CYCLES OF COVERS

E. V. FLYNN AND J. WUNDERLE

Abstract. We initially consider an example of Flynn and Redmond, which gives an infinite family of curves to which Chabauty's Theorem is not applicable, and which even resist solution by one application of a certain bielliptic covering technique. In this article, we shall consider a general context, of which this family is a special case, and in this general situation we shall prove that repeated application of bielliptic covers always results in a sequence of genus 2 curves which cycle after a finite number of repetitions. We shall also give an example which is resistant to repeated applications of the technique.

1. Introduction

We begin with the following result (a variation of the result and argument used in Lemma 2.2.1 of [2]; see also the covering ideas in [8] for general context), which we shall use later.

Lemma 1. *Let $\mathcal{C} : dY^2 = F(X) = F_1(X)F_2(X)$ be defined over a number field K, with $F_1(X), F_2(X)$ each defined over L (a finite extension of K), with disc$(F) \neq 0$, and with $F_1(X), F_2(X)$ not both of odd degree. Then there exists a finite set $\mathcal{D} = \{d_1, \ldots, d_m\} \subseteq L$ such that, for all $(X_0, Y_0) \in \mathcal{C}(K)$ there exist $d_i \in \mathcal{D}, V_1, V_2 \in L$ satisfying $d_i V_1^2 = F_1(X_0)$, $(d/d_i)V_2^2 = F_2(X_0)$.*

Proof We first multiply both sides of $\mathcal{C}$ by a member of $\mathbb{Z}$ so that $d, F, \mathcal{C}$ are defined over $\mathcal{O}_K$, the ring of integers of K, and F_1, F_2 are defined over $\mathcal{O}_L$, the ring of integers of L. Let $R \in \mathcal{O}_L^*$ be the resultant of $F_1(X)$ and $F_2(X)$, and let $p(X), q(X) \in \mathcal{O}_L[X]$ be such that $p(X)F_1(X) + q(X)F_2(X) = R$. Also let $\widetilde{F}_1(X) = F_1(1/X)X^{\deg'(F_1)}, \widetilde{F}_2(X) = F_2(1/X)X^{\deg'(F_2)} \in \mathcal{O}_L[X]$, where each $\deg'(F_i) = \text{degree}(F_i)$ or degree$(F_i) + 1$, when degree(F_i) is even or odd, respectively. Let $\widetilde{R} \in \mathcal{O}_L^*$ be the resultant of $\widetilde{F}_1(X)$ and $\widetilde{F}_2(X)$. For any prime ideal $\mathfrak{p}$ of $\mathcal{O}_L$, let $v_\mathfrak{p}$ denote the corresponding discrete valuation, normalised so that $v_\mathfrak{p}(L^*) = \mathbb{Z}$. Let S denote the set of places of L for which $v_\mathfrak{p}(d) = v_\mathfrak{p}(R) = v_\mathfrak{p}(\widetilde{R}) = 0$, together with all places of L at infinity. Then S is finite and so the set $L(S,2) = \{x \in L^*/(L^*)^2 : v_\mathfrak{p}(x) \text{ is even, for all } \mathfrak{p} \notin S\}$ is also finite (see VIII.1.6 and X.1.2 of [13]); say that $\mathcal{D} = \{d_1, \ldots, d_m\}$ is a set of representatives for $L(S,2)$.

Let $(X_0, Y_0) \in \mathcal{C}(K)$ and let $\mathfrak{p} \notin S$. Either $v_\mathfrak{p}(X_0) \geq 0$ or $v_\mathfrak{p}(1/X_0) = -v_\mathfrak{p}(X_0) \geq 0$; we first consider the case when $v_\mathfrak{p}(X_0) \geq 0$. Then $v_\mathfrak{p}(F_1(X_0)), v_\mathfrak{p}(F_2(X_0)), v_\mathfrak{p}(p(X_0)), v_\mathfrak{p}(q(X_0)) \geq 0$ and we cannot have both $v_\mathfrak{p}(F_1(X_0)) > 0$ and $v_\mathfrak{p}(F_2(X_0)) > 0$ (since this would give $v_\mathfrak{p}(R) = v_\mathfrak{p}(p(X_0)F_1(X_0) + q(X_0)F_2(X_0)) > 0$, contradicting the fact that $v_\mathfrak{p}(R) = 0$). The equation for $\mathcal{C}$ gives $v_\mathfrak{p}(d) + 2v_\mathfrak{p}(Y_0) = v_\mathfrak{p}(F_1(X_0)) + v_\mathfrak{p}(F_2(X_0))$. Since $v_\mathfrak{p}(d) = 0$ and since at least one of $v_\mathfrak{p}(F_1(X_0)) = 0$ or $v_\mathfrak{p}(F_2(X_0)) = 0$, it follows that both $v_\mathfrak{p}(F_1(X_0))$ and $v_\mathfrak{p}(F_2(X_0))$ are even. For the case when $v_\mathfrak{p}(1/X_0) \geq 0$, the same argument, applied to $\widetilde{F}_1, \widetilde{F}_2$, shows

Date: March 17, 2008.

1991 *Mathematics Subject Classification.* Primary 11G30; Secondary 11G10, 14H40.

Key words and phrases. Coverings of Curves, Descent, Jacobians, Method of Chabauty.

The first author thanks the International Center for Transdisciplinary Studies at Jacobs University Bremen for its hospitality during July 2007, and thanks EPSRC for support: grant number EP/F060661/1.

that both $v_{\mathfrak{p}}(\widetilde{F}_1(1/X_0))$ and $v_{\mathfrak{p}}(\widetilde{F}_2(1/X_0))$ are even, and so again $v_{\mathfrak{p}}(F_1(X_0)) = v_{\mathfrak{p}}(\widetilde{F}_1(1/X_0)X_0^{\deg'(F_1)})$ and $v_{\mathfrak{p}}(F_2(X_0)) = v_{\mathfrak{p}}(\widetilde{F}_2(1/X_0)X_0^{\deg'(F_2)})$ are both even. In both cases, we have shown both $v_{\mathfrak{p}}(F_1(X_0))$ and $v_{\mathfrak{p}}(F_2(X_0))$ to be even for all $\mathfrak{p} \notin S$, so that $F_1(X_0)(L^*)^2 \in L(S,2)$, giving that $d_i V_1^2 = F_1(X_0)$ for some $d_i \in \mathcal{D}, V_1 \in L^*$. The equation of $\mathcal{C}$ then gives that $(d/d_i)V_2^2 = F_2(X_0)$, where $V_2 = Y_0/V_1$, as required. □

We say that a curve of genus 2 is *bielliptic* if it is a double cover of an elliptic curve. Let $\mathcal{C} : Y^2 = F(X)$ be any hyperelliptic curve of genus ≥ 2, defined over a number field K. Let L be the splitting field of $F(X)$, and use a map of the form $(X,Y) \mapsto \big((\alpha X+\beta)/(\gamma X+\delta), Y/(\gamma X+\delta)^k\big)$ to map three of the Weierstrass points to infinty, $(0,0)$ and $(1,0)$, so that $\mathcal{C}$ is birationally equivalent over L to a curve of the form $Y^2 = X(X-1)(X-a_1)\dots(X-a_n)$, where $n \geq 3$ is odd.

