Some improvements to 4-descent on an elliptic curve

Tom Fisher

University of Cambridge, DPMMS, Centre for Mathematical Sciences
Wilberforce Road, Cambridge CB3 0WB, UK
T.A.Fisher@dpmms.cam.ac.uk
http://www.dpmms.cam.ac.uk/~taf1000

Abstract. The theory of 4-descent on elliptic curves has been developed in the PhD theses of Siksek [18], Womack [21] and Stamminger [20]. Prompted by our use of 4-descent in the search for generators of large height on elliptic curves of rank at least 2, we explain how to cut down the number of class group and unit group calculations required, by using the group law on the 4-Selmer group.

1 Introduction

Let E be an elliptic curve over a number field K. A 2-descent (see e.g. [2], [4], [19]) furnishes us with a list of quartics $g(X) \in K[X]$ representing the everywhere locally soluble 2-coverings of E, and hence the elements of the 2-Selmer group $S^{(2)}(E/K)$. If we are unable to resolve the existence of K-rational points on the curves $Y^2 = g(X)$, then it may be necessary to perform a 4-descent. Cassels [3] has constructed a pairing on $S^{(2)}(E/K)$ whose kernel is the image of $[2]_*$ in the exact sequence

$$E[2](K) \longrightarrow S^{(2)}(E/K) \xrightarrow{\iota_*} S^{(4)}(E/K) \xrightarrow{[2]_*} S^{(2)}(E/K) \ . \tag{1}$$

We have checked [11] that this pairing agrees with the usual Cassels-Tate pairing on $Ш(E/K)[2]$. An improved method for computing the pairing has recently been found by Steve Donnelly [7].

Computing this pairing is sufficient to determine the structure of $S^{(4)}(E/K)$ as an abelian group, but if our aim is to find generators of $E(K)$ of large height, then we also need to find equations for the 4-coverings parametrised by this group. For this we use the theory of 4-descent, as developed in [14], [21] and [20]. Each quartic $g(X)$ has an associated flex algebra[1] $F = K[X]/(g(X))$, which is usually a degree 4 field extension of K. The existing methods of 4-descent (as implemented in Magma [13] by Tom Womack, and improved by Mark Watkins) require us to compute the class group and units for the flex field of every quartic in the image of $[2]_*$. In this article we explain how to cut down the number of class

[1] We keep the terminology of [6, Paper 1]. Were we to use a term specific to 2-descent then "ramification algebra" would seem more appropriate.

group and unit group calculations, by using the group law on $S^{(4)}(E/K)$. This is a non-trivial task since by properties of the obstruction map [6], [15], we expect to have to solve an explicit form of the local-to-global principle for the Brauer group $\mathrm{Br}(K)$. We also give a test for equivalence of 4-coverings (generalising the tests for 2-coverings and 3-coverings given in [4], [5] and [8]).

Even when the calculation of class groups and unit groups does finish, the output may be unmanageably large. We get round this by using a method described in §2, to find good representatives for elements of $K^\times/(K^\times)^n$. This technique is not specific to descent calculations on elliptic curves.

2 Selmer groups of number fields

Let K be a number field of degree $[K:\mathbb{Q}] = d$ and let S be a finite set of primes of K. The n-Selmer group

$$K(S,n) = \{x(K^\times)^n \in K^\times/(K^\times)^n : \mathrm{ord}_{\mathfrak{p}}(x) \equiv 0 \pmod{n} \text{ for all } \mathfrak{p} \notin S\}$$

plays an important role in the construction of number fields via Kummer theory, and in the theory of descent on elliptic curves.

The height of an algebraic integer x in K is $H(x) = \prod_{i=1}^d \max(|\sigma_i(x)|, 1)$ where $\sigma_1, \ldots, \sigma_d$ are the distinct embeddings of K into $\mathbb{C}$. We write r_1 (resp. r_2) for the number of real (resp. complex) places, and Δ_K for the absolute discriminant. The Minkowski bound is

$$m_K = \left(\frac{4}{\pi}\right)^{r_2} \frac{d!}{d^d}\sqrt{|\Delta_K|} \ .$$

Theorem 2.1. *Let $n \geq 1$ be an integer. Let $\alpha \in K^\times$ with $(\alpha) = \mathfrak{b}\mathfrak{c}^n$ and $\mathfrak{b}$ an integral ideal. Then there exists $\beta \in \mathfrak{b}$ with $\alpha\beta^{-1} \in (K^\times)^n$ and*

$$H(\beta) \leq \max(m_K^n N\mathfrak{b}, \exp(nd)) \ .$$

The proof uses two lemmas.

Lemma 2.2. *If $a_1, \ldots, a_d$ are positive real numbers with $\sum_{i=1}^d a_i \leq dc^{1/d}$ then*

$$\prod_{i=1}^d \max(a_i, 1) \leq \max(c, \exp(d)) \ .$$

Proof. We may assume that $a_i \geq 1$ for $1 \leq i \leq r$ and $a_i < 1$ for $r+1 \leq i \leq d$. By the inequality of the arithmetic and geometric means we obtain

$$\prod_{i=1}^d \max(a_i, 1) = \prod_{i=1}^r a_i \leq f(r/d)$$

where $f(x) = x^{-dx}c^x$. If $\log(c) \geq d$ then $f'(x) \geq 0$ for all $0 < x \leq 1$. Thus $f(r/d) \leq f(1) = c$. On the other hand if $\log(c) \leq d$ we obtain

$$\log f(x) \leq dx(1 - \log x) \leq d \ .$$

□

We extend the embeddings $\sigma_i : K \to \mathbb{C}$ to maps defined on $K \otimes_{\mathbb{Q}} \mathbb{R}$.

Lemma 2.3. *Let Λ be a lattice in $K \otimes_{\mathbb{Q}} \mathbb{R}$ of covolume V. Then there exists non-zero $\xi \in \Lambda$ with*

$$\sum_{i=1}^{d} |\sigma_i(\xi)| \leq \left(\left(\frac{4}{\pi} \right)^{r_2} d!\, V \right)^{1/d} .$$

Proof. This is a standard application of Minkowski's convex body theorem. □

The usual application of Lemma 2.3 is to show that every fractional ideal $\mathfrak{b}$ in K contains an element β with $|N_{K/\mathbb{Q}}(\beta)| \leq m_K N\mathfrak{b}$.

