MATHEMATICS OF COMPUTATION
Volume 84, Number 292, March 2015, Pages 895–922
S 0025-5718(2014)02858-5
Article electronically published on July 29, 2014

EXPLICIT n-DESCENT ON ELLIPTIC CURVES III. ALGORITHMS

J. E. CREMONA, T. A. FISHER, C. O'NEIL, D. SIMON, AND M. STOLL

ABSTRACT. This is the third in a series of papers in which we study the n-Selmer group of an elliptic curve, with the aim of representing its elements as curves of degree n in $\mathbb{P}^{n-1}$. The methods we describe are practical in the case $n = 3$ for elliptic curves over the rationals, and have been implemented in MAGMA.

One important ingredient of our work is an algorithm for trivialising central simple algebras. This is of independent interest; for example, it could be used for parametrising Brauer-Severi surfaces.

1. INTRODUCTION

Descent on an elliptic curve E, defined over a number field K, is a method for obtaining information about both the Mordell-Weil group $E(K)$ and the Tate-Shafarevich group $\text{Ш}(E/K)$. Indeed for each integer $n \geq 2$ there is an exact sequence

$$0 \to E(K)/nE(K) \to \text{Sel}^{(n)}(E/K) \to \text{Ш}(E/K)[n] \to 0,$$

where $\text{Sel}^{(n)}(E/K)$ is the n-Selmer group.

This is the third in a series of papers in which we study the n-Selmer group with the aim of representing its elements (when $n \geq 3$) as curves of degree n in $\mathbb{P}^{n-1}$. Having this representation allows searching for rational points on C (which in turn gives points in $E(K)$, since C may be seen as an n-covering of E) and is a first step towards doing higher descents. A further application is to the study of explicit counterexamples to the Hasse Principle.

The Selmer group $\text{Sel}^{(n)}(E/K)$ is by definition a subgroup of the Galois cohomology group $H^1(K, E[n])$, which parametrises the n-coverings of E. An n-covering $\pi\colon C \to E$ represents a Selmer group element if and only if C is everywhere locally soluble, i.e., C has K_v-rational points for each completion K_v of K. In this case it was shown by Cassels [5] that C admits a K-rational divisor D of degree n. When $n > 2$, we can then use the complete linear system $|D|$ to embed C in $\mathbb{P}^{n-1}$. Following the terminology in [10, Section 1.3], the image is called a *genus one normal curve* of degree n. For $n = 2$ we obtain instead a double cover $C \to \mathbb{P}^1$. More precisely, Cassels' argument shows that $\text{Sel}^{(n)}(E/K)$ is contained in the "kernel" of the obstruction map $\text{Ob}\colon H^1(K, E[n]) \to \text{Br}(K)$.

In the first paper of this series [10] we gave a list of interpretations of $H^1(K, E[n])$ and of the obstruction map. Then we showed how, given $\xi \in H^1(K, E[n])$, to explicitly represent $\text{Ob}(\xi)$ as a central simple algebra A of dimension n^2 over K, by giving structure constants for A; we call A the *obstruction algebra*. In the case

Received by the editor August 31, 2012 and, in revised form, June 4, 2013 and June 28, 2013.
2010 *Mathematics Subject Classification*. Primary 11G05, 14H25, 14H52.

$\xi \in \mathrm{Sel}^{(n)}(E/K)$, we have $A \cong \mathrm{Mat}_n(K)$. Assuming the existence of a "Black Box" to compute such an isomorphism explicitly, a process we call *trivialising the obstruction algebra*, we then outlined three algorithms to compute equations for $C \subset \mathbb{P}^{n-1}$. These were called the Hesse pencil, flex algebra, and Segre embedding methods. In the second paper [11] we developed the Segre embedding method. In this paper we are again concerned with the Segre embedding method. We give further details of the algorithms and, in particular, in Section 6 we explain our method for trivialising the obstruction algebra.

Returning to general n, we observe that

$$\mathrm{Sel}^{(mn)}(E/K) \cong \mathrm{Sel}^{(m)}(E/K) \times \mathrm{Sel}^{(n)}(E/K)$$

whenever m and n are coprime. Therefore for the purposes of computing Selmer groups we can restrict our attention to prime powers n. Then, if $n = p^f$ with $f \geq 2$, the most efficient way to proceed seems to be to first recursively compute $\mathrm{Sel}^{(p^{f-1})}(E/K)$, to realise the elements of that Selmer group as suitable covering curves (using the methods of this paper, for example), and then to compute the fibres of the natural map $\mathrm{Sel}^{(p^f)}(E/K) \to \mathrm{Sel}^{(p^{f-1})}(E/K)$ via p-descents on these covering curves. This has been worked out for $p = 2$ and $f = 2$ by Siksek [35], Merriman, Siksek and Smart [28], Cassels [6] and Womack [39]; for $p = 2$ and $f = 3$ by Stamminger [36]; and for odd p and $f = 2$ by Creutz [14].

In Section 2 we recall the construction of an étale algebra (that is, a product of number fields) R and a homomorphism $\partial\colon R^\times \to (R \otimes R)^\times$ such that $\mathrm{Sel}^{(n)}(E/K)$ may be realised either as a subgroup of $(R\otimes R)^\times/\partial R^\times$, with elements represented by $\rho \in (R\otimes R)^\times$, or as a subgroup of $R^\times/(R^\times)^n$, with elements represented by $\alpha \in R^\times$. The first of these works for any $n \geq 2$ and is better suited to the computation of the obstruction algebra and equations for C. The second only works for prime n, but is better suited to computing the Selmer group itself, in that the class group and unit calculations are more manageable. So in Section 2.4, we discuss how to convert from one representation to the other (from α to ρ). The Segre embedding method is then reviewed in Section 3.

It is sometimes convenient to assume $n > 2$. For example, when $n = 2$ the map $C \to \mathbb{P}^1$ is a double cover rather than an embedding. However, if the Segre embedding method is suitably interpreted in the case $n = 2$, then it corresponds exactly to the classical number field method[1] for 2-descent. This is explained in [12, Section 3]. In Section 4, we give an equally explicit description of our algorithms in the case $n = 3$, assuming that the action of Galois on $E[3]$ is generic. We do not give full details of the modifications required to handle the other Galois actions as this would be unduly tedious, though each case had to be handled in detail in our MAGMA implementation.

Starting with $\alpha \in R^\times$, we write down structure constants for the obstruction algebra A. Then we trivialise the algebra A. Using the trivialisation, we obtain a plane cubic $C \subset \mathbb{P}^2$. Now, the element α is typically of very large height: it comes out of a class group and unit calculation that involves many random choices. Consequently, the first equation for C which we obtain is a ternary cubic with enormous coefficients. In order to obtain a more reasonable equation, we finally

[1] An alternative method for 2-descent over $K = \mathbb{Q}$, based on invariant theory, is implemented in `mwrank` [8], and is competitive over a large range of curves, but seems to become impractical in other cases: when K is a larger number field, or when $n > 2$.

use our algorithms for minimisation and reduction (see [13]) to make a good change of coordinates.

After we wrote our initial implementation for $K = \mathbb{Q}$ and $n = 3$, it became clear that the algorithm could be improved by carrying out steps equivalent to minimisation and reduction at an earlier stage. First, α should be replaced by a good representative modulo nth powers, as described in [19, Section 2]. Then we should choose a good basis for the obstruction algebra, so as to make the structure constants small integers. This is described in Section 5, and makes trivialising the obstruction algebra much easier. In fact, this trivialisation is again a problem of "minimisation and reduction" type. As a result, the algorithms in [13], although still required, do not need to work so hard.

In Section 6 we describe our methods for trivialising the obstruction algebra. Since our methods are of independent interest, we have made this section self-contained. For instance, our methods could be used to improve the algorithm in [24] for parametrising Brauer-Severi surfaces.

One peculiar feature of the Segre embedding method is that in our initial implementation (for $K = \mathbb{Q}$ and $n = 3$) it was necessary to multiply by a "fudge factor" $1/y$ to ensure that the projection of $C \subset \mathbb{P}(A)$ to the trace 0 subspace is contained in the rank 1 locus. The need for this factor was justified by a generic calculation (unpublished) specific to the case $n = 3$. In Section 7 we give a better explanation, based on the theory in [11], that works for all odd integers n.

One application of our work is that it can help find generators of large height on an elliptic curve. Indeed, the logarithmic height of a rational point on an n-covering is expected to be smaller by a factor $2n$ compared to its image on the elliptic curve. See [20] for a precise statement. Our work in the case $n = 3$ is a starting point both for the work on 6- and 12-descents in [18], and for the work on 9-descent in [14]. In Section 8 we illustrate our work by computing some explicit elements of $Ш(E/\mathbb{Q})[3]$. The use of our methods to compute some explicit elements of $Ш(E/\mathbb{Q})[5]$ is described in [22].

Our algorithms have been implemented in (and contributed to) MAGMA [3, Version 2.13 and later] for $K = \mathbb{Q}$ and $n = 3$. A first version of the implementation was written by Michael Stoll; it was restricted to the case of a transitive Galois action on the points of order 3. Steve Donnelly extended the part that computes the 3-Selmer group as an abstract group to cover all possible Galois actions, and Tom Fisher reworked and extended the part that turns abstract Selmer group elements into plane cubic curves, so that it also works for all possible Galois actions.

These programs are currently specific to the case $K = \mathbb{Q}$. The two main obstacles to extending them to general number fields are as follows. First, it would be necessary (unless the Galois action on $E[3]$ is smaller than usual) to compute class group and units over number fields of larger degree. Second, we do not have a suitable theory of lattice reduction over number fields. Notice that our algorithms over $K = \mathbb{Q}$ are dependent on the LLL-algorithm, first in [19, Section 2], then in Sections 5 and 6 and finally in [13]. It is possible that the algorithms described in [17] could be used here, but we have not yet investigated this further.

2. Algorithms in outline: Algebra

In this section we give an outline of the algorithms used in our implementation of explicit 3-descent on elliptic curves over $\mathbb{Q}$. However, as far as possible in this overview, we keep to the case where n is general and the base field is a general number field K. Details specific to the case $n = 3$ can be found in Section 4 below. We begin with a review of the computation of the Selmer group as an abstract group. In the following, we use $E[n]$ to denote both the group scheme of n-torsion points on an elliptic curve E over a field K and the Galois module $E[n](\overline{K}) = E(\overline{K})[n]$. If X is a finite set with G_K-action, then the *étale algebra of* X is the K-algebra $\operatorname{Map}_K(X, \overline{K})$ of G_K-equivariant maps from X to $\overline{K}$; this is simply the coordinate ring of the affine K-scheme whose set of $\overline{K}$-points is X.

2.1. **The étale algebra.** Let E be an elliptic curve over a field K. We will take K to be a number field later. We fix a Weierstraß equation for E and denote the coordinate functions with respect to this equation by x and y. Let $n \geq 2$ be an integer not divisible by the characteristic of K. We let $R = \operatorname{Map}_K(E[n], \overline{K})$ be the étale algebra of $E[n]$. This is a product of finite extensions of K corresponding to the Galois orbits on $E[n]$, where the component corresponding to the orbit of $T \in E[n]$ is $K(T)$, the field of definition of T. There is always a splitting $R = K \times L$ with K corresponding to the singleton orbit $\{O\}$ and $L = \operatorname{Map}_K(E[n] \setminus \{O\}, \overline{K})$. If n is a prime p, then generically the Galois action is transitive on the points of order p, and L/K is a field extension of degree $p^2 - 1$.

The tensor product $R \otimes_K R$ is the étale algebra of $E[n] \times E[n]$. We denote by $\operatorname{Sym}^2_K(R)$ the subalgebra consisting of symmetric functions:

$$\operatorname{Sym}^2_K(R) = \{\rho \in R \otimes_K R \mid \rho(T_1, T_2) = \rho(T_2, T_1) \text{ for all } T_1, T_2 \in E[n]\}.$$

This is the étale algebra of the set of unordered pairs of n-torsion points. As before, these algebras split into products of finite field extensions of K corresponding to the Galois orbits on $E[n] \times E[n]$ and on the set of unordered pairs of n-torsion points, respectively. The algebra $\operatorname{Sym}^2_K(R)$ contains a factor corresponding to unordered bases of $E[n]$ as a $\mathbb{Z}/n\mathbb{Z}$-module. When n is a prime p, then generically, the Galois group acts transitively on these bases, and the corresponding factor of $\operatorname{Sym}^2_K(R)$ is a field extension of K of degree $(p^2 - 1)(p^2 - p)/2$.