Corollary 1. *Let $\mathcal{C} : Y^2 = F(X) = X(X-1)(X-a_1)\dots(X-a_n)$, be a curve of genus ≥ 2, defined over a number field L, where $F(X)$ has nonzero discriminant and $n \geq 3$ is odd. Then there exists a finite extension M of L such that, for any $(X_0,Y_0) \in \mathcal{C}(L)$, there exist $V_0, W_0 \in M$ such that $V_0^2 = X_0(X_0-1)$ and such that (T_0,W_0), where $T_0 = V_0/X_0$, gives an M-rational point on the bielliptic genus 2 curve: $W^2 = -(T^2-1)(a_1T^2+1-a_1)(a_2T^2+1-a_2)$.*

Proof Let $\mathcal{D}$ and $\mathcal{D}'$ be the finite sets of Lemma 1 for the cases when $F_1(X) = X(X-1), F_2(X) = (X-a_1)\dots(X-a_n)$ and $F_1(X) = X(X-a_1)(X-a_2), F_2(X) = (X-1)(X-a_3)\dots(X-a_n)$, respectively. Let M be the finite extension of L such that all members of $\mathcal{D},\mathcal{D}'$ are in $(M^*)^2$. Let $(X_0,Y_0) \in \mathcal{C}(L)$; by Lemma 1, there exist $V_0 \in M, Z_0 \in M$ such that $V_0^2 = X_0(X_0-1)$ and $Z_0^2 = X_0(X_0-a_1)(X_0-a_2)$. Letting $T_0 = V_0/X_0$ gives $X_0 = 1/(1-T_0^2)$ and so: $Z_0^2 = -(a_1T_0^2+1-a_1)(a_2T_0^2+1-a_2)/(T_0^2-1)^3$. Letting $W_0 = Z_0(T_0^2-1)^2$ gives that (T_0,W_0) lies on the required curve. □

The above shows that Falting's Theorem for bielliptic genus 2 curves implies Falting's Theorem for all hyperelliptic curves (for similar ideas in a more general context, see [1]). This provides some motivation for investigating bielliptic genus 2 curves, particularly from the point of view of potential explicit methods.

We briefly recall the main steps of a bielliptic genus 2 example in [12], which we shall later place in a more general context. In [12] the authors consider the family of bielliptic genus 2 curves $\mathcal{C} : Y^2 = (X^2+p)(X^4+p^2)$ over $\mathbb{Q}$, where $p \equiv 7 \bmod 8$ is prime, and observe that it is sufficient to find all points (with $X, Y_0 \in \mathbb{Q}$ and $Y_1, Y_2 \in \mathbb{Q}(i)$, conjugate over $\mathbb{Q}$) on

$$Y_0^2 = \delta_1\delta_2(X^4+p^2), \quad Y_1^2 = \delta_2(X^2+p)(X^2+pi), \quad Y_2^2 = \delta_1(X^2+p)(X^2-pi), \tag{1}$$

for finitely many choices of δ_1,δ_2. Here, $\delta_1,\delta_2 \in \mathbb{Q}(i)^*/(\mathbb{Q}(i)^*)^2$ are conjugate over $\mathbb{Q}$. This can be seen, using Lemma 1, as follows. Taking $F_1(X) = (X^2+p)(X^2+pi)$, $F_2(X) = X^2-pi$, we see from Lemma 1 that there exists a finite set $\mathcal{D}$ such that, for any $(X,Y) \in \mathcal{C}(\mathbb{Q})$, there exist $\delta_2 \in \mathcal{D}, Y_1 \in \mathbb{Q}(i)$ satisfying $Y_1^2 = \delta_2(X^2+p)(X^2+pi)$ (here, δ_2 is the recipricol of the d_i in Lemma 1). Since $X \in \mathbb{Q}$, taking conjugates, from $\mathbb{Q}(i)$ to $\mathbb{Q}$, of both sides gives $Y_2^2 = \delta_1(X^2+p)(X^2-pi)$, where Y_1, Y_2 are conjugate over $\mathbb{Q}$, as are δ_2,δ_1. Multiplying these last two equations gives $Y_0^2 = \delta_1\delta_2(X^4+p^2)$, where $Y_0 = Y_1Y_2/(X^2+p)$.

We can also (using the ideas in Section 2 of [12]) perform the following reduction of the number of δ_1,δ_2 by exploiting an isogeny $\phi : \mathcal{E}^a \times \mathcal{E}^b \to J$, where J is the Jacobian of $\mathcal{C}$, and $\mathcal{E}^a,\mathcal{E}^b$ are the elliptic curves

$Y^2 = (x+p)(x^2+p^2)$, $\underline{Y}^2 = (1+p\underline{x})(1+p^2\underline{x})$, respectively. We can take $\phi = (\phi^a)^* + (\phi^b)^*$, where $\phi^a : \mathcal{C} \to \mathcal{E}^a : (X,Y) \mapsto (X^2, Y)$ and $\phi^b : \mathcal{C} \to \mathcal{E}^b : (X,Y) \mapsto (1/X^2, Y/X^3)$. Further, we may use the injective homomorphism

$$\begin{aligned} \mu \quad &: J(\mathbb{Q})/\phi\big((\mathcal{E}^a \times \mathcal{E}^b)(\mathbb{Q})\big) \to \mathbb{Q}^*/(\mathbb{Q}^*)^2 \times \mathbb{Q}(i)^*/(\mathbb{Q}(i)^*)^2 \times \mathbb{Q}(i)^*/(\mathbb{Q}(i)^*)^2 \\ &: [\textstyle\sum_j n_j (X_j, Y_j)] \mapsto [\textstyle\prod_j (X_j^2+p)^{n_j},\ \prod_j (X_j^2 - pi)^{n_j},\ \prod_j (X_j^2+pi)^{n_j}], \end{aligned} \tag{2}$$

where the left hand [ ] denotes divisor class modulo linear equivalence. We recall Lemma 4 in [12], that im $\mu \subseteq \{[1,1,1],[2,1+i,1-i]\}$. Following [12], we let ∞^+, ∞^- denote the points on the non-singular curve that lie over the singular point at infinity on $\mathcal{C}$, and note that when (X_j, Y_j) is either of ∞^+, ∞^-, then the above expressions $X_j^2+p, X_j^2-pi, X_j^2+pi$ should all be taken to have value 1. Now, let $P = (X,Y) \in \mathcal{C}(\mathbb{Q})$. Then $[P - \infty^+] \in J(\mathbb{Q})$, which is mapped by μ to $[X^2+p, X^2-pi, X^2+pi]$. Our knowledge of im μ then gives that $[X^2+p, X^2-pi, X^2+pi] = [1,1,1]$ or $[2,1+i,1-i]$ in $\mathbb{Q}^*/(\mathbb{Q}^*)^2 \times \mathbb{Q}(i)^*/(\mathbb{Q}(i)^*)^2 \times \mathbb{Q}(i)^*/(\mathbb{Q}(i)^*)^2$. Therefore, $[(X^4+p^2), (X^2+p)(X^2-pi), (X^2+p)(X^2+pi)] = [1,1,1]$ or $[(1+i)(1-i), 2(1+i), 2(1-i)] = [2, 1-i, 1+i]$ in $\mathbb{Q}^*/(\mathbb{Q}^*)^2 \times \mathbb{Q}(i)^*/(\mathbb{Q}(i)^*)^2 \times \mathbb{Q}(i)^*/(\mathbb{Q}(i)^*)^2$. This means that, in (1), we need only consider $[\delta_1\delta_2, \delta_1, \delta_2] = [1,1,1]$ or $[2, 1-i, 1+i]$, which gives us the desired reduction in the number of δ_1, δ_2 which need to be considered (that is, we now have fewer cases to consider than if we had followed only the proof of Lemma 1).