Proof of Theorem 2.1. Let $|\cdot|$ be the map on $K \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{R}^{r_1} \oplus \mathbb{C}^{r_2}$ given componentwise by $x \mapsto |x|$. We apply Lemma 2.3 to the lattice $\Lambda = |\alpha|^{1/n}\mathfrak{c}^{-1}$ and let $\beta = \frac{\alpha}{|\alpha|}\xi^n$. The covolume of Λ is

$$|N_{K/\mathbb{Q}}(\alpha)|^{1/n}(N\mathfrak{c})^{-1}\sqrt{|\Delta_K|} = (N\mathfrak{b})^{1/n}\sqrt{|\Delta_K|} .$$

Thus β satisfies

$$\sum_{i=1}^{d} |\sigma_i(\beta)|^{1/n} \leq d \left(m_K (N\mathfrak{b})^{1/n} \right)^{1/d} .$$

Since $\beta \in \mathfrak{b}$ is an algebraic integer, we deduce by Lemma 2.2 that

$$H(\beta)^{1/n} \leq \max(m_K (N\mathfrak{b})^{1/n}, \exp(d))$$

as required. □

Theorem 2.1 shows that every element of $K(S,n)$ is represented by an element of K of height at most

$$\max\left(m_K^n \Big(\prod_{\mathfrak{p} \in S} N\mathfrak{p} \Big)^{n-1}, \exp(nd) \right) . \tag{2}$$

Since there are only finitely many elements of K of height less than a given bound, this gives a new proof that $K(S,n)$ is finite. More importantly for us, replacing Minkowski's convex body theorem by the LLL algorithm, we obtain an algorithm for computing small representatives of Selmer group elements from large ones. This is particularly useful when using Magma's function `pSelmerGroup` (so $n = p$ a prime here) which returns a list of "small" elements of $K^\times$, and a list of exponents to which they must be multiplied to give generators for $K(S,p)$. In many examples of interest to us, multiplying out directly in $K^\times$ gives elements of unfeasibly large height. Using our algorithm (after every few multiplications) eliminates this problem. Moreover, the process can be arranged so that the only factorisations required are of the original list of "small" elements.

In principle one could also compute $K(S,n)$ by searching up to the bound (2), but of course this would be absurdly slow in practice.

3 Background on quadric intersections

Let $\mathcal{QI}(K)$ be the space of "quadric intersections" i.e. pairs of homogeneous polynomials of degree 2 in $K[x_1, x_2, x_3, x_4]$. Given $(A, B) \in \mathcal{QI}(K)$ we identify A and B with their matrices of second partial derivatives, and compute

$$g(X) = \det(AX + B) = aX^4 + bX^3 + cX^2 + dX + e \ .$$

The invariants of the quartic $g(X)$ are $I = 12ae - 3bd + c^2$ and $J = 72ace - 27ad^2 - 27b^2e + 9bcd - 2c^3$, and the invariants of (A, B) are $c_4 = I$ and $c_6 = \frac{1}{2}J$. It is well known (see [1]) that if $\Delta = (c_4^3 - c_6^2)/1728$ is non-zero then the curves $C_2 = \{Y^2 = g(X)\}$ and $C_4 = \{A = B = 0\} \subset \mathbb{P}^3$ are smooth curves of genus one with Jacobian

$$E: \quad y^2 = x^3 - 27c_4x - 54c_6 \ . \tag{3}$$

Moreover C_4 is a 2-covering of C_2 (see [1], [14]) the composite $C_4 \to C_2 \xrightarrow{X} \mathbb{P}^1$ being given by $-T_1/T_2$ where T_1 and T_2 are the quadrics determined by

$$\mathrm{adj}((\mathrm{adj}A)X + (\mathrm{adj}B)) = a^2AX^3 + aT_1X^2 + eT_2X + e^2B.$$

Following [5], we say that quartics $g_1, g_2 \in K[X]$ are K-equivalent if their homogenisations satisfy $g_1 = \mu^2 g_2 \circ M$ for some $\mu \in K^\times$ and $M \in \mathrm{GL}_2(K)$. Quadric intersections $(A, B), (A', B') \in \mathcal{QI}(K)$ are K-equivalent if

$$(A', B') = (m_{11}A \circ N + m_{12}B \circ N, m_{21}A \circ N + m_{22}B \circ N)$$

for some $(M, N) \in \mathcal{G}_4(K) := \mathrm{GL}_2(K) \times \mathrm{GL}_4(K)$. It is routine to check that the quartics associated to equivalent quadric intersections are themselves equivalent.

In the course of a 4-descent, a 2-covering C_4 of C_2 is computed as follows. Let C_2 have equation $Y^2 = g(X)$ and flex algebra $F = K[\theta] = K[X]/(g(X))$. Suppose we are given $\xi \in F^\times$ with $N_{F/K}(\xi) \equiv a \mod (K^\times)^2$ where a is the leading coefficient of g. (The existence of such a ξ is clearly necessary for the existence of K-rational points on C_2.) We consider the equation

$$X - \theta = \xi(x_1 + x_2\theta + x_3\theta^2 + x_4\theta^3)^2 \ .$$

A quadric intersection, defining a 2-covering C_4 of C_2, is obtained by expanding in powers of θ and taking the coefficients of θ^2 and θ^3. The answer only depends (up to K-equivalence) on the class of ξ in $F^\times/K^\times(F^\times)^2$. Using the method of §2 to find a good representative for this class, can significantly decrease the time subsequently taken to find a good choice of co-ordinates on $\mathbb{P}^3$, that is, to minimise and reduce the quadric intersection (using the algorithms in [21]).

4 Galois cohomology

We keep the notation and conventions of [6, Paper I]. Let $\pi : C \to E$ be the 2-covering corresponding to $\xi \in H^1(K, E[2])$. The flex algebra of ξ is $F =$

$\mathrm{Map}_K(\Phi, \overline{K})$ where Φ is the fibre of π above 0_E. We note that C is a torsor under E, and Φ is a torsor under $E[2]$. Let $\langle\xi\rangle$ be the subgroup of $H^1(K, E[2])$ generated by ξ, and let $\cup$ be the map $H^1(K, E[2]) \times H^1(K, E[2]) \to \mathrm{Br}(K)[2]$ induced by cup product and the Weil pairing $e_2 : E[2] \times E[2] \to \mu_2$. The following theorem is a variant of a standard result (see for example [17], [20]).