The group law $E[n] \times E[n] \to E[n]$ corresponds to the comultiplication homomorphism $\Delta_K \colon R \to \operatorname{Sym}^2_K(R) \subset R \otimes_K R$. We write $\operatorname{Tr}_K \colon R \otimes_K R \to R$ for the trace map obtained by viewing $R \otimes_K R$ as an R-algebra via Δ_K. In terms of maps we have

$$\Delta_K(\alpha) \colon (T_1, T_2) \mapsto \alpha(T_1 + T_2) \quad \text{and} \quad \operatorname{Tr}_K(\rho) \colon T \mapsto \sum_{T_1 + T_2 = T} \rho(T_1, T_2)\,.$$

2.2. **Computation of the Selmer group: Using w_2.** We define

$$\begin{aligned} \partial_K \colon R^\times &\longrightarrow \operatorname{Sym}^2_K(R)^\times \\ \text{by} \qquad \alpha &\longmapsto \frac{\alpha \otimes \alpha}{\Delta_K(\alpha)} = \left((T_1, T_2) \mapsto \frac{\alpha(T_1)\alpha(T_2)}{\alpha(T_1 + T_2)} \right). \end{aligned}$$

In [10, p. 138], we defined another map ∂, which we here denote $\partial_K^{(2)}$ to avoid confusion. It is given by

$$\begin{aligned} \partial_K^{(2)} \colon (R \otimes_K R)^\times &\longrightarrow (R \otimes_K R \otimes_K R)^\times \\ \rho &\longmapsto \left((T_1, T_2, T_3) \mapsto \frac{\rho(T_1, T_2)\rho(T_1 + T_2, T_3)}{\rho(T_1, T_2 + T_3)\rho(T_2, T_3)} \right). \end{aligned}$$

We let $H_K = \mathrm{Sym}^2_K(R)^\times \cap \ker \partial^{(2)}_K$.

Let $\overline{R} = R \otimes_K \overline{K}$, which is the étale algebra of $E[n]$ over $\overline{K}$, and let $\mathrm{Sym}^2_{\overline{K}}(\overline{R})$ be the étale algebra over $\overline{K}$ of the set of unordered pairs of n-torsion points. Similarly, we write $\overline{H}$ for $H_{\overline{K}}$. We usually abbreviate H_K as H, and then drop the subscripts on Δ, ∂, etc.

Let $w\colon E[n] \to \overline{R}^\times$ be given by

$$w(S)\colon T \longmapsto e_n(S,T)$$

where $e_n\colon E[n] \times E[n] \to \mu_n$ denotes the Weil pairing. Then it is easily seen that the image of w equals the kernel of $\partial_{\overline{K}}$. We showed in [10] that the following is an exact sequence of G_K-modules:

$$0 \longrightarrow E[n] \xrightarrow{w} \overline{R}^\times \xrightarrow{\partial_{\overline{K}}} \overline{H} \longrightarrow 0\,.$$

Taking cohomology, this gives an isomorphism

$$w_2\colon H^1(K, E[n]) \longrightarrow H/\partial R^\times\,;$$

see [10, Lemmas 3.2 and 3.5].

Recall the Kummer exact sequence

$$0 \longrightarrow E(K)/nE(K) \xrightarrow{\delta} H^1(K, E[n]) \longrightarrow H^1(K,E)[n] \longrightarrow 0\,.$$

We now give an explicit description of the composition $w_2 \circ \delta$. For $T_1, T_2 \in E[n]$ define rational functions r_{T_1,T_2} on E by (compare [11, p. 67])

$$r_{T_1,T_2} = \begin{cases} 1 & \text{if } T_1 = O \text{ or } T_2 = O,\\ x - x(T_1) & \text{if } T_1 + T_2 = O,\ T_1 \neq O,\\ \dfrac{y + y(T_1+T_2)}{x - x(T_1+T_2)} - \lambda(T_1,T_2) & \text{otherwise,} \end{cases}$$

where $\lambda(T_1,T_2)$ denotes the slope of the line joining T_1 and T_2, or the slope of the tangent line at $T_1 = T_2$ if the points coincide. We can package these functions into a single element $r \in \mathrm{Sym}^2_K(R)(E)^\times = \mathrm{Map}_K(X, \overline{K}(E)^\times)$, where X is the G_K-set of unordered pairs of n-torsion points. We can extend r to divisors on E with support disjoint from $E[n]$ by defining

$$r\Big(\sum_P n_P(P)\Big) = \prod_P r(P)^{n_P}\,.$$

Then for a principal divisor $D = \mathrm{div}(h)$ with support disjoint from $E[n]$ we find by Weil reciprocity

$$\begin{aligned} r_{T_1,T_2}(D) &= r_{T_1,T_1}\big(\mathrm{div}(h)\big) = h\big(\mathrm{div}(r_{T_1,T_2})\big)\\ &= \frac{h(T_1)h(T_2)}{h(O)h(T_1+T_2)} = \frac{1}{h(O)}(\partial h|_{E[n]})(T_1,T_2)\,. \end{aligned}$$

We can scale h so that $h(O) = 1$; then

$$r\big(\mathrm{div}(h)\big) = \partial h|_{E[n]} \in \partial R^\times$$

if $h \in K(E)^\times$. Therefore, we obtain a well-defined map

$$\widetilde{r}\colon E(K) \cong \mathrm{Pic}^0(E/K) \longrightarrow H/\partial R^\times\,.$$

We then have (compare [37, Prop. 2.3]):

Proposition 2.1. *The composition $w_2 \circ \delta$ is given by $\widetilde{r}\colon E(K) \to H/\partial R^\times$.*

We now assume that K is a number field. For a place v of K, we write $R_v = R \otimes_K K_v$ and $H_v = H_{K_v}$. We denote the canonical map $H/\partial R^\times \to H_v/\partial R_v^\times$ by res_v. The maps corresponding to δ and w_2 that we obtain by working over K_v are denoted by δ_v and $w_{2,v}$. By the definition of the n-Selmer group, and the fact that w_2 is an isomorphism, we have

$$w_2\bigl(\mathrm{Sel}^{(n)}(E/K)\bigr) = \{\rho \in H/\partial R^\times \mid \mathrm{res}_v(\rho) \in \mathrm{im}(w_{2,v} \circ \delta_v) \text{ for all places } v \text{ of } K\}\,.$$

Proposition 2.1 is valid over any field of characteristic not dividing n; in particular, it can be applied over K_v to find $\mathrm{im}(w_{2,v} \circ \delta_v)$. In [34] there is a discussion of how to compute images under local descent maps, which applies *mutatis mutandis* to the situation at hand. This gives the following result.

Theorem 2.2. *Let K be a number field, E/K an elliptic curve, and $n \geq 2$. There is an algorithm that computes $\mathrm{Sel}^{(n)}(E/K)$. It is efficient if we assume that the primes of bad reduction of E and the class and unit groups of the number fields $K(\{T_1, T_2\})$ are known, where $\{T_1, T_2\}$ runs through unordered pairs of n-torsion points of E.*

Proof. Compare Theorem 2.4 in [37] and Proposition A.15 and Theorem A.16 in [4]. Note that we can replace $H/\partial R^\times$ by a finite group that encodes the local conditions for all places outside a suitable finite set $\mathcal{S}$ in an efficient way if we know the class and unit groups of the relevant number fields. □

As it stands, this result is rather theoretical, since the number fields that occur are in most cases too large for practical computations: as mentioned earlier, when n is a prime p, then usually there is a component of $\mathrm{Sym}^2_K(R)$ that is a field extension of degree $(p^2-1)(p^2-p)/2$ over K. Even when $n = 3$ and this degree is 24, this makes unconditional computation of the class group nearly impossible in reasonable time with currently available implementations. However, when n is a prime, there is a better alternative, which we describe next.

2.3. **Computation of the Selmer group: Using w_1.** There is a group homomorphism (recalled from [10])

$$w_1 \colon H^1(K, E[n]) \to R^\times/(R^\times)^n\,,$$

which is obtained by applying cohomology to the exact sequence

$$0 \longrightarrow E[n] \xrightarrow{w} \mu_n(\overline{R}) \xrightarrow{\partial} \partial(\mu_n(\overline{R})) \longrightarrow 0\,. \tag{1}$$

It is shown in [16] and [34] that when n is a prime p, the map w_1 is injective for any field K of characteristic different from p, and in [34] a description of the image is given.

We now give an explicit description of the composition $w_1 \circ \delta$. For $T \in E[n]$, let $F_T \in \overline{K}(E)^\times$ denote the function with divisor $n(T) - n(O)$, scaled to have leading coefficient 1 in its Laurent expansion at O with respect to the parameter x/y. We can again package the F_T together in one function $F \in R(E)^\times$. In the same way as discussed earlier for r, F induces a homomorphism

$$\widetilde{F} \colon E(K) \cong \mathrm{Pic}^0(E/K) \longrightarrow R^\times/(R^\times)^n\,.$$

We then have the following well-known fact (see for example [33] or [37]).

Proposition 2.3. *The composition $w_1 \circ \delta \colon E(K) \to R^\times/(R^\times)^n$ is given by $\widetilde{F}$.*

The functions F_T can be evaluated at a given point using Miller's algorithm [29], which follows the computation of nT and keeps track of the functions r_{T_1,T_2} witnessing the intermediate sums; it is not necessary to compute an expression for F_T in terms of the coordinates on a Weierstraß equation of E, which will be quite complicated when n is large. In practice, however, even moderately large n quickly make computations infeasible, so n will be rather small, and it is no problem to work with an explicit expression for F_T as a function. Such an expression is also helpful for computing ε as defined by (7) below.

We now assume that K is a number field. For a place v of K, we denote the canonical map $R^\times/(R^\times)^n \to R_v^\times/(R_v^\times)^n$ by res_v. The maps corresponding to δ and w_1 that we obtain by working over K_v are denoted by δ_v and $w_{1,v}$. If n is prime, and hence w_1 and all $w_{1,v}$ are injective, then the n-Selmer group can be realised as an abstract group via

$$\operatorname{Sel}^{(n)}(E/K) \cong R(\mathcal{S}, n) \cap \operatorname{im}(w_1) \cap \bigcap_{v\in\mathcal{S}} \operatorname{res}_v^{-1}\bigl(\operatorname{im}(w_{1,v}\circ\delta_v)\bigr)\,;$$

see [34]. Here $\mathcal{S}$ is the finite set of places of K specified in Step (1) below. Then $R(\mathcal{S}, n) \subset R^\times/(R^\times)^n$ is the subgroup of elements α unramified outside $\mathcal{S}$, i.e., such that the extension $R[\sqrt[n]{\alpha}]/R$ of étale algebras is unramified outside $\mathcal{S}$.

Theorem 2.4. *Let K be a number field, E/K an elliptic curve and p a prime number. There is a practical algorithm that computes $\operatorname{Sel}^{(p)}(E/K)$, given knowledge of the primes of bad reduction for E and of the class groups and units of the number fields $K(T)$, where T runs through points of order p on E.*

Proof. The algorithm proceeds in the following steps (see [34]).

(1.) Let $\mathcal{S}$ be the set of places v of K that divide p or such that the Tamagawa number of E/K_v is divisible by p, together with the real places of K when $p = 2$.

(2.) Construct the étale algebra R.

(3.) Compute an explicit representation of $R_1 = R(\mathcal{S}, p) \cap \operatorname{im}(w_1)$.

(4.) For each $v \in \mathcal{S}$ construct $R_v^\times/(R_v^\times)^p$, together with the homomorphism $\operatorname{res}_v\colon R(\mathcal{S}, p) \to R_v^\times/(R_v^\times)^p$, and find $\widetilde{F}(E(K_v)) \subset R_v^\times/(R_v^\times)^p$.

(5.) Compute $\operatorname{Sel}^{(p)}(E/K)$ as

$$R_1 \cap \bigcap_{v\in\mathcal{S}} \operatorname{res}_v^{-1}\bigl(\widetilde{F}(E(K_v))\bigr) \subset R(\mathcal{S}, p)\,. \qquad \square$$

2.4. **Changing algebras.** For the purpose of constructing explicit models of n-coverings representing the various elements of the n-Selmer group, we need to represent the Selmer group elements by elements $\rho \in H$. So after computing $\operatorname{Sel}^{(p)}(E/K)$ as in Theorem 2.4, we need to convert the elements $\alpha \in R^\times$ we obtain as representatives into elements $\rho \in H$. Note that for this purpose it is helpful to choose a small representative for the class of α up to nth powers, by applying the method in [19, Section 2] over each constituent field of R.

Recall that H is the subgroup of elements $\rho \in \operatorname{Sym}_K^2(R)^\times$ satisfying

$$\rho(T_1, T_2 + T_3)\rho(T_2, T_3) = \rho(T_1, T_2)\rho(T_1 + T_2, T_3) \text{ for all } T_1, T_2, T_3 \in E[n]. \tag{2}$$

Lemma 2.5. *Let $\alpha \in R^\times$ represent an element in the image of w_1, i.e., we have $\alpha\cdot(R^\times)^n = w_1(\xi)$ for some $\xi \in H^1(K, E[n])$. Then there exists $\rho \in H$ satisfying*

$$\alpha(T) = \textstyle\prod_{i=0}^{n-1} \rho(T, iT) \qquad \textit{for all } T \in E[n]. \tag{3}$$

Then we also have $\partial\alpha = \rho^n$ and $\rho \cdot \partial R^\times = w_2(\xi')$ for some $\xi' \in H^1(K, E[n])$ with $w_1(\xi) = w_1(\xi')$.

Proof. This is [10, Lemma 3.8]. □

To convert α to ρ we first extract an nth root of $\partial\alpha$ in $\mathrm{Sym}^2_K(R)$. We then multiply by an nth root of unity in $\mathrm{Sym}^2_K(R)$ to find ρ satisfying (2) and (3). The simplest case, which occurs frequently in practice, is when $\mathrm{Sym}^2_K(R)$ contains no non-trivial nth roots of unity. There is then a unique choice of ρ. In general we can avoid checking all the conditions in (2) by determining in advance the number of solutions for ρ.