We can resolve the case $[\delta_1\delta_2, \delta_1, \delta_2] = [1,1,1]$, if we can find all $(X, Y_0) \in \mathcal{D}_0(\mathbb{Q})$ or we can find all $(X, Y_j) \in \mathcal{D}_j(\mathbb{Q}(i))$ with $X \in \mathbb{Q}$ (for $j = 1,2$), where

$$\mathcal{D}_0 :\ Y_0^2 = (X^4+p^2),\quad \mathcal{D}_1 :\ Y_1^2 = (X^2+p)(X^2+pi),\quad \mathcal{D}_2 :\ Y_2^2 = (X^2+p)(X^2-pi). \tag{3}$$

We now note that $(X,Y) \mapsto (X^2, XY)$ maps each $\mathcal{D}_i$ to $\mathcal{E}_i$, where:

$$\mathcal{E}_0 :\ y_0^2 = x(x^2+p^2),\quad \mathcal{E}_1 :\ y_1^2 = x(x+p)(x+pi),\quad \mathcal{E}_2 :\ y_2^2 = x(x+p)(x-pi). \tag{4}$$

In order to find all $(x, y_1) \in \mathcal{E}_1(\mathbb{Q}(i))$ with $x \in \mathbb{Q}$, set $y_1 = W + Si$, where $W, S \in \mathbb{Q}$. Taking imaginary and real parts of $(W+Si)^2 = x(x+p)(x+pi)$ gives two equations $2WS = px^2 + xp^2$ and $W^2 - S^2 = x^3 + px^2$. Solving the first of these equations for W, substituting this into the second equation, and letting $t = S^2/(x(x+p))$, gives $4tx = p^2 - 4t^2$, a curve of genus 0 in t, z, which can be parametrised by:

$$t(Z) = (Z+2p)/4,\quad x(Z) = -\frac{Z}{4}\frac{(Z+4p)}{(Z+2p)}. \tag{5}$$

This gives a $\mathbb{Q}$-rational point on the genus 2 curve $S^2 = t(Z)q(x(Z)) = Z(Z+4p)(Z^2-8p^2)/(64(Z+2p))$, and taking $\underline{S} = 8(Z+2p)S$ then gives

$$\mathcal{C}' : \underline{S}^2 = Z(Z+2p)(Z+4p)(Z^2-8p^2). \tag{6}$$

Note that right hand side is the product of $Z^2-8p^2, Z+2p, Z(Z+4p)$, which are linearly dependent, since $(Z^2-8p^2) + 4p(Z+2p) - Z(Z+4p) = 0$; therefore, by Lemma 14.1.1 of [6], the curve $\mathcal{C}'$ is bielliptic. In order to resolve the case $[\delta_1\delta_2, \delta_1, \delta_2] = [1,1,1]$ it is sufficient to find either $\mathcal{E}_0(\mathbb{Q})$ or $\mathcal{C}'(\mathbb{Q})$. Note however (as shown immediately after (21) in [12]) that $\mathcal{E}_0(\mathbb{Q})$ has rank 1, and so $\mathcal{E}_0$ does not allow us to reduce to a finite number of possibilities. Therefore, to deal with this case, it is necessary to compute $\mathcal{C}'(\mathbb{Q})$.

Similarly, in order to resolve the case $[\delta_1\delta_2, \delta_1, \delta_2] = [2, 1-i, 1+i]$, it is sufficient to find all $\mathbb{Q}$-rational points on the elliptic curve $y_0^2 = 2x(x^2+p^2)$ or the genus 2 curve:

$$\underline{S}^2 = Z(Z^2 + 4pZ - 4p^2)(Z^2 - 4pZ - 4p^2). \tag{7}$$

Note again that the right hand side is the product of the linearly dependent $Z, Z^2+4pZ-4p^2, Z^2-4pZ-4p^2$ and so this curve is also bielliptic. Again note that (as shown immediately after (23) in [12]) the elliptic curve $y_0^2 = 2x(x^2+p^2)$ has rank 1, and so, to deal with this case, it is necessary to compute the $\mathbb{Q}$-rational points on the curve (7). In summary, it is sufficient to find all $\mathbb{Q}$-rational points on the genus 2 curves in (6),(7), when we hope to apply following result of Chabauty [7].

Theorem 1. *Let $\mathcal{C}$ be a curve of genus g defined over a number field K, whose Jacobian has Mordell-Weil rank $\leq g-1$. Then $\mathcal{C}$ has only finitely many K-rational points.*

This is a weaker result than Faltings' Theorem [9]; however, when applicable, Chabauty's method can often be used to give good bounds for the number of points on a curve. However (see Lemma 4 of [12]), the original genus 2 curve $\mathcal{C} : Y^2 = (X^2+p)(X^4+p^2)$ (where $p \equiv 7 \bmod 8$ is prime) has Jacobian J, with the rank of $J(\mathbb{Q})$ at least 1, and bounded above by 2, via 2-descent, and we are not able to apply Chabauty's method directly to $\mathcal{C}$. Using the above method, it is alternatively sufficient to find all $\mathbb{Q}$-rational points on the genus 2 curves (6),(7). However, it is also shown (see Lemma 10 of [12], where the above curve (7) is denoted $\mathcal{C}_{2,2}$) that the 2-Selmer bound on the rank of $J(\mathbb{Q})$ is 2 for the curve (7). On the other hand, it is shown in [12] (Theorem 2) that the above method works for $Y^2 = (X^2+2p)(X^2+3p)(X^2+4p)$, where $p \equiv 7 \bmod 8$ is prime.

A feature of the above method is that we have started with a bielliptic genus 2 curve and derived a finite set of new bielliptic genus 2 curves such that finding all $\mathbb{Q}$-rational points on these new curves is sufficient for finding $\mathcal{C}(\mathbb{Q})$. In principle, this method might again be applied to these new genus 2 curves.

The natural more general context, of which the above example is a special case, is when our starting curve is of the form $Y^2 = F_0(X)F_1(X)F_2(X)$, defined over a number field K, where $F_1(X), F_2(X)$ are defined over some $K(\sqrt{d})$ and are conjugate, and $F_0(X)$ is a linear combination of $F_1(X), F_2(X)$. As we shall see, the method which naturally generalises the above example, produces a new set of bielliptic genus 2 curves of this same type, and so there is the potential for the repeated application of the method. It turns out that some finesse will be required with the generalisation of the elliptic curves in (4), as a naive generalisation does not provide an x-coordinate defined over $\mathbb{Q}$. This article has several aims: first, we shall provide explicit formulas for the application of this covering method in our more general context (which should assist others who wish to apply the method); second, we shall show that the resulting genus 2 curves eventually cycle; third, we shall give an example which resists arbitrarily many repeated applications of the method (answering a question raised on p.395 of [12]). As a fringe benefit, we shall also develop some explicit formulas related to maps between genus 2 curves with bielliptic Jacobians, and elliptic curves. See also [3],[4] for some general background and framework.

2. Detailed Description of the Method

We shall consider curves of genus 2, defined over a number field K, of the form

$$\mathcal{C} : Y^2 = F_0(X)F_1(X)F_2(X), \tag{8}$$

where

$$F_1(X) = a_1X^2 + b_1X + c_1,\ F_2(X) = a_2X^2 + b_2X + c_2,\ F_0(X) = k_1F_1(X) + k_2F_2(X), \tag{9}$$

with $a_1, a_2 \neq 0$ and such that $F_0(X)F_1(X)F_2(X)$ has no repeated roots. We suppose moreover that $F_1(X), F_2(X)$ are either both defined over K or are defined over a quadratic extension $K(\sqrt{d})$ of K and are conjugate over K, and that $F_0(X)$ is defined over K and is non-constant (we allow the possibility that $F_0(X)$ is linear). In order to consider these two cases together, we allow $d = 1$ to cover the case where $F_1(X)$ and $F_2(X)$ are defined over K.