Theorem 4.1. *There is a canonical isomorphism*

$$\ker\left(\frac{H^1(K, E[2])}{\langle\xi\rangle} \xrightarrow{\cup\xi} \mathrm{Br}(K)\right) \cong \ker\left(F^\times/K^\times(F^\times)^2 \xrightarrow{N_{F/K}} K^\times/(K^\times)^2\right) \ .$$

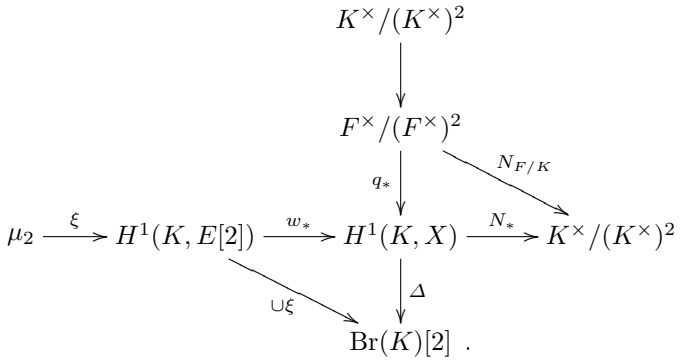
Proof. Let $\overline{F} = F \otimes_K \overline{K}$. We may identify $\overline{F} = \mathrm{Map}(\Phi, \overline{K})$ and $\mu_2(\overline{F}) = \mathrm{Map}(\Phi, \mu_2)$. These are identifications as Galois modules, the action of Galois being given by $\sigma(f) = (P \mapsto \sigma(f(\sigma^{-1}P)))$. An easy generalisation of Hilbert's theorem 90 shows that $H^1(K, \overline{F}^\times) = 0$ and hence $H^1(K, \mu_2(\overline{F})) = F^\times/(F^\times)^2$. We define $N : \mathrm{Map}(\Phi, \mu_2) \to \mu_2$ by $N(f) = \prod_{P \in \Phi} f(P)$. The constant maps give an inclusion $\mu_2 \to \mathrm{Map}(\Phi, \mu_2)$ with quotient X (say). We thus have short exact sequences of Galois modules

$$0 \longrightarrow \mu_2 \longrightarrow \mathrm{Map}(\Phi, \mu_2) \xrightarrow{q} X \longrightarrow 0$$

and

$$0 \longrightarrow E[2] \xrightarrow{w} X \xrightarrow{N} \mu_2 \longrightarrow 0$$

where $w(T)$ is the class of $P \mapsto e_2(P - P_0, T)$, for any fixed choice of $P_0 \in \Phi$. Taking the long exact sequences of Galois cohomology we obtain a diagram



Once we have shown that the diagram commutes, the theorem follows by a routine diagram chase.

We check that the lower left triangle commutes. Let $\eta \in Z^1(K, E[2])$ be a cocycle. Then $w_*(\eta)_\sigma$ is the map $P \mapsto e_2(P - P_0, \eta_\sigma)$. Applying the connecting map Δ gives $a \in Z^2(K, \mu_2)$ with

$$\begin{aligned} a_{\sigma\tau} &= e_2(P - \sigma(P_0), \sigma(\eta_\tau))\ e_2(P - P_0, \eta_\sigma)\ e_2(P - P_0, \eta_{\sigma\tau})^{-1} \\ &= e_2(P_0 - \sigma(P_0), \sigma(\eta_\tau))\ e_2(P - P_0, \sigma(\eta_\tau) + \eta_\sigma - \eta_{\sigma\tau}) \\ &= e_2(\xi_\sigma, \sigma(\eta_\tau)) \ . \end{aligned}$$

This is the cup product of ξ and η. The commutativity of the upper right triangle is clear. □

The case $\xi = 0$ of Theorem 4.1 is well-known. In this case F is the étale algebra $K \times L$ of $E[2]$ where $E : Y^2 = f(X)$ and $L = K[X]/(f(X))$.

Corollary 4.2. *There is a canonical isomorphism*

$$H^1(K, E[2]) \cong \ker\left(L^\times/(L^\times)^2 \stackrel{N_{L/K}}{\longrightarrow} K^\times/(K^\times)^2 \right) \ .$$

The following theorem, due to Steve Donnelly, gives an explicit description of the isomorphism of Theorem 4.1 (in one direction). We make the identification of Corollary 4.2 so that now ξ is represented by some $\alpha \in L^\times$. Let LF be the tensor product $L \otimes_K F$ and let $L[\sqrt{\alpha}]$ be the algebra $L[X]/(X^2 - \alpha)$. By the formulae in [4, §3] there is a natural inclusion $L[\sqrt{\alpha}] \subset LF$. (If $\mathrm{Gal}(F/K) \cong S_4$ then L is the resolvent cubic field, LF is the usual composite of fields, and we are quoting that α is a square in LF.) Let τ be the non-trivial automorphism of $L[\sqrt{\alpha}]$ that fixes L.

Theorem 4.3. *Let $\delta \in F^\times$ with $N_{F/K}(\delta) = k^2$ for some $k \in K$. Suppose we are given $\nu \in L[\sqrt{\alpha}]^\times$ with $N_{LF/L[\sqrt{\alpha}]}(\delta)/k = \tau(\nu)/\nu$. Then*

$$\beta := N_{LF/L[\sqrt{\alpha}]}(\delta)\nu^2 = kN_{L[\sqrt{\alpha}]/L}(\nu) \in L^\times \tag{4}$$

represents an element of $\ker\left(L^\times/(L^\times)^2 \stackrel{N_{L/K}}{\longrightarrow} K^\times/(K^\times)^2 \right)$ *mapping to δ under the isomorphisms of Theorem 4.1 and Corollary 4.2.*

Proof. We identify

$$LF = L \otimes_K F = \mathrm{Map}_K((E[2] \setminus \{0\}) \times \Phi, \overline{K}) \ .$$

Then $N_{LF/L[\sqrt{\alpha}]}(\delta)$ is the map $(T, P) \mapsto \delta(P)\delta(T + P)$. So fixing a base point $P_0 \in \Phi$ we can rewrite the first equality in (4) as

$$\beta(P - P_0) = \delta(P)\delta(P_0)\nu(P - P_0, P)^2 \tag{5}$$

for all $P \in \Phi$ with $P \neq P_0$.

