore none in $\mathbb{Q}$. We also compute $q_{G_2}(D_i) = -34, -17, 2, -34, -17$ and $q_{G_3}(D_i) = -17, 1, -17, -17, 1$ for $i = 3, 4, 6, 7, 8$, respectively, and again find that in each case the pair of equations $v_{i,G_2}^2 = q_{G_2}(D_i)G_2(x)$, $v_{i,G_3}^2 = q_{G_2}(D_i)G_2(x)$ have no solution in $\mathbb{Q}_2$. We have therefore dismissed the possibility that $[(x,y) - \infty^+] = D_i$, for $i = 2, 3, 4, 6, 7, 8$ merely by use of $G = G_2, G_3$ and a 2-adic argument. This leaves only $i = 1, 5$.

For $i = 1, 5$ we compute $q_{G_2}(D_i) = q_{G_3}(D_i) = 1$, and there are $\mathbb{Q}$-rational points at infinity on $v_{i,G_2}^2 = q_{G_2}(D_i)G_2(x)$, $v_{i,G_3}^2 = q_{G_2}(D_i)G_2(x)$. The pair of equations defines an elliptic curve over $\mathbb{Q}$ of nonzero rank, and so this does not provide a way of reducing to a finite number of $x \in \mathbb{Q}$. Attempts to use $G(x)|F(x)$ defined over $\mathbb{Q}(\sqrt{34})$ were also unsuccessful, and so the remaining possibility is to try $G(x)|F(x)$ defined over $\mathbb{Q}(\sqrt{34}, \sqrt{2})$. We take

$$G_4(x) = G_1(x)(x - \alpha_2)(x - \alpha_3) = (9x^2 - 28x + 18)(x - (-6 + \sqrt{34}))(x - \sqrt{2}), \tag{2.7}$$

defined over $K = \mathbb{Q}(\sqrt{34}, \sqrt{2})$. We compute $q_{G_4}(D_1) = 1$, so that if $[(x,y) - \infty^+] = D_1$ then

$$\mathcal{F} : v_{1,G_4}^2 = (9x^2 - 28x + 18)(x - (-6 + \sqrt{34}))(x - \sqrt{2}), \tag{2.8}$$

for some $v_{1,G_4} \in K$. We also compute, using x_1, x_2 as in (2.5),

$$\begin{aligned} q_{G_4}(D_5) &= G_4(x_1)G_4(x_2) \\ &= 12825 - 2106\sqrt{34} - 8550\sqrt{2} + 1404\sqrt{34}\sqrt{2} \\ &= (39 - 9\sqrt{34} - 39\sqrt{2} + 9\sqrt{34}\sqrt{2})^2 \end{aligned} \tag{2.9}$$

which is just 1 in $K^*/(K^*)^2$. Therefore if $[(x,y) - \infty^+] = D_5$ then x must again be an x-coordinate of $\mathcal{F}$. If we can show that there are affine no points in $\mathcal{F}(K)$ with $\mathbb{Q}$-rational

x-coordinate, then there will be no $\mathbb{Q}$-rational affine points on $\mathcal{C}$ whatsoever. We summarise this in the following Lemma.

Lemma 2.2. *Let* $K = \mathbb{Q}(\sqrt{34}, \sqrt{2})$ *and* $\mathcal{F}, \mathcal{C}, \mathcal{D}$ *be as in (2.8),(2.1),(0.1) with* $c = 17$*. If there are no affine points in* $\mathcal{F}(K)$ *with* $\mathbb{Q}$*-rational* x*-coordinate, then* $\mathcal{C}(\mathbb{Q}) = \{\infty^+, \infty^-\}$ *and* $\mathcal{D}(\mathbb{Q}) = \{(\pm 1, \pm 2, 1), (\pm 2, \pm 1, 1)\}$. □

In order to apply the Chabauty style methods of Sections 3,4, we hope that the rank of $\mathcal{F}(K)$ is less than $[K : \mathbb{Q}] = 4$. In fact, a complete 2-descent shows the following.

Lemma 2.3. *Let* $K = \mathbb{Q}(\sqrt{34}, \sqrt{2})$ *and* $\mathcal{F}$ *be as in (2.8). Then* $\mathcal{F}(K)$ *has rank 1, with* $[\infty^+ - (-6 + \sqrt{34}, 0)]$ *a point of infinite order.* □

The computation of the above rank was helped by the fact that K has class number 1. Since there is already considerable literature on computing ranks of elliptic curves over number fields (for example [5,12,13]), we do not include the argument here, but have placed in the file www.maths.ox.ac.uk/~flynn/genus2/serrecurve/rank.computation the details of the computation.

REFERENCES

[1] Bruin, N. *Chabauty methods and covering techniques applied to generalised Fermat equations.* PhD Dissertation, Leiden, 1999.

[2] Cassels, J.W.S. and Flynn, E.V. *Prolegomena to a Middlebrow Arithmetic of Curves of Genus 2.* Cambridge University Press, 1996.

[3] Coombes, K.R. and Grant, D.R. *On Heterogeneous Spaces*, J. London Math. Soc. (2) **40** (1989), no. 3. 385–397.

[4] Cremona, J.E. and Serf, P. *Computing the rank of elliptic curves over real quadratic number fields of class number 1.* To appear in Math. Comp.

[5] Djabri, Z., Schaefer, E.F. and Smart, N.P. *Computing the p-Selmer group of an elliptic curve.* To appear in Trans. A.M.S.

[7] Flynn, E.V., Poonen, B. and Schaefer, E.F. *Cycles of quadratic polynomials and rational points on a genus-two curve.* Duke Math. J. **90** (1997), 435–463.

[8] Flynn, E.V. and Wetherell, J.L. *Finding Rational Points on Bielliptic Genus 2 Curves.* Manuscripta Math. **100** (1999), 519–533.

[9] Flynn, E.V. and Wetherell, J.L. *Covering Collections and a Challenge Problem of Serre.* Acta Arith. **XCVIII.2** (2001), 197–205.

[10] Poonen, B. and Schaefer, E.F. *Explicit descent for Jacobians of cyclic covers of the projective line.* J. reine angew. Math. **488** (1997), 141–188.

[11] Schaefer, E.F. *2-descent on the jacobians of hyperelliptic curves.* J. Number Theory **51** (1995), 219–232.

[12] Siksek, S. *Infinite descent on elliptic curves.* Rocky Mountain Journal of Mathematics **25 No. 4** (1995), 1501–1538.

[13] Silverman, J.H. *The Arithmetic of Elliptic Curves.* Springer-Verlag, New York (1986).

[14] Stoll, M. *Implementing 2-Descent for Jacobians of Hyperelliptic Curves.* Manuscript (2000).

[15] Wetherell, J.L. *Bounding the Number of Rational Points on Certain Curves of High Rank*, PhD Dissertation (1997), University of California at Berkeley.

E. Victor Flynn, Mathematical Institute, 24–29 St. Giles, University of Oxford,
Oxford OX1 3LB, United Kingdom. flynn@maths.ox.ac.uk

Joseph L. Wetherell, Department of Mathematics, University of Southern California,
1042 W.36th Place, Los Angeles, CA 90089-1113, U.S.A. jlwether@alum.mit.edu