Definition 2.6. Let Γ be the group (under pointwise operations) of all maps $\gamma\colon E[n] \to \mu_n$ satisfying

$$\frac{\gamma(\sigma T_1)\gamma(\sigma T_2)}{\gamma(\sigma(T_1+T_2))} = \sigma\left(\frac{\gamma(T_1)\gamma(T_2)}{\gamma(T_1+T_2)}\right)$$

for all $\sigma \in G_K$ and $T_1, T_2 \in E[n]$.

Let $G \cong \mathrm{Gal}(K(E[n])/K)$ be the subgroup of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ describing the action of G_K on $E[n]$. The action of G_K on μ_n is given by the determinants of these matrices. Hence Γ depends only on G. Indeed, given generators for G, it is easy to compute Γ using linear algebra over $\mathbb{Z}/n\mathbb{Z}$. The following lemma shows that the number of solutions for ρ in Lemma 2.5 is $\#\partial\Gamma = (\#\Gamma)/n^2$.

Lemma 2.7. (i) *There is an exact sequence of abelian groups:*

$$0 \longrightarrow E[n] \xrightarrow{w} \Gamma \xrightarrow{\partial} \partial\Gamma \longrightarrow 0.$$

(ii) $\partial\Gamma = \{\rho \in H : \prod_{i=0}^{n-1} \rho(T, iT) = 1$ *for all* $T \in E[n]\}$.

Proof. (i) Since $\Gamma \subset \mu_n(\overline{R})$, this is obtained by restricting the exact sequence (1). We note that if $\gamma \in w(E[n])$, then $\gamma\colon E[n] \to \mu_n$ is a group homomorphism and so clearly $\gamma \in \Gamma$.

(ii) By [10, Corollary 3.6] every $\rho \in H$ can be written as $\rho = \partial\gamma$ for some $\gamma \in \overline{R}^\times$. We note that if $\rho = \partial\gamma$, then

$$\prod_{i=0}^{n-1} \rho(T, iT) = \gamma(T)^n.$$

Hence the group on the right of (ii) consists of elements $\partial\gamma$ where γ belongs to $\mu_n(\overline{R}) = \mathrm{Map}(E[n], \mu_n)$ and $\partial\gamma\colon E[n] \times E[n] \to \mu_n$ is Galois equivariant. From Definition 2.6, we recognise this group as $\partial\Gamma$. □

Lemma 2.8. *The kernel of $w_1\colon H^1(K, E[n]) \to R^\times/(R^\times)^n$ is isomorphic to*

$$(\partial(\mu_n(\overline{R})))^{G_K}/\partial(\mu_n(R)) = \partial\Gamma/\partial(\mu_n(R)).$$

Proof. This is seen by taking Galois cohomology of the short exact sequence (1) and recalling that w_1 is the composite of $w_*\colon H^1(K, E[n]) \to H^1(K, \mu_n(\overline{R}))$ and an isomorphism $H^1(K, \mu_n(\overline{R})) \cong R^\times/(R^\times)^n$. □

In the case $n = p$ is prime, we know that w_1 is injective. Then by Lemma 2.8 each of the $\#\partial\Gamma$ possibilities for ρ represent the same element of $H/\partial R^\times$. The lemma also gives a formula for $\#\partial\Gamma$. Writing dim for the dimension of a $\mathbb{Z}/p\mathbb{Z}$-vector space we have

$$\dim \partial\Gamma = \dim \partial(\mu_p(R)) = \dim \mu_p(R) - \dim E(K)[p].$$

For general n we can use Lemma 2.8 to check whether w_1 is injective. For example, if $n = 4$ and $E/\mathbb{Q}$ is the elliptic curve $y^2 = x^3 + x + 2/13$, then it can be shown that w_1 is not injective. See [12, Section 2.4] for details.

3. Algorithms in outline: Geometry

Let $C_\xi \to E$ be the n-covering corresponding to some $\xi \in H^1(K, E[n])$. We show how to find an explicit model for C_ξ as a genus one normal curve, first of degree n^2 in $\mathbb{P}^{n^2-1}$ (see Section 3.1) and then of degree n in $\mathbb{P}^{n-1}$(see Section 3.2).

3.1. Initial equations for the covering curves.

One approach would be to start with $\alpha \in R^\times$ representing ξ. However, as explained in [12, Section 2.5], this does not work so well. Instead, we start with $\rho \in H$ representing ξ. By Proposition 2.1 we have $w_2 \circ \delta = \widetilde{r}$. The K-rational points on C_ξ should map to the points in $E(K)$ whose image under δ is ξ, so whose image under $\widetilde{r}$ is $w_2(\xi) = \rho\,\partial R^\times$. We can therefore define our covering curve using the relation $r(P) = \rho\,\partial z$ with $z \in R^\times$. Considering the component at $\{O, O\}$, we see that $z_O := z(O) = 1$. Homogenising, this reads as

$$C_\rho = \{(P, z) \in E \times \mathbb{P}(R) : r(P) z_O \Delta(z) = \rho \cdot (z \otimes z)\} \subset E \times \mathbb{P}(R)\,, \tag{4}$$

where $\mathbb{P}(R)$ is the projective space over K associated to the K-vector space R. The covering map $C_\rho \to E$ is given by projection to the first factor. Note that the equation in (4) is quadratic in z. Over $\overline{K}$, in terms of the coordinates $z_T := z(T)$ for $T \in E[n]$, the equations read

$$r_{T_1,T_2}(P) z_O z_{T_1+T_2} = \rho(T_1, T_2) z_{T_1} z_{T_2}$$

with $T_1, T_2 \in E[n]$. It is shown in [11] that projecting to $\mathbb{P}(R)$, which is equivalent to eliminating $P \in E$, gives $n^2(n^2-3)/2$ linearly independent quadrics defining $C_\rho \subset \mathbb{P}(R) \cong \mathbb{P}^{n^2-1}$ as a genus one normal curve of degree n^2.

The equations for $C_\rho \subset \mathbb{P}(R)$ are obtained from

$$(X - x_T) z_O^2 - \rho(T, -T) z_T z_{-T} \tag{5}$$

for $T \in E[n] \setminus \{O\}$ and

$$(\Lambda_T - \lambda(T_1, T_2)) z_O z_T - \rho(T_1, T_2) z_{T_1} z_{T_2} \tag{6}$$

for $T_1, T_2, T \in E[n] \setminus \{O\}$ with $T_1 + T_2 = T$, by taking differences to eliminate the indeterminates X and Λ_T. In fact the equations recorded in [11, Proposition 3.7] are these differences.

3.2. Improved equations for the covering curves.

Suppose $\rho \in H$ represents an element $\xi \in H^1(K, E[n])$ with trivial obstruction, as defined in [10, 11], for example a Selmer group element $\xi \in \mathrm{Sel}^{(n)}(E/K)$. In the previous section we showed how to write the covering curve C_ρ as a curve of degree n^2 in $\mathbb{P}^{n^2-1}$. We now want to write it as a curve of degree n in $\mathbb{P}^{n-1}$. We sketch how to do this using the Segre embedding method, as described in [10, Section 5.3] and [11].

Recall from Section 2.3 that we fixed the scaling of the functions F_T with divisor $n(T) - n(O)$ so that each has leading coefficient 1 when expanded as a Laurent series in the local parameter x/y at O. Then we define $\varepsilon \in (R \otimes_K R)^\times$ by

$$\varepsilon(T_1, T_2) = \frac{F_{T_1+T_2}(P)}{F_{T_1}(P)F_{T_2}(P - T_1)}, \tag{7}$$

which is independent of $P \in E$, compare Step 2 on p. 154 in [10]. This formula for ε is discussed further in Section 7. Let $*_{\varepsilon\rho}$ be the new multiplication on R defined by

$$z_1 *_{\varepsilon\rho} z_2 = \mathrm{Tr}(\varepsilon\rho \cdot (z_1 \otimes z_2)) .$$

Then the *obstruction algebra* $A_\rho = (R, +, *_{\varepsilon\rho})$ is a central simple algebra over K of dimension n^2. Since we are assuming that ρ represents an element with trivial obstruction we have $A_\rho \cong \mathrm{Mat}_n(K)$. In Section 6 we discuss how to find such an isomorphism explicitly.

Recall that we have equations for $C_\rho \subset \mathbb{P}(R)$. Since R and A_ρ have the same underlying vector space, and we have now trivialised the obstruction algebra, we get $C_\rho \subset \mathbb{P}(\mathrm{Mat}_n)$. We project C_ρ away from the identity matrix onto the hyperplane of trace zero matrices. As shown in [11], the result is a curve $\widetilde{C}$ lying in the locus of rank 1 matrices. In other words, the inclusion of this curve in $\mathbb{P}(\mathrm{Mat}_n)$ factors via the Segre embedding

$$\mathbb{P}^{n-1} \times (\mathbb{P}^{n-1})^\vee \to \mathbb{P}(\mathrm{Mat}_n) .$$

Projecting onto a row or column gives either the degree-n curve $C \to \mathbb{P}^{n-1}$ we are looking for, or its dual $C \to (\mathbb{P}^{n-1})^\vee$, which is a curve of degree $n^2 - n$.

Writing $z \in R = K \times L$ as $z = (z_O, z')$, the projection to the subspace of trace-zero matrices corresponds to eliminating z_O from the equations. We note that if $T_1 + T_2 = T_1' + T_2' = T$ and $\{T_1, T_2\} \neq \{T_1', T_2'\}$, then $\lambda(T_1, T_2) \neq \lambda(T_1', T_2')$. Assuming $n \geq 3$, it is clear by (5) and (6) that eliminating z_O by linear algebra will reduce the dimension of the vector space of quadrics by exactly n^2. So after trivialising the algebra we have $n^2(n^2 - 5)/2$ quadrics that are a basis for the space of quadrics vanishing on

$$\widetilde{C} \subset \mathbb{P}(\mathrm{Tr} = 0) \cong \mathbb{P}^{n^2-2} .$$

Together with the quadrics that are a product of a linear form and the trace form, these span the space of quadrics vanishing on

$$\widetilde{C} \subset \mathbb{P}(\mathrm{Mat}_n) \cong \mathbb{P}^{n^2-1}.$$

Lemma 3.1. *Let $C \subset \mathbb{P}^{n-1}$ be a genus one normal curve with homogeneous ideal $I(C) \subset K[x_1, \ldots, x_n]$. Let $\widetilde{C}$ be the image of the map $C \to \mathbb{P}^{n-1} \times (\mathbb{P}^{n-1})^\vee \to \mathbb{P}(\mathrm{Mat}_n)$ with homogeneous ideal $I(\widetilde{C}) \subset K[z_{11}, z_{12}, \ldots, z_{nn}]$. If $f \in K[x_1, \ldots, x_n]$ is a homogeneous form, then*

$$f(x_1, \ldots, x_n) \in I(C) \iff f(z_{11}, z_{21}, \ldots, z_{n1}) \in I(\widetilde{C}) .$$

Proof. This is clear since the dual curve spans $(\mathbb{P}^{n-1})^\vee$. □

The quadrics vanishing on $C \subset \mathbb{P}^{n-1}$ may now be computed by linear algebra. If $n \geq 4$, then these quadrics define C. In fact they generate the homogeneous ideal; see for example [30]. When $n = 3$ the equation for C is a ternary cubic. In Section 4 we explain how this too may be computed using linear algebra.

4. Application to 3-descent

We give further details of our algorithms in the case $n = 3$. Let E be an elliptic curve over a number field K. We fix an isomorphism $E[3] \cong (\mathbb{Z}/3\mathbb{Z})^2$, say $T_{ij} \mapsto (i,j)$, and let $T = T_{11}$. We assume that the Galois action on $E[3]$ is generic, in the sense that $\rho_{E,3} \colon G_K \to \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$ is surjective[2]. Then there is a tower of number fields

$$\begin{tikzcd}
M = K(E[3]) \arrow[d, dash, "2"] \\
M^+ \arrow[d, dash, "3"] \\
L = K(T) \arrow[d, dash, "2"] \\
L^+ \arrow[d, dash, "4"] \\
K
\end{tikzcd}$$

where M^+ is the subfield of M fixed by $T_{ij} \mapsto T_{ji}$ and L^+ is the subfield of L fixed by $\sigma \colon T \mapsto -T$. We write $\iota_{ij} \colon L \to M$ for the embedding given by $T \mapsto T_{ij}$. Thus ι_{11} is the natural inclusion and $\iota_{ij} \circ \sigma = \iota_{-i,-j}$.