The image of β in $H^1(K, X)$ is represented by a cocycle (ψ_σ) where

$$\psi_\sigma(P) = \begin{cases} \frac{\sigma\sqrt{\beta}}{\sqrt{\beta}}(P - P_0) & \text{if } P \neq P_0 \\ 1 & \text{if } P = P_0 \ . \end{cases}$$

It follows by (5) that

$$\psi_\sigma(P) = \tfrac{\sigma\sqrt{\delta}}{\sqrt{\delta}}(P)\tfrac{\sigma\sqrt{\delta}}{\sqrt{\delta}}(P_0)$$

for all $P \in \Phi$. (The case $P = P_0$ is just $1 = (\pm 1)^2$.) By the definition of X we may ignore the term involving P_0, and so (ψ_σ) also represents the image of δ in $H^1(K, X)$. □

Remark 4.4. If $\varepsilon = N_{LF/L[\sqrt{\alpha}]}(\delta)/k$ then $N_{L[\sqrt{\alpha}]/L}(\varepsilon) = 1$. So by Hilbert's theorem 90 there exists $\nu \in L[\sqrt{\alpha}]^\times$ with $\varepsilon = \tau(\nu)/\nu$. The construction of Theorem 4.3 therefore gives a well-defined map

$$\ker\left(F^\times/K^\times(F^\times)^2 \stackrel{N_{F/K}}{\longrightarrow} K^\times/(K^\times)^2\right) \to L^\times/\{1,\alpha\}(L^\times)^2 \ .$$

The ambiguity up to multiplication by α is predicted by Theorem 4.1, and in this construction comes from the arbitrary choice of sign for k.

5 Testing equivalence of 4-coverings

Let $g(X) \in K[X]$ be a (non-singular) quartic with flex algebra $F = K[\theta] = K[X]/(g(X))$. We put $\mathcal{QI}(K)^{\det=g} = \{(A,B) \in \mathcal{QI}(K) : \det(AX+B) = g(X)\}$. If $(A,B) \in \mathcal{QI}(K)^{\det=g}$ then keeping the notation of §3 we define

$$\mathcal{Q} = \theta^{-1}eA + T_1 + \theta T_2 + \theta^2 aB \tag{6}$$

with suitable modifications if $ae = 0$. (For example if $e = 0$ then the "$\theta = 0$ component" of $\mathcal{Q}$ is $-dA + T_1$.) Then $\mathcal{Q}$ is a rank 1 quadratic form, *i.e.* $\mathcal{Q} = \xi\ell^2$ for some $\xi \in F^\times$ and $\ell \in F[x_1,x_2,x_3,x_4]$ a linear form. This defines a map

$$\lambda \ : \ \mathcal{QI}(K)^{\det=g} \longrightarrow F^\times/(F^\times)^2\,; \quad (A,B) \mapsto \xi$$

inverse to the construction of §3.

Lemma 5.1. *Quadric intersections in $\mathcal{QI}(K)^{\det=g}$ define isomorphic coverings of $C_2 = \{Y^2 = g(X)\}$ if and only if they are related by a transformation $(\mu I_2, N) \in \mathcal{G}_4(K)$ with $\mu^2 \det(N) = 1$.*

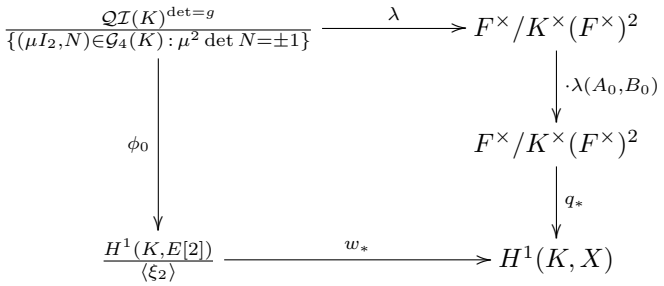
Proof. If $\pi : C_4 \to C_2$ is the 2-covering defined by $(A,B) \in \mathcal{QI}(K)^{\det=g}$ and $P_0 \in C_2$ is a ramification point of $C_2 \to \mathbb{P}^1$ then the divisor $\pi^*(P_0)$ is a hyperplane section of C_4 (in fact cut out by the linear form ℓ). So if a pair of quadric intersections determine isomorphic 2-coverings of C_2, then they must be K-equivalent. Moreover, the equivalence $(M,N) \in \mathcal{G}_4(K)$ is of the form described since, by definition of a 2-covering, the induced self-equivalence of g must be trivial as an automorphism of C_2. □

If $(A_0,B_0) \in \mathcal{QI}(K)^{\det=g}$ defines $C_4 \subset \mathbb{P}^3$ then the 2-coverings of C_2 are parametrised as twists of $C_4 \to C_2$ by $H^1(K, E[2])$. This defines a map

$$\phi_0 \ : \ \frac{\mathcal{QI}(K)^{\det=g}}{\{(\mu I_2, N) \in \mathcal{G}_4(K) \ : \ \mu^2 \det N = 1\}} \longrightarrow H^1(K,E[2]) \ .$$

We find that quotienting out by the transformations with $\mu^2 \det N = -1$ corresponds to quotienting out by $\langle \xi_2 \rangle$ where $\xi_2 \in H^1(K,E[2])$ is the class of g.

Theorem 5.2. *The following diagram is commutative.*



Proof. This is a variant of [20, Theorem 6.1.4]. Let $\mathcal{Q}_0 = \xi_0\ell_0^2$ and $\mathcal{Q}_1 = \xi_1\ell_1^2$ be the rank 1 quadratic forms determined by (A_0, B_0) and (A, B). If $(\mu I_2, N) \in \mathcal{G}_4(\overline{K})$ relates (A, B) and (A_0, B_0) then by properties of the Weil pairing

$$w_*(\phi_0(A,B)) = \left(\sigma \mapsto \frac{\ell_0 \circ \sigma(N) N^{-1}}{\ell_0} = \frac{\sigma(\ell_0 \circ N)}{\ell_0 \circ N}\right) \quad .$$

Since $\mathcal{Q}_1 = \mu\, \mathcal{Q}_0 \circ N$, this works out as $q_*(\xi_0\xi_1)$. □

The maps ϕ_0 and w_* of Theorem 5.2 are injective. It follows that λ is injective. So to test whether a pair of quadric intersections $(A_1, B_1), (A_2, B_2) \in \mathcal{QI}(K)$ are equivalent we proceed as follows. We have implemented this test in the case $K = \mathbb{Q}$ and contributed it to Magma [13].