Let $\tau(X)$ be the following involution, which swaps the roots of each of $F_1(X)$ and $F_2(X)$ (and therefore $F_0(X)$ since this is a linear combination of $F_1(X)$ and $F_2(X)$), and let M_τ be its associated matrix:

$$\tau(X) = \frac{(a_1c_2 - a_2c_1)X + (b_1c_2 - c_1b_2)}{(a_2b_1 - a_1b_2)X + (a_2c_1 - a_1c_2)},\quad M_\tau = \begin{pmatrix} a_1c_2 - a_2c_1 & b_1c_2 - c_1b_2 \\ a_2b_1 - a_1b_2 & a_2c_1 - a_1c_2 \end{pmatrix}. \tag{10}$$

The eigenvalues of M_τ are $\pm\sqrt{R}$, where R is the resultant of $F_1(X)$ and $F_2(X)$ with respect to X. Provided that $a_1b_2 - b_1a_2 \neq 0$, we can take as corresponding nonzero eigenvectors:

$$[s_1, s_2] = [a_1b_2 - a_2b_1,\ a_1c_2 - a_2c_1 - \sqrt{R}],\quad [t_1, t_2] = [a_1b_2 - a_2b_1,\ a_1c_2 - a_2c_1 + \sqrt{R}],$$

satisfying $[s_1, s_2]M_\tau = \sqrt{R}\,[s_1, s_2]$ and $[t_1, t_2]M_\tau = -\sqrt{R}\,[t_1, t_2]$. When $a_1b_2-b_1a_2 = 0$ and $b_1c_2-c_1b_2 \neq 0$ we can instead take: $[s_1, s_2] = [a_1c_2-c_1a_2+\sqrt{R}, b_1c_2-b_2c_1], [t_1, t_2] = [a_1c_2-c_1a_2-\sqrt{R}, b_1c_2-b_2c_1]$. When both expressions are zero, then we can take $[s_1, s_2] = [1, 0], [t_1, t_2] = [0, 1]$ as our eigenvectors. Since composition of fractional linear transformations gives the same result as matrix multiplication of the corresponding matrices, it follows that $\sigma(X) = (s_1X + s_2)/(t_1X + t_2)$ is negated by replacing X with $\tau(X)$. Note also that $\sigma(X)$ is defined over the quartic number field $K(\sqrt{d}, \sqrt{R})$, but that the combined action $\sqrt{d} \to -\sqrt{d}$, $\sqrt{R} \to -\sqrt{R}$, swaps $F_1(X)$ and $F_2(X)$, negates the numerator and denominator of $\sigma(X)$ and so leaves it unchanged. Therefore $\sigma(X)$ is defined over $K(\sqrt{dR})$. We summarise this in the following lemma.

Lemma 2. *Let $\mathcal{C}$ be as in (8) and τ as in (10), and define R to be the resultant of $F_1(X)$ and $F_2(X)$ with respect to X; as usual, $F_1(X), F_2(X)$ are defined over $K(\sqrt{d})$ and are conjugate over K. The following function $\sigma(X)$ is defined over $K(\sqrt{dR})$ and is negated by τ [that is, $\sigma(\tau(X)) = -\sigma(X)$], so that $\sigma(X)^2$ is invariant under τ.*

Case 1: $a_1b_2 - b_1a_2 \neq 0$,

$$\sigma(X) = \frac{(a_1b_2 - b_1a_2)X + a_1c_2 - a_2c_1 - \sqrt{R}}{(a_1b_2 - b_1a_2)X + a_1c_2 - a_2c_1 + \sqrt{R}}.$$

Case 2: $a_1b_2 - b_1a_2 = 0$ and $b_1c_2 - c_1b_2 \neq 0$,

$$\sigma(X) = \frac{(a_1c_2 - c_1a_2 + \sqrt{R})X + b_1c_2 - b_2c_1}{(a_1c_2 - c_1a_2 - \sqrt{R})X + b_1c_2 - b_2c_1}.$$

Case 3: $a_1b_2 - b_1a_2 = 0$ and $b_1c_2 - c_1b_2 = 0$,

$$\sigma(X) = X.$$

If we replace X by $\sigma^{-1}(T)$ in the equation of $\mathcal{C}$ and multiply both sides by $R(a_1b_2-a_2b_1)^6(T-1)^6$, our curve $\mathcal{C}$ becomes:

$$\left(Y\sqrt{R}(a_1b_2-a_2b_1)^3(T-1)^3\right)^2 = RF_{0x}(T^2)F_{1x}(T^2)F_{2x}(T^2),$$

where

$$\begin{aligned} F_{1x}(x) &= 2a_1R(x+1) + (-2a_1a_2c_1 + 2a_1^2c_2 + a_2b_1^2 - b_1a_1b_2)\sqrt{R}(x-1), \\ F_{2x}(x) &= 2a_2R(x+1) + (-2a_2^2c_1 + 2a_2a_1c_2 - a_1b_2^2 + b_2a_2b_1)\sqrt{R}(x-1), \qquad (11) \\ F_{0x}(x) &= k_1F_{1x}(x) + k_2F_{2x}(x). \end{aligned}$$

Therefore $\phi^a : (X,Y) \mapsto (x,y) = (\sigma(X)^2, Y\sqrt{R}(a_1b_2-a_2b_1)^3(\sigma(X)-1)^3)$ maps $\mathcal{C}$ to the elliptic curve

$$\mathcal{E}^a : y^2 = RF_{0x}(x)F_{1x}(x)F_{2x}(x). \qquad (12)$$

Similarly, $\phi^b : (X,Y) \mapsto (\underline{x},\underline{y}) = (1/\sigma(X)^2, Y\sqrt{R}(a_1b_2-a_2b_1)^3(\sigma(X)-1)^3/\sigma(X)^3)$ maps $\mathcal{C}$ to

$$\mathcal{E}^b : \underline{y}^2 = R\underline{x}^3F_{0x}(1/\underline{x})F_{1x}(1/\underline{x})F_{2x}(1/\underline{x}). \qquad (13)$$

Letting $A = \mathcal{E}^a \times \mathcal{E}^b$, we have $\phi = (\phi^a)^* + (\phi^b)^* : A \to J$, where J is the Jacobian of $\mathcal{C}$. We define $A(K)$ to be the pairs $[P,P']$, where $P \in \mathcal{E}^a(K(\sqrt{dR}))$, $P' \in \mathcal{E}^b(K(\sqrt{dR}))$ are conjugate over K.

The above applies when $a_1b_2 - b_1a_2 \neq 0$. In the case when $a_1b_2 - b_1a_2 = 0$ and $b_1c_2 - c_1b_2 \neq 0$, everything is as above, except that we start with the formula for σ, as in the second case of Lemma 2. In the case when $a_1b_2 - b_1a_2 = 0$ and $b_1c_2 - c_1b_2 = 0$, then $b_1 = b_2 = 0$ (otherwise there would be repeated roots in the right hand side of $\mathcal{C}$, contradicting the fact that $\mathcal{C}$ is of genus 2), and so we already have that $\mathcal{C}$ is of the form $Y^2 = G(X^2) = r_3X^6 + r_2X^4 + r_1X^2 + r_0$; in this case, we have our simplified situation that the maps $(X,Y) \mapsto (x,y) = (X^2,Y)$ and $(X,Y) \mapsto (\underline{x},\underline{y}) = (1/X^2, Y/X^3)$ are, respectively, from $\mathcal{C}$ to $\mathcal{E}^a : r_3X^3 + r_2X^2 + r_1X + r_0$ and $\mathcal{E}^b : r_0X^3 + r_1X^2 + r_2X + r_3$.