There are two orbits for the action of G_K on $E[3]$, with representatives O and T, and six orbits for the action of G_K on $E[3] \times E[3]$, with representatives

$$(O,O),\ (T,O),\ (O,T),\ (-T,-T),\ (T,-T),\ (T_{10},T_{01})$$

chosen so that each pair sums to either O or T. Using these representatives we identify $R = K \times L$ and, writing $r = (r_1, r_2)$, $s = (s_1, s_2)$ with $r_1, s_1 \in K$, $r_2, s_2 \in L$,

$$\begin{aligned} R \otimes_K R &\cong K \times L \times L \times L \times L \times M \\ r \otimes s &\mapsto (r_1 s_1, r_2 s_1, r_1 s_2, \sigma(r_2)\sigma(s_2), r_2 \sigma(s_2), \iota_{10}(r_2)\iota_{01}(s_2)) . \end{aligned} \tag{8}$$

The comultiplication $\Delta \colon R \to R \otimes_K R$ is given by

$$(r_1, r_2) \mapsto (r_1, r_2, r_2, r_2, r_1, r_2)$$

and the trace map $\mathrm{Tr} \colon R \otimes_K R \to R$ by

$$(a, b_1, b_2, b_3, b_4, c) \mapsto \big(a + \mathrm{Tr}_{L/K}(b_4), b_1 + b_2 + b_3 + \mathrm{Tr}_{M/L}(c)\big) . \tag{9}$$

In Section 2.3 we showed how to compute $\alpha = (1, a) \in R^\times$ representing an element of $\mathrm{Sel}^{(3)}(E/K)$. We now compute

$$u = \sqrt[3]{a\sigma(a)}, \qquad v = \sqrt[3]{\iota_{10}(a)\iota_{01}(a)/a},$$

by extracting cube roots in L^+ and M^+. Since $\det \rho_{E,3}$ is the cyclotomic character, these fields have no non-trivial cube roots of unity. Hence u and v are uniquely determined. The elements ε and ρ in $R \otimes_K R$ are defined by

$$\begin{aligned} \varepsilon &= (1,1,1,1,1,e_3(T_{10},T_{01})), \\ \rho &= (1,1,1,\sigma(a)/u, u, v), \end{aligned} \tag{10}$$

[2] If $K = \mathbb{Q}$, then there are exactly 8 possibilities for $\mathrm{im}(\rho_{E,3})$ up to conjugacy. Our MAGMA implementation relies on a similar analysis of all 8 cases. In three of these cases the group $\partial\Gamma$ in Section 2.4 is non-trivial.

where $e_3 \colon E[3] \times E[3] \to \mu_3$ is the Weil pairing. The reader is warned that this ε is different from the one given in (7). We explain how to correct for this in Section 7. The sign convention we use for the Weil pairing does matter, but is not worth fixing here since we can correct for it later if necessary.

Let $u_1, \ldots, u_8$ be a basis for L over K. In Section 5 we describe how to make a good choice of basis. Then R has basis $r_1, \ldots, r_9$ where $r_1 = (1,0)$ and $r_{i+1} = (0, u_i)$. Structure constants $c_{ijk} \in K$ for the obstruction algebra $A = (R, +, *_{\varepsilon\rho})$ are now given by

$$\operatorname{Tr}(\varepsilon\rho \cdot (r_i \otimes r_j)) = \textstyle\sum_{k=1}^{9} c_{ijk} r_k.$$

The c_{ijk} are computed using the formulae (8), (9) and (10). Since α represents a Selmer group element we know that $A_\rho \cong \operatorname{Mat}_3(K)$. In Section 6 we show how to find such an isomorphism explicitly. In other words, we find (non-zero) matrices $M_1, \ldots, M_9 \in \operatorname{Mat}_3(K)$ satisfying

$$M_i M_j = \textstyle\sum_{k=1}^{9} c_{ijk} M_k. \tag{11}$$

We fix a Weierstraß equation $y^2 = x^3 + ax + b$ for E and let $T = (x_T, y_T)$. The tangent line to E at T has slope $\lambda_T = \lambda(T,T) = (3x_T^2 + a)/(2y_T)$. We define linear forms in indeterminates $z_1, \ldots, z_8$,

$$\begin{aligned} z_T &= \textstyle\sum_{i=1}^{8} u_i z_i, & z_{10} &= \textstyle\sum_{i=1}^{8} \iota_{10}(u_i) z_i, \\ z_{-T} &= \textstyle\sum_{i=1}^{8} \sigma(u_i) z_i, & z_{01} &= \textstyle\sum_{i=1}^{8} \iota_{01}(u_i) z_i, \end{aligned}$$

where $u_1, \ldots, u_8$ is our basis for L over K. Let Q_1 and Q_2 be the quadrics with coefficients in L^+ and M^+ defined by

$$\begin{aligned} Q_1(z_0, \ldots, z_8) &= x_T z_0^2 + \rho_5 z_T z_{-T}, \\ Q_2(z_0, \ldots, z_8) &= (\lambda_T + \kappa_T) z_0 z_T - \rho_4 z_{-T}^2 + \rho_6 z_{10} z_{01}, \end{aligned}$$

where the ρ_i are the components of ρ, and $\kappa_T = \frac{1}{3}(\iota_{10}(\lambda_T) + \iota_{01}(\lambda_T) - \lambda_T)$. Writing each coefficient in terms of fixed K-bases for L^+ and M^+, we obtain $[L^+ : K] = 4$ quadrics from Q_1 and $[M^+ : K] = 24$ quadrics from Q_2. In [10] these are called the quadrics of types I and II. We choose our basis for L^+ so that its first element is 1, and ignore the first type I quadric. The result is 27 quadrics in $K[z_0, \ldots, z_8]$.

Lemma 4.1. *These* 27 *quadrics generate the homogeneous ideal of the degree* 9 *curve* $C_\rho \subset \mathbb{P}(R) = \mathbb{P}^8$.

Proof. Let $v_1 = 1, v_2, v_3, v_4$ be a basis for L^+ over K. We write

$$x_T z_0^2 + \rho(T, -T) z_T z_{-T} = \textstyle\sum_{i=1}^{4} v_i q_i(z_0, \ldots, z_8)$$

where $q_1, \ldots, q_4 \in K[z_0, \ldots, z_8]$. Then (5) becomes

$$\begin{aligned} X &= q_1(z_0, \ldots, z_8), \\ 0 &= q_i(z_0, \ldots, z_8) \qquad \text{for } i = 2, 3, 4. \end{aligned}$$

We eliminate X by ignoring the first quadric q_1.

Next we take $(T_1, T_2) = (T_{10}, T_{01})$ and $(-T, -T)$ in (6). Subtracting to eliminate Λ_T gives the quadric

$$(\lambda(T_{10}, T_{01}) - \lambda(-T, -T)) z_0 z_T - \rho(-T, -T) z_{-T}^2 + \rho(T_{10}, T_{01}) z_{10} z_{01}.$$

Assuming that

$$\lambda(T_{10}, T_{01}) = \tfrac{1}{3}\big(\lambda(T_{10}, T_{10}) + \lambda(T_{01}, T_{01}) - \lambda(T, T)\big) \tag{12}$$

this is precisely the quadric Q_2. To complete the proof we note that (12) is a special case of the following lemma. □

Lemma 4.2. *Let $T_1, T_2, T_3 \in E[3] \setminus \{O\}$ with $T_1 + T_2 + T_3 = O$. Then*

$$\lambda(T_1, T_2) = \tfrac{1}{3} \sum_{i=1}^{3} \lambda(T_i, T_i).$$

Proof. Let $f = y - \lambda x - \nu$ be the equation of the chord through T_1, T_2 and T_3 and $f_i = y - \lambda_i x - \nu_i$ the equation of the tangent line at T_i. As rational functions on E we have $f_1 f_2 f_3 = f^3$. Expanding as power series in the local parameter x/y at O it follows that $\lambda = \frac{1}{3}(\lambda_1 + \lambda_2 + \lambda_3)$ as required. □

The remainder of the algorithm is the same for all Galois actions on $E[3]$. As specified in Section 3.2, we intersect the above space of quadrics with $K[z_1, \ldots, z_8]$ to leave an 18-dimensional space of quadrics defining the projection of $C_\rho \subset \mathbb{P}(R) = \mathbb{P}^8$ to $\mathbb{P}(L) = \mathbb{P}^7$. In other words, we eliminate the monomials $z_0 z_i$ by linear algebra. We then make the following changes of coordinates:

- A change of coordinates corresponding to pointwise multiplication by the “fudge factor” $1/y_T \in L$ (relative to the basis $u_1, \ldots, u_8$). This is to make up for the fact that the definitions of ε in (7) and (10) are different. We explain this further in Section 7.
- A change of coordinates corresponding to the trivialisation of the obstruction algebra.

We now have 18 quadrics in variables z_{ij} where $1 \le i, j \le 3$. These coordinates correspond to the standard basis for $\mathrm{Mat}_3(K)$.

Lemma 4.3. *Substituting $z_{ij} = x_i y_j$ gives a basis for the space of $(2,2)$-forms vanishing on the image of $C \to \mathbb{P}^2 \times (\mathbb{P}^2)^\vee$.*

Proof. We start with a basis for the 18-dimensional space of quadrics vanishing on $\widetilde{C} \subset \mathbb{P}(\mathrm{Tr} = 0)$. This may be identified with the space of quadrics vanishing on $\widetilde{C} \subset \mathbb{P}(\mathrm{Mat}_3)$ that are “singular at I_3”. A quadric is “singular at I_3” if when we write it relative to a basis for $\mathrm{Mat}_3(K)$ with first basis vector I_3, the first variable does not appear. Substituting $z_{ij} = x_i y_j$ gives a surjective linear map Φ from the 45-dimensional space of quadrics in $z_{11}, \ldots, z_{33}$ to the 36-dimensional space of $(2,2)$-forms in x_1, x_2, x_3 and y_1, y_2, y_3. The kernel is spanned by the 2×2 minors of the matrix (z_{ij}) and is a complement to the space of quadrics “singular at I_3”. Thus Φ induces an isomorphism between the space of quadrics vanishing on $\widetilde{C} \subset \mathbb{P}(\mathrm{Tr} = 0)$ and the space of $(2,2)$-forms vanishing on the image of $C \to \mathbb{P}^2 \times (\mathbb{P}^2)^\vee$. □

We multiply each of the forms constructed in Lemma 4.3 by the x_i to obtain 54 forms of bidegree $(3,2)$. The following lemma shows that there is a ternary cubic f, unique up to scalars, such that $y_1^2 f(x_1, x_2, x_3)$ belongs to the span of these 54 forms. Moreover, f is the equation of the curve $C \subset \mathbb{P}^2$ we are looking for.

Lemma 4.4. *Let $C \subset \mathbb{P}^2$ be a non-singular plane cubic with equation $f = 0$. Let V be the space of $(2,2)$-forms vanishing on the image of $C \to \mathbb{P}^2 \times (\mathbb{P}^2)^\vee$. Then $y_1^2 f(x_1, x_2, x_3)$ is a $(3,2)$-form in the ideal generated by V. Moreover, this is the only such polynomial up to scalars.*

Proof. By Euler's identity $3f = \sum x_i \frac{\partial f}{\partial x_i}$ we have

$$3y_1^2 f = x_2 y_1 g_{12} + x_3 y_1 g_{13} + \tfrac{\partial f}{\partial x_1} y_1 \ell. \tag{13}$$

where $\ell = \sum_{i=1}^3 x_i y_i$ and $g_{ij} = y_i \frac{\partial f}{\partial x_j} - y_j \frac{\partial f}{\partial x_i}$ are bihomogeneous forms vanishing on the image of $C \to \mathbb{P}^2 \times (\mathbb{P}^2)^\vee$. Exactly as in the proof of Lemma 3.1, the uniqueness statement follows from the fact that the dual curve spans $(\mathbb{P}^2)^\vee$. □

Lemma 4.4 allows us to compute the ternary cubic f by linear algebra. If we had made the wrong choice of sign for the Weil pairing, then the matrices M_i in (11) would be the transposes of the desired ones; switching the roles of the x_i and y_j corrects for this.

Our implementation in MAGMA over $K = \mathbb{Q}$ finishes by minimising and reducing the ternary cubic as described in [13]. The covering map, computed using the classical formulae in [1], is also returned.

5. A good basis for the obstruction algebra

The obstruction algebra $A_\rho = (R, +, *_{\varepsilon\rho})$ was defined in Section 3.2. In the case $K = \mathbb{Q}$ we explain how to choose a $\mathbb{Q}$-basis for R so that the structure constants for A_ρ are small integers. This is useful for the later parts of our algorithm, for example, when trivialising the obstruction algebra as described in the next section.

We recall that R is a product of number fields. Its ring of integers $\mathcal{O}_R$ is the product of the rings of integers of these fields. A fractional ideal in R is just a tuple of fractional ideals, one for each field, and a prime ideal is a tuple where one component is a prime ideal, and all other components are unit ideals.

Let $\alpha \in R^\times$ represent $w_1(\xi)$ for some $\xi \in H^1(\mathbb{Q}, E[n])$. We write $(\alpha) = \mathfrak{b}\mathfrak{c}^n$ where $\mathfrak{b}$ is integral and nth power free. We then choose as our $\mathbb{Q}$-basis for R a $\mathbb{Z}$-basis for $\mathfrak{c}^{-1}$ that is LLL-reduced with respect to the inner product

$$\langle z_1, z_2 \rangle = \sum_{T \in E[n]} |\alpha(T)|^{2/n} z_1(T) \overline{z_2(T)}, \tag{14}$$

where the bar denotes complex conjugation. In the remainder of this section we explain why this is a good choice. Notice that in defining the inner product we have implicitly fixed an embedding $\overline{\mathbb{Q}} \subset \mathbb{C}$.