Step 1. Let $g_i(X) = \det(A_i X + B_i)$ for $i = 1, 2$. We test whether g_1 and g_2 are equivalent, using one of the tests in [4], [5]. We are now reduced to the case $g_1 = g_2$. (If there is more than one equivalence between g_1 and g_2 then we must repeat the remaining steps for each of these.)

Step 2. Compute $\xi_i = \lambda(A_i, B_i)$ for $i = 1, 2$ by evaluating the quadratic form (6) at points in $\mathbb{P}^3(K)$. It helps with Step 3 if we use several points in $\mathbb{P}^3(K)$ to give several representatives for the class of ξ_i in $F^\times/(F^\times)^2$. (Spurious prime factors can then be removed from consideration by computing gcd's.)

Step 3. Let S be a finite set of primes of K, including all primes that ramify in F. We enlarge S so that $\xi_1, \xi_2 \in F(S', 2)$ where S' is the set of primes of F above S.

Step 4. The quadric intersections are equivalent if and only if $\xi_1\xi_2^{-1}$ is in the image of the natural map $K(S, 2) \to F(S', 2)$. We cut down the subgroup of $K(S, 2)$ to be considered by reducing modulo some random primes, and then loop over all possibilities.

In the case that (A_1, B_1) and (A_2, B_2) are equivalent, we can reduce to the case $\mathcal{Q}_1 = \xi_1\ell_1^2$ and $\mathcal{Q}_2 = \xi_2\ell_2^2$ with $\xi_1\xi_2^{-1} \in K$. Then solving $\ell_1 \circ N = \ell_2$ for $N \in \mathrm{Mat}_4(K)$, gives the change of co-ordinates relating the two quadric intersections. This transformation is also returned by our Magma function.

6 Adding 2-Selmer and 4-Selmer elements

In §8 we describe a general method for adding 4-Selmer group elements. This involves solving an explicit form of the local-to-global principle for $\mathrm{Br}(K)$. But in the special case where we add 2-Selmer and 4-Selmer elements, no such problem need be solved. This is essentially because (by a theorem of Zarhin [22] relating the cup product in Theorem 4.1 to the obstruction map in [6, Paper I], [15]) we have already solved all the conics we need when doing the original 2-descent. To make this explicit we have found the following partial description of the isomorphism of Theorem 4.1.

Let $g(X) \in K[X]$ be a quartic with invariants I and J. Let $L = K[\varphi]$ where φ is a root of $f(X) = X^3 - 3IX + J$. We assume that the discriminant $\Delta_0 = 27(4I^3 - J^2)$ is non-zero. Formulae in [4], [5] allow us to represent g by $\alpha = a_0 + a_1\varphi \in L^\times$ with $a_0, a_1 \in K$ and $N_{L/K}(\alpha) \in (K^\times)^2$. We assume $\alpha \notin (L^\times)^2$. As in §4 we put $F = K[X]/(g(X))$ and $LF = L \otimes_K F$.

Theorem 6.1. *If $\beta, \gamma \in L^\times$ are linear in φ with $N_{L/K}(\beta), N_{L/K}(\gamma) \in (K^\times)^2$ and $\alpha\beta\gamma \in (L^\times)^2$, then the isomorphisms of Theorem 4.1 and Corollary 4.2 map each of β and γ to the class of*

$$\delta := \mathrm{Tr}_{LF/F}\left(\frac{\sqrt{\alpha}}{f'(\varphi)}\right)\mathrm{Tr}_{LF/F}\left(\frac{\sqrt{\beta\gamma}}{f'(\varphi)}\right) \in F^\times \ .$$

Proof. Let $\varphi_1 = \varphi, \varphi_2, \varphi_3$ be the K-conjugates of φ, and likewise for α, β, γ, m where $\alpha\beta\gamma = m^2$. Using that α, β, γ are linear in φ we compute

$$N_{LF/L[\sqrt{\alpha}]}(\delta) = \frac{(\sqrt{\alpha_2} - \sqrt{\alpha_3})^2(\sqrt{\beta_2\gamma_3} - \sqrt{\beta_3\gamma_2})^2}{\Delta_0\ (\varphi_2 - \varphi_3)^2} \ .$$

The hypotheses of Theorem 4.3 are therefore satisfied with

$$k = \frac{(\alpha_2 - \alpha_3)(\beta_2\gamma_3 - \beta_3\gamma_2)}{\Delta_0\ (\varphi_2 - \varphi_3)^2} = \frac{a_1(b_1c_0 - b_0c_1)}{\Delta_0} \in K^\times$$

and (swapping β and γ if necessary to avoid dividing by zero)

$$\nu^{-1} = \frac{(\sqrt{\alpha_2} - \sqrt{\alpha_3})(\sqrt{\beta_2\gamma_3} - \sqrt{\beta_3\gamma_2})}{\sqrt{\alpha_2\beta_2\gamma_3} + \sqrt{\alpha_3\beta_3\gamma_2}} = 1 - \frac{m_2\beta_3 + m_3\beta_2}{m_2\gamma_3 + m_3\gamma_2}\sqrt{\frac{\gamma_2\gamma_3}{\beta_2\beta_3}} \ .$$

We are done since

$$(\sqrt{\alpha_2\beta_2\gamma_3} + \sqrt{\alpha_3\beta_3\gamma_2})^2 = \frac{(m_2\gamma_3 + m_3\gamma_2)^2}{\gamma_2\gamma_3} \equiv \gamma \mod (L^\times)^2 \ .$$