We now return to our main motivation: that of finding $\mathcal{C}(K)$, for $\mathcal{C}$ of the form (8). Let S be the set of primes of K at which the reduction of $\mathcal{C}$ is singular, and the primes above 2. Using Lemma 1, as in the discussion immediately after (1), it is sufficient to find all points (with $X, Y_0 \in \mathbb{Q}$ and $Y_1, Y_2 \in \mathbb{Q}(\sqrt{d})$, conjugate over $\mathbb{Q}$) on

$$\mathcal{D}_0 : Y_0^2 = \delta_1\delta_2F_1(X)F_2(X), \quad \mathcal{D}_1 : Y_1^2 = \delta_2F_0(X)F_2(X), \quad \mathcal{D}_2 : Y_2^2 = \delta_1F_0(X)F_1(X). \qquad (14)$$

for finitely many choices of δ_1, δ_2, namely $\delta_1, \delta_2 \in \mathbb{Q}(\sqrt{d})(S,2)$, with δ_1, δ_2 conjugate over $\mathbb{Q}$. In the case where there exists a known $P_0 \in \mathcal{C}(K)$ we could if we wished, as in the discussion immediately before and after (2), reduce the number of δ_1, δ_2 by exploiting an isogeny $\phi : A = \mathcal{E}^a \times \mathcal{E}^b \to J$, and generalising the map of (2); however, we shall not concern ourselves with this refinement.

For the moment, we shall restrict ourselves to the case $\delta_1 = \delta_2 = 1$. Note that later we shall be able to recover the case for general δ_1, δ_2, by replacing, for $j = 1,2$, each a_j, b_j, c_j, k_j by $\delta_ja_j, \delta_jb_j, \delta_jc_j, k_j/\delta_j$, respectively.

Our initial aim is, for $j = 1,2$, to find a 2-to-1 map $(X, Y_j) \mapsto (u, \psi_j)$ from the above genus 1 curves to elliptic curves in the form $\phi_j^2 = $ (quadratic in v over K)$\cdot$(linear in v over $K(\sqrt{d})$). Furthermore, we wish the map $X \mapsto u$ to be defined over K. If we were to imitate the previous section, we would apply $X \to x = \sigma(X)^2$

to map to the x-coordinate of an elliptic curve. However, this map (which was K-rational for the special case when $\sigma(X) = X$) will not be K-rational in general, and so we require a finesse not immediately apparent from the example in the last section.

Lemma 3. *Let $\mathcal{C}$ be as in (8), let $R, \sigma(X)$ as in Lemma 2, and $x = \sigma(X)^2$. Define v by:*

$$v = \sqrt{dR}\frac{x+1}{x-1}, \text{ so that } x = \frac{v+\sqrt{dR}}{v-\sqrt{dR}}.$$

Then $X \to v$ is a K-rational map.

Proof Recall from Lemma 2 that $\sigma(X)$, and hence $x = \sigma(X)^2$, is defined over $K(\sqrt{dR})$. Furthermore, we rewrite the formulas in Lemma 2 (in the typical case – the other cases being similar) as:

$$\sigma(X) = \frac{\sqrt{R}(a_1b_2 - b_1a_2)X + \sqrt{R}(a_1c_2 - a_2c_1) - R}{\sqrt{R}(a_1b_2 - b_1a_2)X + \sqrt{R}(a_1c_2 - a_2c_1) + R}, \tag{15}$$

and note that expressions such as $a_1b_2 - b_1a_2$ are of the form $\sqrt{d}\,k$ for some $k \in K$ (since a_1, a_2 are conjugate, as are b_1, b_2 and c_1, c_2). We see that $\sqrt{dR} \mapsto -\sqrt{dR}$ swaps the numerator and denominator of $\sigma(X)$ and negates them. Hence $\sqrt{dR} \mapsto -\sqrt{dR}$ sends $\sigma(X)$ to $1/\sigma(X)$ and so sends $\sigma(X)^2$ to $1/\sigma(X)^2$; that is, x is sent to $1/x$. Hence $\frac{x+1}{x-1}$ is negated by $\sqrt{dR} \mapsto -\sqrt{dR}$, and so $v = \sqrt{dR}\frac{x+1}{x-1}$ is left invariant, giving that v is defined over K, as required. □

We begin by replacing X with $\sigma^{-1}(T)$ in $F_0(X)$, $F_1(X)$, $F_2(X)$ of (9), and obtain

$$F_{1T}(T) = \frac{2a_1R(T^2+1) + (-2a_1a_2c_1 + 2a_1^2c_2 + a_2b_1^2 - b_1a_1b_2)\sqrt{R}(T^2-1)}{(a_1b_2 - a_2b_1)^2(T-1)^2},$$

$$F_{2T}(T) = \frac{2a_2R(T^2+1) + (-2a_2^2c_1 + 2a_2a_1c_2 - a_1b_2^2 + b_2a_2b_1)\sqrt{R}(T^2-1)}{(a_1b_2 - a_2b_1)^2(T-1)^2}, \tag{16}$$

$$F_{0T}(T) = k_1F_{1T}(T) + k_2F_{2T}(T).$$

Take $\mathcal{D}_1 : Y_1^2 = F_0(X)F_2(X)$, and substitute $X = \sigma^{-1}(T)$ so that the curve becomes $Y_1^2 = F_{0T}(T)F_{2T}(T)$, as above. Multiplying both sides by $\big(2Td(a_1b_2 - a_2b_1)^2/(T+1)^2\big)^2$ puts $\mathcal{D}_1$ in the form

$$y_1^2 = \big(2Td(a_1b_2 - a_2b_1)^2/(T+1)^2\big)^2 F_{0T}(T)F_{2T}(T), \tag{17}$$

where

$$y_1 = \frac{2Td(a_1b_2 - a_2b_1)^2}{(T+1)^2} = \frac{2\sigma(X)d(a_1b_2 - a_2b_1)^2}{(\sigma(X)+1)^2}. \tag{18}$$

The right hand side of (17), after simplifying, has only even powers of T. Replacing T^2 by x and then replacing x by $(v+\sqrt{dR})(v-\sqrt{dR})$, as in (15), we see that (17) becomes:

$$y_1^2 = Q(v)L(v)M(v), \tag{19}$$

where

$$\begin{aligned}
Q(v) &= v^2 - dR,\\
L(v) &= 2(k_1a_1 + k_2a_2)v + (k_1A_1 + k_2A_2)\sqrt{d},\\
M(v) &= 2a_2v + (-2a_2^2c_1 + 2a_1a_2c_2 - a_1b_2^2 + b_2a_2b_1)\sqrt{d},\\
A_1 &= -2a_1a_2c_1 + 2a_1^2c_2 + a_2b_1^2 - b_1a_1b_2,\\
A_2 &= -2a_2^2c_1 + 2a_2a_1c_2 - a_1b_2^2 + b_2a_2b_1.
\end{aligned}$$

The 2-to-1 map $(X, Y_1) \to (v, y_1)$ from $\mathcal{D}_1$ to (19) is given by

$$v = \sqrt{d}R\frac{\sigma(X)^2+1}{\sigma(X)^2-1} \text{ and } y_1 = \frac{2dY_1\sigma(X)(a_1b_2-a_2b_1)^2}{(\sigma(X)+1)^2}.$$

Note that the quadratic $Q(v)$ and the linear $L(v)$ are defined over K, and the linear $M(v)$ is defined over $K(\sqrt{d})$.