We restrict to the case n is odd, say $n = 2m - 1$, and take for ε the square root of the Weil pairing, i.e., $\varepsilon(S,T) = e_n(S,T)^m$. This is also the choice we made in Section 4 for $n = 3$. See Section 7 for a discussion of the possible choices for ε and their relation. By definition of w_1 (see [10, Section 3]) there exists $\gamma \in \overline{R}^\times$ with $\gamma^n = \alpha$ and $w(\xi_\sigma) = \sigma(\gamma)/\gamma$ for all $\sigma \in G_{\mathbb{Q}}$. Then $w_2(\xi) = \rho\, \partial R^\times$ where $\rho = \partial\gamma \in (R \otimes R)^\times$.

Lemma 5.1. *The structure constants for A_ρ with respect to a $\mathbb{Z}$-basis for $\mathfrak{c}^{-1}$ are integers, i.e., $(\mathfrak{c}^{-1}, +, *_{\varepsilon\rho}) \subset A_\rho$ is an order.*

Proof. Let $\mathfrak{p}$ be a prime of R. Put $r = \operatorname{ord}_\mathfrak{p}(\mathfrak{b})$ and $q = \operatorname{ord}_\mathfrak{p}(\mathfrak{c})$ so that $\operatorname{ord}_\mathfrak{p}(\alpha) = qn + r$ with $0 \le r < n$. Let $z_1, z_2 \in \mathfrak{c}^{-1}$. Then $\operatorname{ord}_\mathfrak{p}(z_i) \ge -q$ for $i = 1, 2$. Extending $\operatorname{ord}_\mathfrak{p}$ to $\overline{R}^\times$ and recalling that $\gamma^n = \alpha$, we have $\operatorname{ord}_\mathfrak{p}(\gamma z_i) \ge 0$. Then

$$\begin{aligned} z_1 *_{\varepsilon\rho} z_2 &= \operatorname{Tr}(\varepsilon\rho \cdot (z_1 \otimes z_2)) \\ &= \gamma^{-1} \operatorname{Tr}(\varepsilon \cdot (\gamma z_1 \otimes \gamma z_2)). \end{aligned}$$

Since $\varepsilon \in R \otimes_K R$ is integral and the trace map $\mathrm{Tr}\colon R \otimes_K R \to R$ preserves integrality we deduce $\mathrm{ord}_{\mathfrak{p}}(z_1 *_{\varepsilon\rho} z_2) \geq -(qn+r)/n$. Since this valuation is an integer we must therefore have $\mathrm{ord}_{\mathfrak{p}}(z_1 *_{\varepsilon\rho} z_2) \geq -q$. Repeating for all primes $\mathfrak{p}$ of R it follows that $z_1 *_{\varepsilon\rho} z_2 \in \mathfrak{c}^{-1}$ as required. □

Recall that we fixed an embedding $\overline{\mathbb{Q}} \subset \mathbb{C}$, and write $E[n]$ for $E[n](\overline{\mathbb{Q}}) = E[n](\mathbb{C})$. Let $\tau \in G_{\mathbb{Q}}$ be complex conjugation. Since n is odd we have $H^1(\mathbb{R}, E[n]) = 0$ and so $\tau(\gamma)/\gamma = w(\xi_\tau) = w(\tau(S) - S)$ for some $S \in E[n]$. Therefore, dividing γ by $w(S)$ we may assume that $\gamma\colon E[n] \to \overline{\mathbb{Q}}$ is $G_{\mathbb{R}}$-equivariant. It follows by [10, Lemma 4.6] that pointwise multiplication by γ defines an isomorphism $A_\rho \otimes \mathbb{R} \cong A_1 \otimes \mathbb{R}$.

Let T_1, T_2 be a basis for $E[n]$ with $\overline{T}_1 = T_1$, $\overline{T}_2 = -T_2$ and $e_n(T_1, T_2) = \zeta_n$. We define

$$h(T_1) = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ 1 & 0 & 0 & \cdots & 0 \end{pmatrix}, \quad h(T_2) = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & \zeta_n & 0 & \cdots & 0 \\ 0 & 0 & \zeta_n^2 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & \zeta_n^{n-1} \end{pmatrix},$$

and

$$\begin{array}{rcl} h\colon E[n] & \to & \mathrm{Mat}_n(\mathbb{C}) \\ rT_1 + sT_2 & \mapsto & \zeta_n^{-rs/2} h(T_1)^r h(T_2)^s \end{array}$$

where the exponent of ζ_n is an element of $\mathbb{Z}/n\mathbb{Z}$. It may be verified that

$$h(S)h(T) = \varepsilon(S,T)h(S+T)$$

for all $S, T \in E[n]$. Hence there is an isomorphism $A_1 \otimes \mathbb{C} \cong \mathrm{Mat}_n(\mathbb{C})$ given by $z \mapsto \sum_T z(T)h(T)$. Since this isomorphism respects complex conjugation it restricts to an isomorphism $A_1 \otimes \mathbb{R} \cong \mathrm{Mat}_n(\mathbb{R})$.

Composing the isomorphisms defined in the previous two paragraphs gives a trivialisation of A_ρ over $\mathbb{R}$, i.e.,

$$A_\rho \otimes \mathbb{R} \cong \mathrm{Mat}_n(\mathbb{R})\,; \quad z \mapsto \sum_{T \in E[n]} \gamma(T) z(T) h(T). \tag{15}$$

We use this trivialisation first to compute the discriminant of the order in Lemma 5.1 and then to explain why we chose the inner product (14). The *discriminant* $\mathrm{Disc}(R)$ of R is the product of the discriminants of the constituent fields. The *norm* of $\mathfrak{b} \subset \mathcal{O}_R$ is $\mathrm{Norm}\,\mathfrak{b} = \#(\mathcal{O}_R/\mathfrak{b})$.

Lemma 5.2. *The order $\mathcal{O} = (\mathfrak{c}^{-1}, +, *_{\varepsilon\rho}) \subset A_\rho$ has discriminant*

$$n^{n^2} (\mathrm{Norm}\,\mathfrak{b})^{2/n}\, \mathrm{Disc}(R).$$

Proof. Let $r_1, \ldots, r_{n^2}$ be a $\mathbb{Z}$-basis for $\mathfrak{c}^{-1}$ mapping to matrices $M_1, \ldots, M_{n^2}$ (say) under the trivialisation (15). We write Trd for the reduced trace on A_ρ, as defined in Section 6.1. Then the discriminant of $\mathcal{O}$ is $\mathrm{Disc}(\mathcal{O}) = \det(\mathrm{Trd}(r_i r_j)_{ij}) = \det(\mathrm{Tr}(M_i M_j)_{ij})$. But

$$\mathrm{Tr}(h(S)h(T)) = \begin{cases} n & \text{if } S + T = O, \\ 0 & \text{otherwise.} \end{cases}$$

Noting that $[-1]$ is an even permutation of $E[n]$ we compute

$$\begin{aligned}\operatorname{Disc}(\mathcal{O}) &= \det\big(n \textstyle\sum_{T\in E[n]} \gamma(T) r_i(T)\gamma(-T)r_j(-T)\big)_{i,j} \\ &= n^{n^2} \big(\textstyle\prod_{T\in E[n]} \gamma(T)^2\big)\big(\det(r_i(T))_{i,T}\big)^2.\end{aligned}$$

By considering the basis for $\overline{R} = \operatorname{Map}(E[n], \overline{K})$ consisting of indicator functions it is clear that for $z \in R$ we have $\operatorname{Tr}_{R/\mathbb{Q}}(z) = \sum_T z(T)$ and $N_{R/\mathbb{Q}}(z) = \prod_T z(T)$. Since γ is $G_{\mathbb{R}}$-equivariant we also have $\prod_T \gamma(T) \in \mathbb{R}$. Hence $\prod_T \gamma(T)^2 = |N_{R/\mathbb{Q}}(\alpha)|^{2/n}$ and

$$\big(\det(r_i(T))_{i,T}\big)^2 = \operatorname{Disc}(r_1, \dots, r_{n^2}) = (\operatorname{Norm}\mathfrak{c})^{-2}\operatorname{Disc}(R).$$

Recalling that $(\alpha) = \mathfrak{b}\mathfrak{c}^n$ the result is now clear. □

Remark 5.3. If we start with a Selmer group element, then the discriminant computed in Lemma 5.2 is a product of primes dividing n and primes of bad reduction for E. Indeed, if $\mathfrak{p}$ is a prime of R not dividing any of these primes, then $\operatorname{ord}_{\mathfrak{p}}(\alpha) \equiv 0 \pmod{n}$. The term $\operatorname{Disc}(R)$ is of the stated form by (the easier implication of) the criterion of Néron-Ogg-Shafarevich.

Next we give some justification for our choice of inner product. See also Section 6.5 and the example in Section 8.

Lemma 5.4. *The real trivialisation* (15) *identifies the inner product* (14) *with (a scalar multiple of) the standard Euclidean inner product* $\langle\ ,\ \rangle$ *on* $\operatorname{Mat}_n(\mathbb{R}) \cong \mathbb{R}^{n^2}$.

Proof. Extending $\langle\ ,\ \rangle$ to an inner product on $\operatorname{Mat}_n(\mathbb{C})$ we have

$$\langle h(S), h(T)\rangle = \begin{cases} n & \text{if } S = T, \\ 0 & \text{otherwise.}\end{cases}$$

Therefore, if $z_1, z_2 \in R$ map to $M_1, M_2 \in \operatorname{Mat}_n(\mathbb{R})$, then

$$\begin{aligned}\langle M_1, M_2\rangle &= n \sum_{T\in E[n]} |\gamma(T)|^2 z_1(T)\overline{z_2(T)} \\ &= n \sum_{T\in E[n]} |\alpha(T)|^{2/n} z_1(T)\overline{z_2(T)}.\end{aligned}$$ □

In principle we could now bound the size of the structure constants. But in practice the structure constants are much smaller than these bounds would suggest. We encounter a similar situation at the end of Section 6.

6. Inside the "Black Box": How to trivialise a matrix algebra

Our work on n-descent on elliptic curves requires us to make the Hasse principle explicit. In the case $n = 2$ this means we have to solve a conic in order to represent a 2-Selmer group element as a double cover of $\mathbb{P}^1$ rather than as an intersection of quadrics in $\mathbb{P}^3$. In this section we discuss the general case and, in particular, give an algorithm that is practical when $K = \mathbb{Q}$ and $n = 3$. See [27] for a complexity analysis of our method and its natural generalisation to arbitrary K and n.

6.1. **Central simple algebras.** We recall some standard theory. See for example [38, Part II]. Let K be a field. A central simple algebra A over K is a finite-dimensional algebra over K with centre K and no two-sided ideals (except 0 and A). Wedderburn's Theorem states that A is then isomorphic to a matrix algebra over a division algebra (i.e., skew field) D with centre K. The Brauer group $\mathrm{Br}(K)$ of K is the set of equivalence classes of central simple algebras over K, where A and A' are equivalent if they are matrix algebras over the same division algebra D. The group law is given by tensor product, i.e., $[A]\cdot[A'] = [A \otimes_K A']$, and the inverse of $[A]$ is the class of the opposite algebra A^{op} obtained by reversing the order of multiplication. The identity element is the class of matrix algebras over K.

If A is a central simple algebra over K and L/K is any field extension, then $A_L = A \otimes_K L$ is a central simple algebra over L. The reduced trace and norm are defined as $\mathrm{Trd}(a) = \mathrm{tr}(\varphi(a))$ and $\mathrm{Nrd}(a) = \det(\varphi(a))$ where $\varphi\colon A_{\overline{K}} \cong \mathrm{Mat}_n(\overline{K})$ is an isomorphism of $\overline{K}$-algebras. These definitions are independent of the choice of φ by the Noether-Skolem theorem. Likewise, we define the rank of $a \in A$ to be the rank of $\varphi(a)$.

Now let K be a number field. For each place v of K there is a natural map $\mathrm{Br}(K) \to \mathrm{Br}(K_v)$ given by $[A] \mapsto [A_{K_v}]$. We recall [31, Section 32] that A_{K_v} is a matrix algebra over K_v for all v outside a finite set of places depending on A. It is then one of the main results of class field theory that the map

$$\mathrm{Br}(K) \to \bigoplus_{v \in M_K} \mathrm{Br}(K_v) \tag{16}$$

is injective. Explicitly, this says that a central simple algebra A over K can be *trivialised*, i.e., is isomorphic to a matrix algebra over K, if and only it can be trivialised everywhere locally. In particular, deciding whether a central simple algebra over K can be trivialised is essentially a local problem, given some global information restricting the places to consider to a finite set. The latter usually involves factorisation.