□

We give an example in the case $K = \mathbb{Q}$. The quartics

$$\begin{aligned} g_1(X) &= -675X^4 - 7970X^3 - 18923X^2 + 27176X - 7848 \\ g_2(X) &= -5483X^4 + 10470X^3 + 8869X^2 - 13240X - 8768 \\ g_3(X) &= -3728X^4 - 8536X^3 + 9037X^2 + 15940X - 13000 \end{aligned}$$

have invariants $I = 1071426889$ and $J = 70141299507574$. Moreover they sum to zero in $S^{(2)}(E/\mathbb{Q})$ where $E : -3Y^2 = f(X) = X^3 - 3IX + J$. Let $L = \mathbb{Q}(\varphi) = \mathbb{Q}[X]/(f(X))$ and $F_1 = \mathbb{Q}(\theta) = \mathbb{Q}[X]/(g_1(X))$. We use the existing `FourDescent` routine in Magma to compute 2-coverings D_i of $C_i = \{Y^2 = g_i(X)\}$ for $i = 2, 3$ and then add these using the method of §8 to give a 2-covering D_1 of $C_1 = \{Y^2 = g_1(X)\}$. By a formula in [4] the quartics g_1, g_2, g_3 are represented by

$$\begin{aligned} \alpha &= -900\varphi + 29459500 \\ \beta &= (-21932\varphi + 717892516)/3 \\ \gamma &= (-14912\varphi + 488109376)/3 \end{aligned}$$

in $L^\times/(L^\times)^2$. Theorem 6.1 and the map λ in §5 convert C_2 and D_1 to

$$\delta = 265659750\theta^3 + 32764441\,5\theta^2 + 91778693\,6\theta - 582546987$$

and $\xi_1 = 4725\theta^3 + 59165\theta^2 + 168496\theta - 106600$ in $F_1^\times/\mathbb{Q}^\times(F_1^\times)^2$. We then multiply δ and ξ_1 in $F_1^\times$ and recover a new 2-covering D_1' of C_1 by the method of §3. By Theorem 5.2 this new 4-covering of E represents the sum of $\iota_*(C_2)$ and D_1 in $S^{(4)}(E/\mathbb{Q})$ where ι_* is the map in (1). Notice that at no stage of the computation of D_1 and D_1' did we need to find the class group and units of F_1, although it is only for much larger examples that this saving becomes worthwhile.

7 Computing the action of the Jacobian

In this section we generalise the formulae of [8, §7] from 3-coverings to 4-coverings. The main new ingredient is a certain generalisation of the Hessian, introduced in [9]. This is an $\mathrm{SL}_2(K) \times \mathrm{SL}_4(K)$-equivariant polynomial map $H : \mathcal{QI}(K) \to \mathcal{QI}(K)$. In the notation of §3 it is given by

$$H \ : \ (A, B) \mapsto (6T_2 - cA - 3bB,\ 6T_1 - cB - 3dA) \ . \tag{7}$$

The analogue of the Hesse pencil of plane cubics, is the "Hesse family" of quadric intersections

$$U(a, b) = (a(x_1^2 + x_3^2) - 2bx_2x_4,\ a(x_2^2 + x_4^2) - 2bx_1x_3)$$

with invariants

$$\begin{aligned} c_4(a, b) &= 2^8(a^8 + 14a^4b^4 + b^8) \\ c_6(a, b) &= -2^{12}(a^{12} - 33a^8b^4 - 33a^4b^8 + b^{12}) \\ \Delta(a, b) &= 2^{20}a^4b^4(a^4 - b^4)^4 \end{aligned}$$

and Hessian $U(a', b')$ where $a' = -2^4a(a^4 - 5b^4)$ and $b' = 2^4b(5a^4 - b^4)$.

If $U \in \mathcal{QI}(K)$ is a non-singular quadric intersection with Jacobian E, then the pencil of quadric intersections spanned by U and its Hessian is a twist of the Hesse family. So there are exactly six singular fibres, and each singular fibre is a "square" (really a quadrilateral spanning $\mathbb{P}^3$). Each square is uniquely the

intersection of a pair of rank 2 quadrics and the union of these quadrics is the set of fixed planes for the action of M_T on $\mathbb{P}^3$ for some $T \in E[4] \setminus E[2]$. So there is a Galois equivariant bijection between the syzygetic squares and the cyclic subgroups of $E[4]$ of order 4. (Our terminology generalises that in [12, §II.7].)

Lemma 7.1. *Let U be a non-singular quadric intersection with invariants c_4, c_6 and Hessian H. Let $T = (x_T, y_T)$ be a point of order 4 on the Jacobian (3). Then the syzygetic square corresponding to $\pm T$ is defined by $\mathcal{S} = \frac{1}{3}x_T U + H$, and this quadric intersection satisfies $H(\mathcal{S}) = \nu_T^2 \mathcal{S}$ where*

$$\nu_T = (x_T^4 - 54c_4x_T^2 - 216c_6x_T - 243c_4^2)/(18y_T) \ .$$

Proof. We may assume that U belongs to the Hesse family and that $T = (2^4 3(a^4 - 5b^4), 2^7 3^3 i(a^4 - b^4)b^2)$. The lemma follows by direct calculation. □

Let $C \subset \mathbb{P}^3$ be a genus one normal curve of degree 4, defined over K, and with Jacobian E. Let L/K be any field extension. Given $T \in E(L)$ a point of order 4, we aim to construct $M_T \in \mathrm{GL}_4(L)$ describing the action of T on C. We start with a quadric intersection U defining C. Then we compute the syzygetic square $\mathcal{S} = \frac{1}{3}x_T U + H$ as described in Lemma 7.1. Making a change of co-ordinates (defined over K) we may assume

- The point $(1 : 0 : 0 : 0)$ does not lie on either of the rank 2 quadrics whose intersection is the syzygetic square.
- The line $\{x_3 = x_4 = 0\}$ does not meet either diagonal of the square.

Let A and B be the rank 2 quadrics in the pencil spanned by $\mathcal{S}$, scaled so that the coefficient of x_1^2 is 1 in each case. These quadrics are defined over a field L' with $[L' : L] \leq 2$, and are easily found by factoring the determinant of a generic quadric in the pencil. We factor A and B over $\overline{K}$ as

$$\begin{aligned} A &= (x_1 + \alpha_1 x_2 + \beta_1 x_3 + \gamma_1 x_4)(x_1 + \alpha_3 x_2 + \beta_3 x_3 + \gamma_3 x_4) \\ B &= (x_1 + \alpha_2 x_2 + \beta_2 x_3 + \gamma_2 x_4)(x_1 + \alpha_4 x_2 + \beta_4 x_3 + \gamma_4 x_4) \ . \end{aligned}$$

Then we put

$$P = \begin{pmatrix} 1 & \alpha_1 & \beta_1 & \gamma_1 \\ 1 & \alpha_2 & \beta_2 & \gamma_2 \\ 1 & \alpha_3 & \beta_3 & \gamma_3 \\ 1 & \alpha_4 & \beta_4 & \gamma_4 \end{pmatrix}$$

and $\xi = \alpha_1 - i\alpha_2 - \alpha_3 + i\alpha_4$ where $i = \sqrt{-1}$.