In order to put the curve (19) into the form **square = cubic**, we take the root v_0 of $L(v)$, namely:

$$v_0 = -\frac{(k_1A_1+k_2A_2)\sqrt{d}}{2(k_1a_1+k_2a_2)}.$$

and map it to infinity, by changing variable to $u = \frac{1}{v-v_0}$. Substituting the inverse map $v = v_0 + \frac{1}{u}$ into (19) and multiplying both sides by $4(k_1a_1+k_2a_2)^2u^4$ gives

$$\psi_1^2 = 4(k_1a_1+k_2a_2)^2u^4Q\Big(v_0+\frac{1}{u}\Big)L\Big(v_0+\frac{1}{u}\Big)M\Big(v_0+\frac{1}{u}\Big), \tag{20}$$

where

$$\psi_1 = 2y_1(k_1a_1+k_2a_2)u^2, \quad u = \frac{1}{v-v_0}. \tag{21}$$

In detail, (20) gives

$$\mathcal{E}_1 : \psi_1^2 = Q_0(u)L_2(u), \tag{22}$$

where

(23)
$$\begin{aligned}
Q_0(u) = \;& d(a_1b_2-a_2b_1)^2(k_2^2b_2^2+2k_1b_1k_2b_2-4a_1c_1k_1^2-4a_1k_1c_2k_2-4k_2^2a_2c_2+k_1^2b_1^2-4c_1k_1k_2a_2)u^2 \\
& +4\sqrt{d}(k_1a_1+k_2a_2)(2k_1a_1a_2c_1-2k_1a_1^2c_2-k_1a_2b_1^2+k_1b_1a_1b_2-k_2b_2a_2b_1 \\
& \qquad -2k_2a_2a_1c_2+k_2a_1b_2^2+2c_1k_2a_2^2)u+4(k_1a_1+k_2a_2)^2, \\
L_2(u) = \;& -2\sqrt{d}k_1(a_1b_2-a_2b_1)^2u+4a_2(k_1a_1+k_2a_2).
\end{aligned}$$

The map $(X, Y_1) \mapsto (u, \psi_1)$ is a 2-to-1 map from the genus 1 curve $\mathcal{D}_1$ to the elliptic curve $\mathcal{E}_1$, and the map $X \mapsto u$ is defined over K. Similarly, the curve $\mathcal{D}_2$ (which is the conjugate of $\mathcal{D}_1$) maps to $\mathcal{E}_2$, the conjugate of $\mathcal{E}_1$. Recall that we want to determine all $(X, Y_1) \in \mathcal{D}_1(K(\sqrt{d}))$ such that $X \in K$. It is sufficient to find all $(u, \psi_1) \in \mathcal{E}_1(K(\sqrt{d}))$ such that $u \in K$. The problem of finding all $(u, \psi_2) \in \mathcal{E}_2(K(\sqrt{d}))$ such that $u \in K$, is equivalent, since $\mathcal{E}_1$ and $\mathcal{E}_2$ are conjugate, and so we can just focus on $\mathcal{E}_1$.

So far, we have taken d to be such that $\mathcal{F}_1, F_2$ are defined over $K(\sqrt{d})$ without specifying the representative in $K^*/(K^*)^2$. We now fix $\sqrt{d}$ to be $k_1 - k_2$ so that $d = (k_1-k_2)^2$. Then (23) can be expressed as:

$$Q_0(u) = au^2+bu+c, \quad L_2(u) = n_1(u)+n_2(u)\sqrt{d}, \text{ where } n_1(u) = i_1u+i_2, \quad n_2(u) = j_1u+j_2, \tag{24}$$

where $a, b, c, i_1, i_2, j_1, j_2 \in K$ and $\sqrt{d}$ are given by:

(25)
$$\begin{aligned}
a = \;& (k_1-k_2)^2(a_1b_2-a_2b_1)^2 \\
& (k_2^2b_2^2+2k_1b_1k_2b_2-4a_1c_1k_1^2-4a_1k_1c_2k_2-4k_2^2a_2c_2+k_1^2b_1^2-4c_1k_1k_2a_2), \\
b = \;& 4(k_1-k_2)(k_1a_1+k_2a_2) \\
& (2k_1a_1a_2c_1-2k_1a_1^2c_2-k_1a_2b_1^2+k_1b_1a_1b_2-k_2b_2a_2b_1-2k_2a_2a_1c_2+k_2a_1b_2^2+2c_1k_2a_2^2), \\
c = \;& 4(k_1a_1+k_2a_2)^2, \; i_1 = -(k_1-k_2)^2(a_1b_2-a_2b_1)^2, \; i_2 = 2(a_1+a_2)(k_1a_1+k_2a_2), \\
j_1 = \;& -(k_1+k_2)(a_1b_2-a_2b_1)^2, \; j_2 = 2(-a_1+a_2)(k_1a_1+k_2a_2)/(k_1-k_2), \; \sqrt{d} = k_1-k_2.
\end{aligned}$$

We shall now find a new bielliptic genus 2 curve, defined over K, with the property that any such (u, ψ_1) gives rise to a K-rational point on the genus 2 curve. This genus 2 curve will turn out to have a 2-to-1 map to the elliptic curve $\mathcal{E}_1$, with the map to u being K-rational. Let $\psi_1 = W + S\sqrt{d}$, with $W, S \in K$, so that (22) becomes $(W+S\sqrt{d})^2 = Q_0(u)(n_1(u)+n_2(u)\sqrt{d})$. Equating the coefficient of $\sqrt{d}$ and the K-rational part, gives two equations in W, S.

$$2WS = Q_0(u)n_2(u), \quad W^2 + dS^2 = Q_0(u)n_1(u). \tag{26}$$

We can use the first equation to eliminate, say, W, using $W = Q_0(u)n_2(u)/(2S)$ and substitute this into the second equation, to give

$$\frac{Q_0(u)^2 n_2(u)^2}{4S^2} + dS^2 - Q_0(u)n_1(u) = 0. \tag{27}$$

Letting $t = S^2/Q_0(u)$, we see that t, u satisfy

$$n_2(u)^2 + 4dt^2 - 4tn_1(u) = 0. \tag{28}$$

This describes a genus 0 curve in t, u which can be parametrised, using the parameter $Z = t/(j_1 u + j_2)$, as

$$u(Z) = \frac{-4dj_2Z^2 + 4i_2Z - j_2}{4j_1dZ^2 - 4i_1Z + j_1}, \quad t(Z) = \frac{4Z^2(i_2j_1 - i_1j_2)}{4dj_1Z^2 - 4i_1Z + j_1}, \tag{29}$$

provided that $j_1 \neq 0$. In the special case when $j_1 = 0$, we can instead take $Z = t$ as our parameter, giving the parametrisation $u(Z) = (4dZ^2 - 4i_2Z + j_2^2)/(4i_1Z)$ and $t(Z) = Z$.

In either case, since $t = S^2/Q_0(u)$, we see that there exists $Z \in K$ such that $S^2 = t(Z)Q_0(u(Z))$, giving a genus 2 curve in Z, S, which is defined over K. Furthermore, the above shows that any $K(\sqrt{d})$-rational point on (22) with $u \in K$, gives rise to a K-rational point on the genus 2 curve $S^2 = t(Z)Q_0(u(Z))$. Also note that if (Z, S) is a K-rational point on the genus 2 curve $S^2 = t(Z)Q_0(u(Z))$, then $(Z, S) \mapsto \big(u(Z), Q_0(u(Z))n_2(u(Z))/(2S) + S\sqrt{d}\big)$ gives a map to a point (u, ψ) on (22) [using the facts that $W = Q_0(u)n_2(u)/(2S)$ and $\psi = W + S\sqrt{d}$], so that $S^2 = t(Z)Q_0(u(Z))$ is bielliptic. This produces the new bielliptic genus 2 curve, and completes one cycle of the process.