6.2. **Statement of the problem.** The problem we address is rather different. Given a K-algebra A known to be isomorphic to $\mathrm{Mat}_n(K)$, we would like to find such an isomorphism explicitly. More specifically, we want a practical algorithm that takes as input a list of structure constants $c_{ijk} \in K$, giving the multiplication on A relative to a K-basis $\mathbf{a}_1, \ldots, \mathbf{a}_{n^2}$ by the rule

$$\mathbf{a}_i \mathbf{a}_j = \sum_k c_{ijk} \mathbf{a}_k,$$

and returns as output a basis $M_1, \ldots, M_{n^2}$ for $\mathrm{Mat}_n(K)$ satisfying

$$M_i M_j = \sum_k c_{ijk} M_k. \tag{17}$$

The output is far from unique, as we are free to conjugate the M_i by any fixed matrix in $\mathrm{GL}_n(K)$.

6.3. **Zero-divisors.** Let A be a central simple algebra of dimension n^2 over a field K. If n is prime, then by Wedderburn's theorem either $A \cong \mathrm{Mat}_n(K)$ or A is a division algebra. In particular, $A \cong \mathrm{Mat}_n(K)$ if and only if it contains a zero-divisor.

Once we have found a zero-divisor it is easy to find a trivialisation $A \cong \mathrm{Mat}_n(K)$. More generally, i.e., dropping our assumption that n is prime, it is enough to find $x \in A$ of rank r with $(r, n) = 1$. Indeed, as A-modules we have $Ax \cong M^r$ and $A \cong M^n$ where M is the unique faithful simple module. By taking kernels (or cokernels) of sufficiently general A-linear maps we can apply Euclid's algorithm to the dimensions and so explicitly compute M. Since the natural map $A \to \mathrm{End}_K(M) \cong \mathrm{Mat}_n(K)$ is an isomorphism, this gives the required trivialisation of A.

6.4. **Maximal orders.** Let A be a central simple algebra of dimension n^2 over $\mathbb{Q}$. An *order* in A is a subring $\mathcal{O} \subset A$ whose additive group is a free $\mathbb{Z}$-module of rank n^2. Thus a $\mathbb{Q}$-basis $a_1 = 1, a_2, \ldots, a_{n^2}$ for A is a $\mathbb{Z}$-basis for an order $\mathcal{O}$ if and only if the structure constants are integers. We can reduce to this case by clearing denominators. The discriminant of $\mathcal{O}$ is defined as

$$\mathrm{Disc}(\mathcal{O}) = |\det(\mathrm{Trd}(a_i a_j)_{ij})|.$$

A *maximal order* $\mathcal{O} \subset A$ is an order that is not a proper subring of any other order in A. It is shown in [31, Section 25] that all maximal orders in A have the same discriminant, which we denote $\mathrm{Disc}(A)$. Moreover if, for p a prime, $A_{\mathbb{Q}_p} \cong \mathrm{Mat}_{\kappa_p}(D_p)$ where D_p is a division algebra over $\mathbb{Q}_p$ with $[D_p : \mathbb{Q}_p] = m_p^2$, then

$$\mathrm{Disc}(A) = (\prod_p p^{(m_p - 1)\kappa_p})^n. \tag{18}$$

By the injectivity of (16) it follows that $A \cong \mathrm{Mat}_n(\mathbb{Q})$ if and only if $\mathrm{Disc}(A) = 1$ and $A_\mathbb{R} \cong \mathrm{Mat}_n(\mathbb{R})$. In fact, we can dispense with the real condition, in view of the description of the image of (16) also given by class field theory.

It is well known that every maximal order in $\mathrm{Mat}_n(\mathbb{Q})$ is conjugate to $\mathrm{Mat}_n(\mathbb{Z})$. By computing a maximal order our original problem (in the case $K = \mathbb{Q}$) is reduced to the following: given structure constants for a ring known to be isomorphic to $\mathrm{Mat}_n(\mathbb{Z})$, find such an isomorphism explicitly.

6.5. **Lattice reduction.** Let $L \subset \mathbb{R}^m$ be a lattice and suppose L is spanned by the rows of an m by m matrix B. Then $\det L = |\det B|$ depends only on L and not on B. By the geometry of numbers, L contains a non-zero vector x with

$$||x||^2 \leq c(\det L)^{2/m}$$

where c is a constant depending only on m. Here, $||x|| = (\sum_{i=1}^m x_i^2)^{1/2}$ is the usual Euclidean norm. The best possible value of c is called Hermite's constant and denoted γ_m. Blichfeldt [2] has shown that

$$\gamma_m^m \leq \left(\frac{2}{\pi}\right)^m \Gamma\left(1 + \frac{m+2}{2}\right)^2. \tag{19}$$

Let A be a central simple algebra over $\mathbb{Q}$ of dimension n^2. For $n \in \{3, 5\}$ the following argument gives a direct proof that if $A_{\mathbb{Q}_p} \cong \mathrm{Mat}_n(\mathbb{Q}_p)$ for all primes p, then $A \cong \mathrm{Mat}_n(\mathbb{Q})$. This should be viewed as generalising the geometry of numbers proof of the Hasse principle for conics over $\mathbb{Q}$. First, let $\mathcal{O}$ be a maximal order in A. Since n is odd we may trivialise A over the reals, and hence identify $\mathcal{O}$ as a subring of $\mathrm{Mat}_n(\mathbb{R})$. We identify $\mathrm{Mat}_n(\mathbb{R}) = \mathbb{R}^{n^2}$ in the obvious way. Then

$$\mathrm{Disc}(\mathcal{O}) = (\det B)^2\,\mathrm{Disc}(\mathrm{Mat}_n(\mathbb{Z}))$$

where B is an n^2 by n^2 matrix whose rows are a basis for $\mathcal{O}$. Our local assumptions show by (18) that $\mathrm{Disc}(\mathcal{O}) = 1$. Since $\mathrm{Disc}(\mathrm{Mat}_n(\mathbb{Z})) = 1$ it follows that $\det \mathcal{O} = |\det B| = 1$. Hence by the geometry of numbers there is a non-zero matrix $M \in \mathcal{O} \subset \mathrm{Mat}_n(\mathbb{R})$ with $||M||^2 \leq \gamma_{n^2}$. Blichfeldt's bound (19) gives

$$\gamma_9 \leq \frac{2}{\pi}\left(\frac{12!}{2^{12}6!}\sqrt{\pi}\right)^{2/9} \approx 2.24065,$$

$$\gamma_{25} \leq \frac{2}{\pi}\left(\frac{28!}{2^{28}14!}\sqrt{\pi}\right)^{2/25} \approx 4.29494.$$

Hence $||M||^2 < n$. Applying the Gram Schmidt algorithm to the columns of M, we can write $M = QR$ where Q is orthogonal and R is upper triangular, say with diagonal entries $r_1, \ldots, r_n$. Then by the AM-GM inequality

$$|\det M|^{2/n} = (\prod_{i=1}^{n} r_i^2)^{1/n} \leq \tfrac{1}{n}\sum_{i=1}^{n} r_i^2 \leq \tfrac{1}{n}||R||^2 = \tfrac{1}{n}||M||^2 < 1.$$

But $\det M$ is the reduced norm of an element of $\mathcal{O}$, and therefore an integer. Hence $\det M = 0$, i.e., M is a zero-divisor. As we have seen, this implies that $A \cong \mathrm{Mat}_n(\mathbb{Q})$ (recall that n is prime).

This proof suggests the following algorithm. Starting with a $\mathbb{Q}$-algebra A, known to be isomorphic to $\mathrm{Mat}_n(\mathbb{Q})$, we perform the following steps.

- Compute a maximal order $\mathcal{O} \subset A$. See, for example, [26], [32], [23], or the MAGMA implementation by de Graaf.
- Trivialise A over the reals. In practice (for n odd) we split the algebra by a number field of odd degree, and then take a real embedding.
- Use the real trivialisation to embed $\mathcal{O}$ as a lattice in $\mathrm{Mat}_n(\mathbb{R}) \cong \mathbb{R}^{n^2}$. Then compute an LLL-reduced basis for $\mathcal{O}$.
- Search through small linear combinations of the basis elements of $\mathcal{O}$ until we find an element with reducible minimal polynomial. If n is prime we can then compute a trivialisation as described in Section 6.3.

In practice for $n \in \{3, 5\}$ the first basis vector of $\mathcal{O}$ is a zero-divisor, and so no searching is required in the final stage. The bounds in the LLL-algorithm are, unfortunately, not quite strong enough to prove this. In the case $n = 3$ we were able to rectify this by proving an analogue of Hunter's theorem [25], [7, Theorem 6.4.2]. We omit the details. For general n the algorithm still finds a basis for A with respect to which the structure constants are small integers, and is therefore worth applying before attempting any other method (for example using norm equations).

We give some theoretical justification for the last remark. Suppose $\mathcal{O} \subset \mathrm{Mat}_n(\mathbb{R})$ has basis $M_1, \ldots, M_{n^2}$. As observed above, the n^2 by n^2 matrix B whose ith row contains the entries of M_i has determinant 1. So by Cramer's rule the structure constants, defined by (17), satisfy

$$|c_{ijk}| \leq ||M_i M_j|| \prod_{s \neq k} ||M_s||. \tag{20}$$

The LLL algorithm bounds $\prod_{i=1}^{n^2} ||M_i||$ by a constant depending only on n. So either $||M_i|| < \sqrt{n}$ for some i, in which case we have found a zero-divisor, or the $||M_i||$ are bounded by a constant depending only on n. In this latter case, by (20) and the fact $||M_i M_j|| \leq ||M_i|| \cdot ||M_j||$, the structure constants are also bounded by a constant depending only on n. These constants turn out to be rather large, but fortunately, the method works much better in practice.

7. Projecting to the rank 1 locus

In this section we explain the "fudge factor" $1/y_T$ used in our description (see Section 4) of the Segre embedding method in the case $n = 3$.

Let E/K be an elliptic curve. We write $\tau_P \colon E \to E$ for translation by $P \in E$. The *theta group* of level n for E is

$$\Theta_E = \{(f, T) \in \overline{K}(E)^\times \times E[n] : \operatorname{div}(f) = \tau_T^*(n(O)) - n(O)\}$$

with group law

$$(f_1, T_1) * (f_2, T_2) = (\tau_{T_2}^*(f_1)f_2, T_1 + T_2).$$

It sits in an exact sequence

$$0 \longrightarrow \mathbb{G}_{\mathrm{m}} \xrightarrow{\alpha} \Theta_E \xrightarrow{\beta} E[n] \longrightarrow 0$$

where the structure maps α and β are given by $\alpha \colon \lambda \mapsto (\lambda, O)$ and $\beta \colon (f, T) \mapsto T$. The commutator is given by the Weil pairing, i.e., $xyx^{-1}y^{-1} = \alpha e_n(\beta x, \beta y)$ for all $x, y \in \Theta_E$.

The construction of the obstruction algebra depends on an element $\varepsilon \in (R \otimes_K R)^\times$. In [10] it is shown that we can take

$$\varepsilon(T_1, T_2) = \frac{\phi(T_1)\phi(T_2)}{\phi(T_1 + T_2)} \tag{21}$$

where $\phi \colon E[n] \to \Theta_E$ is any Galois equivariant set-theoretic section for β. This element has the property that

$$\varepsilon(T_1, T_2)\varepsilon(T_2, T_1)^{-1} = e_n(T_1, T_2). \tag{22}$$

If we change ϕ by multiplying by an element $z \in R^\times$, viewed as a map $E[n] \to \overline{K}^\times$, then ε is multiplied by ∂z. It is shown in [10, Lemma 4.6] that this does not change the obstruction algebra (up to isomorphism).

Theorem 7.1. *For $T \in E[n]$ let $F_T \in \overline{K}(E)$ be the rational function with divisor $n(T) - n(O)$, scaled as specified in Section 2.3. Let $\varepsilon \in (R \otimes_K R)^\times$ be as defined in (7), and let $e \in (R \otimes_K R)^\times$ be the Weil pairing. If n is odd, say $n = 2m - 1$, then $e^m = \varepsilon\,\partial u$ where $u \in R^\times$ is defined by $u(O) = 1$ and $u(T) = -1/F_T(mT)$ for $T \in E[n] \setminus \{O\}$.*

Proof. One choice of ϕ is to take

$$\phi(T) = (F_T, -T)^{-1} = (\tau_T^*(1/F_T), T).$$

Then

$$\begin{aligned}\phi(T_1)\phi(T_2) &= (\tau_{T_1}^*(1/F_{T_1}), T_1) * (\tau_{T_2}^*(1/F_{T_2}), T_2) \\ &= (\tau_{T_1+T_2}^*(1/F_{T_1})\tau_{T_2}^*(1/F_{T_2}), T_1 + T_2) \\ &= \frac{\tau_{T_1+T_2}^*(F_{T_1+T_2})}{\tau_{T_1+T_2}^*(F_{T_1})\tau_{T_2}^*(F_{T_2})}\phi(T_1 + T_2).\end{aligned}$$

By (21) this gives the formula (7) for ε. We recall from [10, Section 3] that when n is odd, say $n = 2m - 1$, an alternative choice of ε, suggested by (22), is

$$\varepsilon(T_1, T_2) = e_n(T_1, T_2)^m. \tag{23}$$

This choice of ε corresponds to choosing ϕ so that $\iota(\phi(T)) = \phi(T)^{-1}$ and $\phi(T)^n = 1$ for all $T \in E[n]$, where $\iota\colon \Theta_E \to \Theta_E$ is the involution $(f, T) \mapsto (f \circ [-1], -T)$. Indeed, applying the involution ι to

$$\phi(T_1)\phi(T_2) = \varepsilon(T_1, T_2)\phi(T_1 + T_2)$$

gives

$$\phi(T_1)^{-1}\phi(T_2)^{-1} = \varepsilon(T_1, T_2)\phi(T_1 + T_2)^{-1}$$

and so

$$e_n(T_1, T_2) = \phi(T_1)\phi(T_2)\phi(T_1)^{-1}\phi(T_2)^{-1} = \varepsilon(T_1, T_2)^2$$

as required.