Theorem 7.2. *If $\xi \neq 0$ then the matrix*

$$M_T = \xi P^{-1} \begin{pmatrix} 1 & & & \\ & i & & \\ & & -1 & \\ & & & -i \end{pmatrix} P$$

belongs to $\mathrm{GL}_4(L)$ and describes the action of T (or $-T$) on C.

Proof. The image of this matrix in PGL_4 has order 4, and acts on $\mathbb{P}^3$ with fixed planes defined by the linear factors of A and B. So the second statement is clear. Theorem 7.3 shows that M_T has entries in L. (It may also be checked directly that each entry is fixed by $\mathrm{Gal}(L'(i)/L)$.) □

Any polynomial in the α_i, β_i, γ_i invariant under the action of $C_2 \times C_2$ that swaps the subscripts $1 \leftrightarrow 3$ and $2 \leftrightarrow 4$ may be rewritten as a polynomial in the coefficients of A and B. We write $A = \sum_{i \le j} a_{ij} x_i x_j$ and $B = \sum_{i \le j} b_{ij} x_i x_j$. Then by computer algebra we find an expression for $\kappa = (\alpha_1 - \alpha_3)(\alpha_2 - \alpha_4)\det(P)$ as a polynomial in the a_{ij} and b_{ij}, and likewise for the entries of

$$M_1 = (\alpha_2 - \alpha_4)\mathrm{adj}(P)\mathrm{Diag}(1, 0, -1, 0)P$$

and

$$M_2 = (\alpha_1 - \alpha_3)\mathrm{adj}(P)\mathrm{Diag}(0, 1, 0, -1)P \ .$$

Let $\mathcal{S} = (\lambda_1 A + \mu_1 B, \lambda_2 A + \mu_2 B)$ with $\lambda_i, \mu_i \in L'$. Then $\kappa \in L$, whereas if A and B are not defined over L then $\mathrm{Gal}(L'/L)$ interchanges $\lambda_1 \leftrightarrow \lambda_2$, $\mu_1 \leftrightarrow \mu_2$ and $M_1 \leftrightarrow M_2$.

Theorem 7.3. *The matrix M_T of Theorem 7.2 is given by*

$$M_T = \frac{a_{12}^2 - 4a_{22}}{\kappa} M_1 + \frac{b_{12}^2 - 4b_{22}}{\kappa} M_2 \pm \frac{\lambda_1\mu_2 - \lambda_2\mu_1}{\nu_T}(M_1 - M_2)$$

where $\nu_T = (x_T^4 - 54c_4x_T^2 - 216c_6x_T - 243c_4^2)/(18y_T)$.

Proof. By our choice of co-ordinates we have $\alpha_1 \neq \alpha_3$ and $\alpha_2 \neq \alpha_4$. So $\kappa \in L$ is non-zero. We compute

$$\begin{aligned} \kappa M_T &= \xi(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_4)\mathrm{adj}(P)\mathrm{Diag}(1, i, -1, -i)P \\ &= \xi(\alpha_1 - \alpha_3)M_1 + i\xi(\alpha_2 - \alpha_4)M_2 \\ &= (\alpha_1 - \alpha_3)^2 M_1 + (\alpha_2 - \alpha_4)^2 M_2 - i\kappa(\det P)^{-1}(M_1 - M_2) \ . \end{aligned}$$

Since $H(x_1x_3, x_2x_4) = (-x_1x_3, -x_2x_4)$ we have

$$H(\mathcal{S}) = -(\lambda_1\mu_2 - \lambda_2\mu_1)^2 \det(P)^2 \mathcal{S} \ .$$

By Lemma 7.1 we deduce $\nu_T = \pm i(\lambda_1\mu_2 - \lambda_2\mu_1)\det(P)$, and substituting this into the above expression for κM_T completes the proof of the theorem. □

By our choice of co-ordinates it is impossible that both $\xi = \alpha_1 - i\alpha_2 - \alpha_3 + i\alpha_4$ and $\xi' = \alpha_1 + i\alpha_2 - \alpha_3 - i\alpha_4$ vanish. So if our formula for M_T gives the zero matrix, we can instead use the formula for M_{-T} and take the inverse.

8 Adding 4-Selmer group elements

Finally we outline how the theory in [6] can be used to add elements of $S^{(4)}(E/K)$. (Of course, the method in §6 should be used in preference whenever it applies.)

Let $C \subset \mathbb{P}^3$ be a 4-covering of E. We embed E in $\mathbb{P}^3$ via $(x, y) \mapsto (1 : x : y : x^2)$. In [10, §6.2] we gave a practical algorithm for computing $B \in \mathrm{GL}_4(\overline{K})$ describing a change of co-ordinates on $\mathbb{P}^3$ taking C to E.

Now let R be the étale algebra of $E[4]$. Applying the formulae of §7 over each constituent field of R, we compute $M, M' \in \mathrm{GL}_4(R)$ describing the actions of $E[4]$ on $E \subset \mathbb{P}^3$ and $C \subset \mathbb{P}^3$ respectively. We scale these matrices by using the method of §2 to find good representatives for their determinants in $R^\times/(R^\times)^4$. These matrices now determine $\gamma \in \overline{R}^\times = \mathrm{Map}(E[4], \overline{K}^\times)$ by the rule

$$BM'_TB^{-1} = \gamma(T)M_T$$

for all $T \in E[4]$. It is shown in [6, Paper I] that we may identify $H^1(K, E[4])$ with a certain subquotient of $(R \otimes R)^\times$. Our 4-covering corresponds to $\rho \in (R \otimes R)^\times$ given by the rule

$$\rho(S, T) = \frac{\gamma(S)\gamma(T)}{\gamma(S + T)} \tag{8}$$

for all $S, T \in E[4]$. So if 4-coverings C_1 and C_2 determine $\gamma_1, \gamma_2 \in \overline{R}^\times$, then their sum (by the group law of $H^1(K, E[4])$) corresponds to the product $\gamma_1\gamma_2$.