Letting $\underline{S} = Sa(4j_1Z^2d - 4Zi_1 + j_1)^2/Z$ our genus 2 curve $S^2 = t(Z)Q_0(u(Z))$ becomes (for the typical case when $j_1 \neq 0$):

$$\underline{S}^2 = G_0(Z)G_1(Z)G_2(Z), \tag{30}$$

where

$$\begin{aligned} G_1(Z) &= 4bj_1dZ^2 - 8adj_2Z^2 + 8ai_2Z - 4bi_1Z - 2aj_2 + bj_1 + (4j_1dZ^2 - 4i_1Z + j_1)\sqrt{b^2-4ac}, \\ G_2(Z) &= 4bj_1dZ^2 - 8adj_2Z^2 + 8ai_2Z - 4bi_1Z - 2aj_2 + bj_1 - (4j_1dZ^2 - 4i_1Z + j_1)\sqrt{b^2-4ac}, \\ G_0(Z) &= a(i_2j_1 - i_1j_2)(4j_1dZ^2 - 4i_1Z + j_1). \end{aligned} \tag{31}$$

Note also that

$$G_0(Z) = \frac{a(i_2j_1 - i_1j_2)}{2\sqrt{b^2-4ac}}(G_1(Z) - G_2(Z)),$$

so that our new genus 2 curve has the same properties as our starting genus 2 curve: it is of the form $\underline{S}^2 = G_0(Z)G_1(Z)G_2(Z)$, where G_0, G_1, G_2 satisfy the conditions of (9). Note that the field of definition of G_1, G_2 is now $K(\sqrt{b^2-4ac})$, rather than $K(\sqrt{d})$. If we now substitute (25) into (31), let $\underline{X} = Z$ and let $\underline{Y}$ denote

$$\frac{\underline{S}R(b_1^2 - 4a_1c_2 + b_2^2 - 4a_2c_2 - 2b_1b_2 + 4a_1c_2 + 4a_2c_1)}{8\big(k_1^2(b_1^2 - 4a_1c_1) + k_2^2(b_2^2 - 4a_2c_2) + 2k_1k_2(b_1b_2 - 2a_1c_2 - 2a_2c_1)\big)(k_1-k_2)^2(a_2b_1 - a_1b_2)^4(k_1a_1 + k_2a_2)^3},$$

then our genus 2 curve (30) becomes:

$$\mathcal{C}' : \underline{Y}^2 = G_0(\underline{X})G_1(\underline{X})G_2(\underline{X}), \tag{32}$$

where

$$G_1(\underline{X}) = a_1'\underline{X}^2 + b_1'\underline{X} + c_1',\ G_2(\underline{X}) = a_2'\underline{X}^2 + b_2'\underline{X} + c_2',\ G_0(\underline{X}) = k_1'G_1(\underline{X}) + k_2'G_2(\underline{X}), \tag{33}$$

and where

(34)

$$\begin{aligned}
a_1' = &\ \ a_2' = 4(k_1-k_2)^2(b_1^2 - 2b_2b_1 + 4a_1c_2 + 4a_2c_1 - 4c_2a_2 + b_2^2 - 4c_1a_1),\\
b_1' = &\ \ 4(k_1-k_2)(b_1^2 - 4c_1a_1 + 4c_2a_2 - b_2^2 + 4\sqrt{R}),\ b_2' = 4(k_1-k_2)(b_1^2 - 4c_1a_1 + 4c_2a_2 - b_2^2 - 4\sqrt{R}),\\
c_1' = &\ \ c_2' = b_1^2 - 2b_2b_1 + 4a_1c_2 + 4a_2c_1 - 4c_2a_2 + b_2^2 - 4c_1a_1,\\
k_1' = &\ \ \tfrac{1}{2}(k_1+k_2)(a_2b_1 - a_1b_2)^2R^2 - \tfrac{1}{4}R(a_2b_1 - a_1b_2)^2\sqrt{R}(-4a_1k_1c_1 + 2a_1k_1c_2 - 2a_1k_2c_2 + 2a_2k_1c_1\\
&\qquad -2a_2k_2c_1 + b_1^2k_1 - b_1k_1b_2 + b_1b_2k_2 + 4a_2k_2c_2 - b_2^2k_2),\\
k_2' = &\ \ \tfrac{1}{2}(k_1+k_2)(a_2b_1 - a_1b_2)^2R^2 + \tfrac{1}{4}R(a_2b_1 - a_1b_2)^2\sqrt{R}(-4a_1k_1c_1 + 2a_1k_1c_2 - 2a_1k_2c_2 + 2a_2k_1c_1\\
&\qquad -2a_2k_2c_1 + b_1^2k_1 - b_1k_1b_2 + b_1b_2k_2 + 4a_2k_2c_2 - b_2^2k_2).
\end{aligned}$$

The above applies to the case $\delta_1 = \delta_2 = 1$; note that our new G_1, G_2 are each defined over $K(\sqrt{dR})$ rather than $K(\sqrt{d})$. We can recover the equation for general δ_1, δ_2 in the manner described after (14). We are now in a position to describe the method explicitly.

Method 1. Let $\mathcal{C}$ be as in (8). In order to find $\mathcal{C}(K)$ it is sufficient, for each $\delta \in K(\sqrt{d})(S, 2)$, either to find all K rational points on the genus 1 curve $\mathcal{D}_0$ in (14) or all K-rational points on the genus 2 curve obtained from $\mathcal{C}'$ in (32),(33),(34) by replacing, for $j = 1, 2$, each a_j, b_j, c_j, k_j by $\delta_j a_j, \delta_j b_j, \delta_j c_j, k_j/\delta_j$, respectively. We attempt the second of these by hoping that the rank of Mordell-Weil group (over K) of the Jacobian is at most 1, and applying Chabauty techniques, such as those in [10]. We initially attempt to compute the rank via 2-descent; there are also refinements which have recently been developed (for example, see [5]) which attempt to find the rank even when there are members of the Shafarevich-Tate group.

We have now obtained a finite set of new genus 2 curves, all defined over K, with the property that if we can find all of their K-rational points then we can do the same for $\mathcal{C}$. Furthermore, since all of these new genus 2 curves are of the same type as $\mathcal{C}$, there is the potential for the method to be repeatedly applied.

3. Proof of Cycling

We shall focus on the case $\delta_1 = \delta_2 = 1$ and show that repeated applications of this case lead to cycling. For simplicity, we replace $\underline{X}, \underline{Y}$ by X, Y, respectively, so that $\mathcal{C}' : Y^2 = G_0(X)G_1(X)G_2(X)$, where G_0, G_1, G_2 are as in (33),(34), which describe the coefficients of $\mathcal{C}'$ in terms of the coefficients of our original curve $\mathcal{C}$ in (8). We can find the result of a second application, simply by a recursive substitution of (34), where each a_j, b_j, c_j, k_j in the right hand side is replaced by a_j', b_j', c_j', k_j', respectively, and with the same substitution performed on the expression for R, the resultant of $F_1(X)$ and $F_2(X)$. After performing this substituting, and then a minor adjustment to the variables X, Y (multiplying each by a constant) gives the following nice form for the result of two applications.

$$\mathcal{C}'' : Y^2 = H_0(X)H_1(X)H_2(X), \tag{35}$$

where

$$\begin{aligned}
H_1(X) &= X^2 + (-b_1^2 + b_2b_1 - 2a_1c_2 - 2a_2c_1 + 4c_1a_1)X + R,\\
H_2(X) &= X^2 + (-4c_2a_2 - b_2b_1 + b_2^2 + 2a_1c_2 + 2a_2c_1)X + R,\\
H_0(X) &= k_1''H_1(X) + k_2''H_2(X),\ \text{with}\ k_j'' = R(a_2b_1 - a_1b_2)^2k_j,\ \text{for}\ j = 1, 2.
\end{aligned} \tag{36}$$

If we again substitute recursively to repeat the process from $\mathcal{C}$ to $\mathcal{C}''$, again followed by a minor adjustment to the variables X, Y (multiplying each by a constant) gives the following for the result of four applications.

$$\mathcal{C}''''' : Y^2 = RH_0(X)H_1(X)H_2(X), \tag{37}$$

which is a quadratic twist of $\mathcal{C}''$. This twist is removed after two further applications, giving the following result.