The formulae (7) and (23) differ by ∂u where $u \in R^\times$ satisfies

$$\begin{aligned} \iota(u(T)F_T, -T) &= (u(T)F_T, -T)^{-1}, \\ (u(T)F_T, -T)^n &= 1, \end{aligned}$$

equivalently,

$$u(T)^2 F_T(P)F_T(T - P) = 1, \tag{24}$$

$$u(T)^n \textstyle\prod_{i=0}^{n-1} F_T(P + iT) = 1, \tag{25}$$

where $P \in E$ is arbitrary, subject to avoiding the zeros and poles of these functions. Taking $P = mT$ in (24) gives

$$u(T) = \pm 1/F_T(mT).$$

What matters for the application of Theorem 7.1 is that the sign here is independent of $T \in E[n] \setminus \{O\}$. If Galois acts transitively on $E[n] \setminus \{O\}$, then this is already clear. In general we use (25) and the following lemma.

Lemma 7.2. *Let $n \geq 3$ be an odd integer and $O \neq T \in E[n]$ a point of order r. Then the rational function*

$$g_i\colon P \mapsto F_T(P + iT)F_T(P + (1 - i)T)$$

satisfies

$$g_i(O) = \begin{cases} u(T)^{-2} & \text{if } i \not\equiv 0, 1 \pmod{r}, \\ -u(T)^{-2} & \text{if } i \equiv 0, 1 \pmod{r}. \end{cases}$$

Proof. By (24) the rational function

$$h_i\colon P \mapsto F_T(-P + iT)F_T(P + (1 - i)T)$$

is constant with value $u(T)^{-2}$. If $i \not\equiv 0, 1 \pmod{r}$, then g_i and h_i take the same value at $P = O$. If $i \equiv 0, 1 \pmod{r}$, then an extra minus sign arises since F_T has a pole of odd order at O. Indeed, expanding F_T as a power series in $t = x/y$ about O, it is clear that the rational function $P \mapsto F_T(-P)/F_T(P)$ takes value -1 at $P = O$. □

To compute the product in (25) we put $P = O$ in

$$\prod_{i=0}^{n-1} F_T(P + iT) = F_T(P + mT) \prod_{i=1}^{m-1} g_i(P)$$

and use Lemma 7.2. Since n/r is odd if follows that $u(T) = -1/F_T(mT)$ for all $T \in E[n] \setminus \{O\}$. □

If $n = 3$, then relative to the Weierstraß equation $y^2 = x^3 + ax + b$ we have

$$F_T(x, y) = (y - y_T) - \lambda_T(x - x_T)$$

where λ_T is the slope of the tangent line at $T = (x_T, y_T)$. Therefore,

$$u(T) = -1/F_T(-T) = 2/y_T.$$

In Section 3.2, following [11], we took ε given by (7). In Sections 4 and 5 we took ε given by (23). This difference does not matter when computing the obstruction algebra, but it does matter when we subsequently compute equations using the Segre embedding method. For instance, if we used the wrong ε then it would not be true (after projection to the trace zero subspace) that we get a curve in the rank 1 locus of $\mathbb{P}(\mathrm{Mat}_n)$. In view of [10, Lemma 4.6] the situation is remedied by multiplying by the factor $u(T)$. Here we use the usual pointwise multiplication in R. In Section 4 we used the factor $1/y_T$. The constant 2, or indeed any scalar in $K^\times$, can be ignored since the scalar matrices act trivially on projective space.

8. Example

We illustrate our work by using it to compute some explicit elements of order 3 in the Tate-Shafarevich group of an elliptic curve. See the MAGMA file stored with the arXiv version of this paper [12] for further details of the calculations. Other applications of our work are discussed in the introduction and at the end of this section.

Let $E/\mathbb{Q}$ be the elliptic curve

$$y^2 + xy = x^3 + x^2 - 1154x - 15345$$

labelled 681b1 in [9]. This curve has generic 3-torsion in the sense that the map $\rho_{E,3}\colon G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$ is surjective. We work with the Weierstraß equation $y^2 = x^3 + a_4x + a_6$ where $a_4 = -1496259$ and $a_6 = -693495810$. Relative to this Weierstraß equation a 3-torsion point is given by $T = (x_T, y_T)$ where

$$x_T = 12u^6 - 36u^2 + 2115, \quad y_T = -2820u^7 - 144u^5 + 16920u^3 - 662268u,$$

and u is a root of $f(X) = X^8 - 6X^4 + 235X^2 - 3$. The slope of the tangent line at T is $\lambda_T = (3x_T^2 + a_4)/(2y_T) = -3u^7 + 15u^3 - 705u$.

Using the algorithm in [34] (a summary is given in Section 2.3) we find that $\mathrm{Sel}^{(3)}(E/\mathbb{Q}) \cong (\mathbb{Z}/3\mathbb{Z})^2$. One of the non-trivial elements is represented by

$$a = \tfrac{1}{18}(u^6 - u^4 - 9u^3 - 5u^2 - 27u - 3).$$

In this example we find the corresponding plane cubic.

Let $L = \mathbb{Q}(u)$ and $M = L(v)$ where v is a root of

$$g(X) = \frac{f(X)}{X^2 - u^2} = X^6 + u^2X^4 + (u^4 - 6)X^2 + u^6 - 6u^2 + 235.$$

We also put $L^+ = \mathbb{Q}(u^2)$ and $M^+ = L(v^2)$. Let σ and τ be the automorphisms generating $\mathrm{Gal}(L/L^+)$ and $\mathrm{Gal}(M/M^+)$. The polynomial $f(X)$ splits over M with roots $\pm u$, $\pm v$, $\pm u_{10}$ and $\pm u_{01}$. There are embeddings $\iota_{10}\colon L \to M$ and $\iota_{01}\colon L \to M$ given by $u \mapsto u_{10}$ and $u \mapsto u_{01}$. We choose u_{10} and u_{01} so that $\tau(u_{10}) = u_{01}$ and $\iota_{10}(T) + \iota_{01}(T) = T$.

Following the description in Section 4 we put

$$R = \mathbb{Q} \times L \quad \text{and} \quad R \otimes R = \mathbb{Q} \times L \times L \times L \times L \times M.$$

Then $\alpha = (1, a)$ and $\rho = (1, 1, 1, \sigma(a)/s, s, t/s)$ where $s = -u^2$ and

$$\begin{aligned} t = {} & \tfrac{1}{486}(u^7 - u^5 - 5u^3 - 27u^2 + 240u - 27)v^4 \\ & + \tfrac{1}{486}(-2u^7 + 2u^5 - 27u^4 + 10u^3 - 237u + 27)v^2 \\ & + \tfrac{1}{162}(-u^7 - 9u^6 + u^5 + 86u^3 + 54u^2 - 240u + 45). \end{aligned}$$

We put $\varepsilon = (1, 1, 1, 1, 1, \zeta_3)$ where $\zeta_3 \in M$ is a primitive cube root of unity. It is not worth recording our choice of ζ_3 since a different choice only has the effect of reversing the order of multiplication in the obstruction algebra.

The basis for L as a $\mathbb{Q}$-vector space suggested in Section 5 is

$$\begin{aligned} u_1 &= 1, \\ u_2 &= \tfrac{1}{3}(-u^7 + 6u^3 - 235u), \\ u_3 &= \tfrac{1}{18}(80u^7 - 9u^6 + u^5 - 481u^3 + 54u^2 + 18795u - 2124), \\ & \vdots \\ u_7 &= \tfrac{1}{54}(97u^7 - 9u^6 + 2u^5 - 584u^3 + 63u^2 + 22785u - 2133), \\ u_8 &= \tfrac{1}{54}(462u^7 - 53u^6 + 6u^5 - u^4 - 2769u^3 + 319u^2 + 108549u - 12423). \end{aligned}$$

Then R has basis $r_1, \dots, r_9$ where $r_1 = (1, 0)$ and $r_{i+1} = (0, u_i)$. Let A be the obstruction algebra $(R, +, *_{\varepsilon\rho})$ with basis $\mathbf{a}_1, \dots, \mathbf{a}_9$ corresponding to $r_1, \dots, r_9$. Then $\mathbf{a}_1$ is the identity, and left multiplication by $\mathbf{a}_2$ is given by

$$\begin{aligned} \mathbf{a}_2^2 &= -3\mathbf{a}_3 - 3\mathbf{a}_5 - 3\mathbf{a}_6, \\ \mathbf{a}_2\mathbf{a}_3 &= 2\mathbf{a}_2 + 3\mathbf{a}_3 + 3\mathbf{a}_8, \\ & \vdots \\ \mathbf{a}_2\mathbf{a}_8 &= 7\mathbf{a}_2 - 3\mathbf{a}_3 + 9\mathbf{a}_4 - 3\mathbf{a}_8, \\ \mathbf{a}_2\mathbf{a}_9 &= -3\mathbf{a}_1 + 4\mathbf{a}_2 + 3\mathbf{a}_3 - 3\mathbf{a}_5 + 6\mathbf{a}_6 - 3\mathbf{a}_7 + 3\mathbf{a}_8. \end{aligned}$$

We do not record the full table of structure constants, but note that the above sample is typical in that most entries are single digit integers. The basis vectors $\mathbf{a}_i$ have minimal polynomials

$$\begin{gathered} X - 1,\ X^3 + 162,\ X^3 - 12X - 227,\ X^2,\ X^3 - 12X - 470,\ X^3 - 12X - 470, \\ X^3 - 147X - 367,\ X^3 - 201X + 1307,\ X^3 + 123X + 254. \end{gathered}$$

Notice that $\mathbf{a}_4$ is a zero-divisor, so in this example it is particularly easy to find a trivialisation.

The discriminant of L is $3^{11} \cdot 227^4$ and the ideal generated by a is a cube. The order with basis the $\mathbf{a}_i$ has discriminant $|\det(\mathrm{Trd}(\mathbf{a}_i\mathbf{a}_j))| = 3^{20} \cdot 227^4$ as predicted by Lemma 5.2. A basis for a maximal order in A is given by

$$\begin{aligned}
\mathbf{b}_1 &= \tfrac{1}{3}(\mathbf{a}_1 + 56\mathbf{a}_6 + 126\mathbf{a}_7 + 101\mathbf{a}_8 + 2438\mathbf{a}_9),\\
\mathbf{b}_2 &= \tfrac{1}{2043}(3\mathbf{a}_2 + 38\mathbf{a}_4 + 471\mathbf{a}_5 + 95432\mathbf{a}_6 + 50049\mathbf{a}_7 + 75876\mathbf{a}_8 + 1408079\mathbf{a}_9),\\
\mathbf{b}_3 &= \tfrac{1}{2043}(\mathbf{a}_3 + 167\mathbf{a}_4 + 543\mathbf{a}_5 + 175106\mathbf{a}_6 + 57658\mathbf{a}_7 + 87258\mathbf{a}_8 + 1872296\mathbf{a}_9),\\
\mathbf{b}_4 &= \tfrac{1}{9}(\mathbf{a}_4 + 529\mathbf{a}_6 + 2041\mathbf{a}_9),\\
\mathbf{b}_5 &= \tfrac{1}{3}(\mathbf{a}_5 + 159\mathbf{a}_6 + 105\mathbf{a}_7 + 160\mathbf{a}_8 + 2802\mathbf{a}_9),\\
\mathbf{b}_6 &= \tfrac{1}{3}(\mathbf{a}_6 + \mathbf{a}_9),\\
\mathbf{b}_7 &= \tfrac{1}{3}(\mathbf{a}_7 + 8\mathbf{a}_9),\\
\mathbf{b}_8 &= \tfrac{1}{3}(\mathbf{a}_8 + 8\mathbf{a}_9),\\
\mathbf{b}_9 &= \mathbf{a}_9
\end{aligned}$$

with minimal polynomials

$$\begin{aligned}
&X^3 - X^2 + 67882988X + 153570178243,\ X^3 + 46000395X + 93752525874,\\
&X^3 + 80434914X + 198363227932,\ X^3 + 4444433X + 1099577331,\\
&X^3 + 84844655X + 243745052250,\ X^3 - 3X,\\
&X^3 + 725X + 3507,\ X^3 + 671X + 9393,\ X^3 + 123X + 254.
\end{aligned}$$