It remains to explain how, if C is everywhere locally soluble, we can recover equations for $C \subset \mathbb{P}^3$ from $\gamma \in \overline{R}^\times$. Let $\varepsilon \in (R \otimes R)^\times$ be the element determined by $\varepsilon(S, T)I_4 = M_S M_T M_{S+T}^{-1}$ for all $S, T \in E[4]$, and let ρ be given by (8). We view $R \otimes R$ as an R-algebra via the comultiplication $R \to R \otimes R$ and write $\mathrm{Tr} : R \otimes R \to R$ for the corresponding trace map. In [6, Paper I] we defined the obstruction algebra $A_\rho = (R, +, *_{\varepsilon\rho})$ to be the K-vector space R equipped with a new multiplication $z_1 *_{\varepsilon\rho} z_2 = \mathrm{Tr}(\varepsilon\rho.(z_1 \otimes z_2))$.

In our situation, we already have a trivialisation of A_ρ over $\overline{K}$, namely the isomorphism of $\overline{K}$-algebras $A_\rho \otimes_K \overline{K} \cong \mathrm{Mat}_4(\overline{K})$ given by

$$z \mapsto \sum_{T \in E[4]} z(T)\gamma(T)M_T \ .$$

So picking a basis $r_1, \ldots, r_{16}$ for R gives matrices $M_1, \ldots, M_{16} \in \mathrm{Mat}_4(\overline{K})$. We then compute structure constants $c_{ijk} \in K$ for the obstruction algebra A_ρ by the rule $M_iM_j = \sum_{k=1}^{16} c_{ijk}M_k$.

Our only implementation so far is in the case $K = \mathbb{Q}$. In practice we fix an embedding $\overline{\mathbb{Q}} \subset \mathbb{C}$, and so γ is represented by a 16-tuple of complex numbers (to some precision). In [6, Paper III] we will explain how to choose a basis for R so that the structure constants c_{ijk} are (reasonably small) integers. This makes it easy to recognise them from their floating point approximations.

Since C is everywhere locally soluble, it is guaranteed by class field theory that there is an isomorphism of K-algebras $A_\rho \cong \mathrm{Mat}_4(K)$. We must find such an isomorphism explicitly, and for this we use the method of Pílniková [16], who reduces the problem to that of solving conics over (at most quadratic) extensions of K. Finally any one of the three methods in [6, Paper I, §5] may be used to recover equations for C. In practice we use the Hesse pencil method, which by virtue of the Hessian (7) has a natural generalisation from 3-descent to 4-descent.

Acknowledgements

I would like to thank John Cremona, Michael Stoll and Denis Simon for many useful discussions in connection with this work, and Steve Donnelly for providing me with the construction described in Theorem 4.3 and Remark 4.4. All computer calculations in support of this work were performed using Magma [13].

References

1. S.Y. An, S.Y. Kim, D.C. Marshall, S.H. Marshall, W.G. McCallum and A.R. Perlis, Jacobians of genus one curves, *J. Number Theory* 90 (2001), no. 2, 304–315.
2. J.W.S. Cassels, *Lectures on elliptic curves*, LMS Student Texts, 24, CUP, Cambridge, 1991.
3. J.W.S. Cassels, Second descents for elliptic curves, *J. reine angew. Math.* 494 (1998), 101–127.
4. J.E. Cremona, Classical invariants and 2-descent on elliptic curves, *J. Symbolic Comput.* 31 (2001), no. 1-2, 71–87.
5. J.E. Cremona and T.A. Fisher, On the equivalence of binary quartics, *submitted*.
6. J.E. Cremona, T.A. Fisher, C. O'Neil, D. Simon and M. Stoll, Explicit n-descent on elliptic curves, I Algebra, *J. reine angew. Math.* 615 (2008), II Geometry, *submitted*, III Algorithms, *in preparation*.
7. S. Donnelly, Computing the Cassels-Tate pairing, *in preparation*.
8. T.A. Fisher, Testing equivalence of ternary cubics, *Algorithmic number theory*, 333–345, Lecture Notes in Comput. Sci., 4076, Springer, Berlin, 2006.
9. T.A. Fisher, The Hessian of a genus one curve, *preprint*.
10. T.A. Fisher, Finding rational points on elliptic curves using 6-descent and 12-descent, *submitted*.
11. T.A. Fisher, E.F. Schaefer and M. Stoll, The yoga of the Cassels-Tate pairing, *submitted*.
12. D. Hilbert, *Theory of algebraic invariants*, CUP, Cambridge, 1993.
13. MAGMA is described in W. Bosma, J. Cannon and C. Playoust, The Magma algebra system I: The user language, *J. Symbolic Comput.* 24 (1997), no. 3-4, 235–265. The Magma home page is at `http://magma.maths.usyd.edu.au/magma/`
14. J.R. Merriman, S. Siksek and N.P. Smart, Explicit 4-descents on an elliptic curve, *Acta Arith.* 77 (1996), no. 4, 385–404.
15. C. O'Neil, The period-index obstruction for elliptic curves, *J. Number Theory* 95 (2002), no. 2, 329–339.
16. J. Pílniková, Trivializing a central simple algebra of degree 4 over the rational numbers, *J. Symbolic Comput.* 42 (2007), no. 6, 579–586.
17. B. Poonen and E.F. Schaefer, Explicit descent for Jacobians of cyclic covers of the projective line, *J. reine angew. Math.* 488 (1997), 141–188.
18. S. Siksek, *Descent on curves of genus* 1, PhD thesis, University of Exeter, 1995.
19. D. Simon, Computing the rank of elliptic curves over number fields, *LMS J. Comput. Math.* 5 (2002), 7–17 (electronic).
20. S. Stamminger, *Explicit 8-descent on elliptic curves*, PhD thesis, International University Bremen, 2005.
21. T. Womack, *Explicit descent on elliptic curves*, PhD thesis, University of Nottingham, 2003.
22. Yu. G. Zarhin, Noncommutative cohomology and Mumford groups, *Math. Notes* 15 (1974), 241–244.