Theorem 2. *Let $\mathcal{C}$ be as in (8) and $\mathcal{C}'$ be as in (32). On repeated application, the process eventually cycles; in particular $\mathcal{C}''''''$ is the same curve, up to a K-rational linear change in variable, as $\mathcal{C}''$.*

Of course, we should really regard each curve $Y^2 = F(X)$ as a member of the family of twists $Y^2 = \delta F(X)$ for $\delta \in K(S, 2)$. From this point of view, the family containing $\mathcal{C}''''$ is the same as that containing $\mathcal{C}''$, and so we have cycles of length 2 (rather than 4) on these families of curves.

Since the case $\delta_1 = \delta_2 = 1$ must always be included in any attempt to apply Method 1, any curve $\mathcal{C}$ for which Chabauty's Theorem is repeatedly not applicable (and for which the genus 1 curves $\mathcal{D}_0$ have infinitely many K-rational points), and if this continues until cycling occurs, then such a curve will defy the method entirely, however many times it is repeated. In the following example, we shall include two interesting cases which defy repeated applications of the method: in one case, the version of the method with 2-Selmer bounds, and in the other case, the version which uses the actual ranks.

Example 1. Let $\mathcal{C} : Y^2 = (X^2 + n)(X^4 + n^2)$ be as in Section 1, but where $n \in \mathbb{Z}\backslash\{0\}$ need not be prime. Then repeatedly applying the process of the last section gives the following genus 2 curves $\mathcal{C}', \mathcal{C}'', \mathcal{C}''', \mathcal{C}'''' = \mathcal{C}$; the corresponding genus 1 curve $\mathcal{D}_0$ at each stage is on each line.

$$\begin{array}{rrrl}
\mathcal{C}': & Y^2 = X(X+2n)(X+4n)(X^2-8n^2), & \mathcal{D}'_0: & Y_0^2 = X^4 + n^2, \\
\mathcal{C}'': & Y^2 = (X^2-n)(X^4+n^2), & \mathcal{D}''_0: & Y_0^2 = X(X+2n)(X+4n), \\
\mathcal{C}''': & Y^2 = X(X-2n)(X-4n)(X^2-8n^2), & \mathcal{D}'''_0: & Y_0^2 = X^4 + n^2, \\
\mathcal{C}'''': & Y^2 = (X^2+n)(X^4+n^2), & \mathcal{D}''''_0: & Y_0^2 = X(X-2n)(X-4n).
\end{array}$$

For $n = 31$, it can be checked in Magma [15] that each of the genus 1 curves is an elliptic curve of rank 1 and the 2-Selmer bound on the Jacobian of each genus 2 curve is at least 2, and so $\mathcal{C}$ defies arbitrarily many repeated applications of Method 1, although note that a second descent shows that $J'(\mathbb{Q})$ has rank 0, where J' is the Jacobian of $\mathcal{C}'$, giving a member of the Shafarevich-Tate group. A stronger example is the case $n = 2415$, when each of the genus 1 curves is an elliptic curve of rank at least 1, and the rank is at least 2 for the Jacobian of each genus 2 curve. Therefore $\mathcal{C}$ defies the stronger version of Method 1. In each case, the generators are small and easy to find; the only exception is for J', the Jacobian of $\mathcal{C}'$, when one first uses the fact that $J'(\mathbb{Q})$ has the same rank as that of $\mathcal{E}'(\mathbb{Q}(i))$ for $\mathcal{E}' : y^2 = 2415x(x+1)(x+i)$, which has the obvious $\mathbb{Q}(i)$-rational point $\left(-\frac{35}{12}, \frac{805}{24} + \frac{805}{4}i\right)$. Another independent point: $\left(-\frac{105}{92} - \frac{20}{69}i, -\frac{3815}{276} + \frac{17815}{552}i\right)$ was found using programs made available by Denis Simon in [14].

It should also be noted that, in principle, these techniques can be applied to any starting genus 2 curve $\mathcal{C} : Y^2 = F(X)$, even if not bielliptic, and indeed any hyperelliptic curve of genus at least 2. After extending the ground field K, if necessary, there will factors $F_0(X), F_1(X), F_2(X)$ of $F(X)$ such that $F_1(X)$ and $F_2(X)$ are defined over some $K(\sqrt{d})$ and are conjugate, and such that $F_0(X)$ is defined over K. We only lack the condition that $F_0(X)$ is a linear combination of $F_0(X), F_1(X)$. Nevertheless, we can still apply resultants, as usual, to say that any $(X,Y) \in \mathcal{C}(K)$ must satisfy $\mathcal{D}_1 : Y_1^2 = \delta_2 F_0(X) F_2(X)$ for some $Y_1 \in K(\sqrt{d})$ and some $\delta \in K(\sqrt{d})(S,2)$. One can then apply the method in the last section to obtain the corresponding genus 2 curves, which will now be bielliptic; applying Method 1 repeatedly will then give cycling, as before.

The authors thank Nils Bruin, Tim Dokchitser and Tom Fisher for helpful discussions.

References

[1] F. Bogomolov and Y. Tschinkel. Couniformisation of curves over number fields. *Geometric methods in algebra and number theory,* 43–57, Prog. Math. **235**. Birkhäuser, Boston.

[2] N. Bruin. *Chabauty methods and covering techniques applied to generalised Fermat equations*, Ph.D. thesis, Universiteit Leiden, 1999.

[3] N. Bruin. The arithmetic of Prym varieties in genus 3. Manuscript, 2004, available at: arxiv.org/abs/math.NT/0408069

[4] N. Bruin and E.V. Flynn. Towers of 2-Covers of hyperelliptic curves. *Trans. Amer. Math. Soc.* **357** (2005), 4329–4347.

[5] N. Bruin and E.V. Flynn. Exhibiting SHA[2] on hyperelliptic Jacobians. *J. Number Theory.*, 118:266–291, 2006.

[6] J.W.S. Cassels and E.V. Flynn. *Prolegomena to a middlebrow arithmetic of curves of genus 2.* London Mathematical Society Lecture Note Series **230** (1996), Cambridge University Press.

[7] C. Chabauty. Sur les points rationnels des courbes algébriques de genre supérieur à l'unité. *C.R. Acad. Sci. Paris* **212** (1941), 882–885.

[8] C. Chevalley and A. Weil. Un theorème d'arithmetique sur les courbes algebriques. *C.R. Acad. Sci. Paris* **195** (1930), 570–572.

[9] G. Faltings. *Rational Points.* Friedrich Vieweg & Sons, 1992.

[10] E.V. Flynn. A flexible method for applying Chabauty's theorem. *Compositio Mathematica* **105** (1997), 79–94.

[11] E.V. Flynn. Coverings of Curves of Genus 2. Algorithmic Number Theory, Wieb Bosma, ed. *Lecture Notes in Computer Science* **1838** (2000), 65–84. Springer-Verlag.

[12] E.V. Flynn and J. Redmond. Application of covering techniques to families of curves. *J. Number Theory* **101** (2003), 376–397.

[13] J.H. Silverman. *The arithmetic of elliptic curves.* Graduate Texts in Mathematics **106** (1986). Springer-Verlag.

[14] D. Simon. Computing the rank of elliptic curves over number fields. *London Math. Soc. J. Comput. Math.* **5** (2002), 7–17. Programs available at: www.math.unicaen.fr/~simon/ell.gp

[15] *The Magma computational algebra system*, produced and distributed by the Computational Algebra Group within the School of Mathematics and Statistics of the University of Sydney, available at: http://magma.maths.usyd.edu.au/magma/

Mathematical Institute, University of Oxford, 24–29 St. Giles, Oxford OX1 3LB, UNITED KINGDOM
E-mail address: flynn@maths.ox.ac.uk

Department of Mathematics, Bancroft's School, High Road, Woodford Green, Essex IG8 0RF, UNITED KINGDOM
E-mail address: john.wunderle@bancrofts.essex.sch.uk