In defining the $\mathbf{b}_i$ we have not made use of the fact the $\mathbf{a}_i$ are already LLL-reduced with respect to a real trivialisation. The simplest way to correct for this is to run LLL on the rows of the change of basis matrix. So instead of the $\mathbf{b}_i$ we consider the basis

$$\begin{aligned}
\mathbf{b}'_1 &= \tfrac{1}{2043}(-12\mathbf{a}_2 - 63\mathbf{a}_3 - 4\mathbf{a}_4 - 73\mathbf{a}_6 + 18\mathbf{a}_7 + 8\mathbf{a}_9),\\
\mathbf{b}'_2 &= \tfrac{1}{2043}(-81\mathbf{a}_2 - 28\mathbf{a}_3 - 27\mathbf{a}_4 + 18\mathbf{a}_6 + 8\mathbf{a}_7 + 54\mathbf{a}_9),\\
&\ \vdots\\
\mathbf{b}'_8 &= \tfrac{1}{2043}(-36\mathbf{a}_2 + 37\mathbf{a}_3 + 48\mathbf{a}_4 + 138\mathbf{a}_5 - 81\mathbf{a}_6 - 173\mathbf{a}_7 - 90\mathbf{a}_8 + 24\mathbf{a}_9),\\
\mathbf{b}'_9 &= \tfrac{1}{2043}(-681\mathbf{a}_1 - 27\mathbf{a}_2 - 85\mathbf{a}_3 - 9\mathbf{a}_4 + 6\mathbf{a}_6 - 73\mathbf{a}_7 + 18\mathbf{a}_9)
\end{aligned}$$

with minimal polynomials

$$X^2,\ X^2,\ X^2,\ X^3 - X,\ X^3 - X,\ X^3,\ X^3 - X,\ X^3 - X,\ X^2 + X.$$

Now every vector in our basis is a zero-divisor! Recall that to find a trivialisation we only needed to find one zero-divisor. Using the method in Section 6.3 we find a trivialisation:

$$\begin{array}{lll}
\mathbf{a}_1 \mapsto \begin{pmatrix} 1 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & 1 \end{pmatrix} & \mathbf{a}_2 \mapsto \begin{pmatrix} 6 & -6 & 3\\ 6 & -6 & 0\\ 0 & -9 & 0 \end{pmatrix} & \mathbf{a}_3 \mapsto \begin{pmatrix} -4 & -3 & -3\\ 0 & 2 & -3\\ 9 & -9 & 2 \end{pmatrix}\\
\mathbf{a}_4 \mapsto \begin{pmatrix} 0 & 0 & 0\\ 0 & 0 & 0\\ 12 & 15 & 0 \end{pmatrix} & \mathbf{a}_5 \mapsto \begin{pmatrix} 2 & 3 & 3\\ 0 & -4 & 3\\ 18 & -18 & 2 \end{pmatrix} & \mathbf{a}_6 \mapsto \begin{pmatrix} 2 & 9 & -6\\ 0 & 2 & -6\\ -9 & 9 & -4 \end{pmatrix}\\
\mathbf{a}_7 \mapsto \begin{pmatrix} -5 & 3 & 3\\ 0 & -11 & 3\\ -9 & -9 & 16 \end{pmatrix} & \mathbf{a}_8 \mapsto \begin{pmatrix} 1 & -12 & 3\\ -12 & -8 & 3\\ -9 & 9 & 7 \end{pmatrix} & \mathbf{a}_9 \mapsto \begin{pmatrix} 7 & -9 & -3\\ 9 & -11 & 6\\ 15 & -15 & 4 \end{pmatrix}.
\end{array}$$

We recall that $R = \mathbb{Q} \times L$ and L has basis $u_1, \dots, u_8$. The space of quadrics vanishing on the projection of $C_\rho \subset \mathbb{P}(R)$ to $\mathbb{P}(L)$ has basis

$$\begin{aligned}
q_1 &= z_4z_6 - z_5z_6 - z_5z_7 + z_6z_8 + z_7z_8,\\
q_2 &= 2z_1z_6 - z_3z_6 + z_4z_5 + z_5^2 - z_5z_8 - 2z_6z_7 + z_6z_8,\\
q_3 &= -z_1z_6 - z_3z_6 - 2z_4z_5 + z_4z_8 + z_5^2 - z_5z_8 + z_6z_8,\\
&\ \vdots\\
q_{18} &= z_1^2 - z_1z_3 - z_1z_4 + z_1z_5 + 2z_1z_6 - z_1z_7 - z_2z_4 + 2z_2z_5 - 2z_2z_6 - 2z_3^2\\
&\quad + 2z_3z_4 - 2z_3z_5 - z_3z_6 - z_3z_7 + 3z_3z_8 + 2z_4^2 - z_4z_5 + z_4z_6 - 4z_4z_7\\
&\quad - z_4z_8 + z_5z_6 + 3z_5z_7 + z_5z_8 + z_6^2 + 2z_6z_7 + z_6z_8 - z_7^2 - z_8^2.
\end{aligned}$$

Multiplication by the factor $1/y_T \in L$ (relative to the basis $u_1, \dots, u_8$) followed by the above trivialisation, prompts us to substitute

$$\begin{pmatrix} z_1\\ z_2\\ z_3\\ z_4\\ z_5\\ z_6\\ z_7\\ z_8 \end{pmatrix} = \begin{pmatrix} -70 & -54 & 144 & 12 & 86 & 423 & 6 & -48 & -16\\ 360 & 615 & 1128 & -444 & -510 & 663 & -372 & 207 & 150\\ 160 & -180 & -621 & 222 & -257 & 648 & 174 & 291 & 97\\ -75 & -48 & 195 & -195 & 21 & -285 & -69 & -81 & 54\\ 3 & -24 & -267 & 24 & -192 & -21 & 87 & 81 & 189\\ -69 & -81 & -108 & -9 & 57 & -135 & 117 & 36 & 12\\ -105 & -81 & -270 & 18 & 129 & 27 & 9 & -72 & -24\\ 252 & -72 & -801 & 72 & -333 & 423 & 261 & 243 & 81 \end{pmatrix} \begin{pmatrix} z_{11}\\ z_{12}\\ z_{13}\\ z_{21}\\ z_{22}\\ z_{23}\\ z_{31}\\ z_{32}\\ z_{33} \end{pmatrix}.$$

Next we substitute $z_{ij} = x_iy_j$ to give 18 forms of bidegree $(2,2)$. Multiplying each of these by the x_i gives 54 forms of bidegree $(3,2)$. We then solve by linear algebra for the ternary cubic F_1 (unique up to scalars) such that $y_1^2F_1(x_1,x_2,x_3)$ belongs to the span of these forms:

$$F_1(x,y,z) = 3x^3 - 13x^2y + 4x^2z + 2xy^2 + xyz - y^3 - 5y^2z - yz^2 + z^3.$$

This is the ternary cubic corresponding to a. Since $E(\mathbb{Q})/3E(\mathbb{Q}) = 0$ it represents a non-trivial element of $\text{Ш}(E/\mathbb{Q})[3]$. In general, we now minimise and reduce using the algorithms in [13]. However, in this example we find that F_1 is already minimised and close to being reduced.

Repeating for different a we find that the other non-trivial elements of $\text{Ш}(E/\mathbb{Q})[3]$ are represented by

$$\begin{aligned}
F_2(x,y,z) &= x^3 + 6x^2y + 4x^2z + 4xy^2 + 5xyz + 2xz^2 + y^3 - 3y^2z + 7yz^2 + 6z^3,\\
F_3(x,y,z) &= x^3 - 2x^2y - x^2z - 7xyz + 8xz^2 + 4y^3 - 5y^2z + 6yz^2 + z^3,\\
F_4(x,y,z) &= x^3 - 2x^2z + 4xy^2 + 3xyz - 5xz^2 - y^3 + 6y^2z + 2yz^2 + 7z^3.
\end{aligned}$$

We recall that inverses in the 3-Selmer group are represented by the same cubic but with different covering maps. Thus our 3-descent programs return a list of $(3^s-1)/2$ ternary cubics where s is the dimension of the Selmer group as an $\mathbb{F}_3$-vector space.

We have computed equations for all elements of $\text{Ш}(E/\mathbb{Q})[3]$ for all elliptic curves $E/\mathbb{Q}$ of conductor $N_E < 300\,000$. The results can be found on the website [21]. In compiling this list we only ran our programs on the elliptic curves with analytic order of Ш divisible by 3, and did not compute the class groups rigorously. Thus the completeness of our list remains conditional on the Birch–Swinnerton-Dyer conjecture.[3] It is, however, unconditional that every cubic in our list is a counterexample to the Hasse Principle.

Some further examples, illustrating that the kernel of the obstruction map for 3-coverings is not a group, are included in the arXiv version of this paper [12].

References

[1] Sang Yook An, Seog Young Kim, David C. Marshall, Susan H. Marshall, William G. McCallum, and Alexander R. Perlis, *Jacobians of genus one curves*, J. Number Theory **90** (2001), no. 2, 304–315, DOI 10.1006/jnth.2000.2632. MR1858080 (2002g:14040)

[2] H. F. Blichfeldt, *A new principle in the geometry of numbers, with some applications*, Trans. Amer. Math. Soc. **15** (1914), no. 3, 227–235, DOI 10.2307/1988585. MR1500976

[3] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, DOI 10.1006/jsco.1996.0125. Computational algebra and number theory (London, 1993). MR1484478

[4] N. Bruin, B. Poonen and M. Stoll, *Generalized explicit descent and its application to curves of genus 3*, Preprint (2012), arXiv:1205.4456v1 [math.NT]

[5] J. W. S. Cassels, *Arithmetic on curves of genus* 1. *IV. Proof of the Hauptvermutung*, J. Reine Angew. Math. **211** (1962), 95–112. MR0163915 (29 #1214)

[6] J. W. S. Cassels, *Second descents for elliptic curves*, J. Reine Angew. Math. **494** (1998), 101–127, DOI 10.1515/crll.1998.001. Dedicated to Martin Kneser on the occasion of his 70th birthday. MR1604468 (99d:11058)

[7] Henri Cohen, *A course in computational algebraic number theory*, Graduate Texts in Mathematics, vol. 138, Springer-Verlag, Berlin, 1993. MR1228206 (94i:11105)

[8] J.E. Cremona, `mwrank`, part of the `eclib` library. Available at `http://www.warwick.ac.uk/staff/J.E.Cremona/mwrank/`.

[9] J.E. Cremona, *Elliptic Curve Data*. Available at `http://www.warwick.ac.uk/staff/J.E.Cremona/ftp/data/INDEX.html`.

[10] 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), 121–155, DOI 10.1515/CRELLE.2008.012. MR2384334 (2009g:11067)

[11] J. E. Cremona, T. A. Fisher, C. O'Neil, D. Simon, and M. Stoll, *Explicit n-descent on elliptic curves. II. Geometry*, J. Reine Angew. Math. **632** (2009), 63–84, DOI 10.1515/CRELLE.2009.050. MR2544143 (2011d:11128)

[12] J.E. Cremona, T.A. Fisher, C. O'Neil, D. Simon and M. Stoll, *Explicit n-descent on elliptic curves, III Algorithms*, arXiv:1107.3516v2 [math.NT]. This is the preprint version of this paper; it has a more detailed version of Sections 2 and 3, contains more examples and comes with a file that shows how to do the computations for the examples in MAGMA.

[13] John E. Cremona, Tom A. Fisher, and Michael Stoll, *Minimisation and reduction of 2-, 3- and 4-coverings of elliptic curves*, Algebra Number Theory **4** (2010), no. 6, 763–820, DOI 10.2140/ant.2010.4.763. MR2728489 (2012c:11120)

[14] B. Creutz, *Explicit second p-descent on elliptic curves*, Doctoral Thesis, Jacobs University Bremen, 2010. Available at `http://www.jacobs-university.de/phd/files/1283816493.pdf`.

[15] Brendan Creutz and Robert L. Miller, *Second isogeny descents and the Birch and Swinnerton-Dyer conjectural formula*, J. Algebra **372** (2012), 673–701, DOI 10.1016/j.jalgebra.2012.09.029. MR2990032

[16] Z. Djabri, Edward F. Schaefer, and N. P. Smart, *Computing the p-Selmer group of an elliptic curve*, Trans. Amer. Math. Soc. **352** (2000), no. 12, 5583–5597, DOI 10.1090/S0002-9947-00-02535-6. MR1694286 (2001b:11047)

[17] Claus Fieker and Damien Stehlé, *Short bases of lattices over number fields*, Algorithmic number theory, Lecture Notes in Comput. Sci., vol. 6197, Springer, Berlin, 2010, pp. 157–173, DOI 10.1007/978-3-642-14518-6_15. MR2721419 (2012d:11247)

[3] However, for curves of rank 0 and 1 and conductor < 5000 the verification of the full BSD conjecture has recently been completed by B. Creutz and R.L. Miller [15].

[18] Tom Fisher, *Finding rational points on elliptic curves using 6-descent and 12-descent*, J. Algebra **320** (2008), no. 2, 853–884, DOI 10.1016/j.jalgebra.2008.04.007. MR2422319 (2009g:11068)

[19] Tom Fisher, *Some improvements to 4-descent on an elliptic curve*, Algorithmic number theory, Lecture Notes in Comput. Sci., vol. 5011, Springer, Berlin, 2008, pp. 125–138, DOI 10.1007/978-3-540-79456-1_8. MR2467841 (2009m:11078)

[20] T. A. Fisher and G. F. Sills, *Local solubility and height bounds for coverings of elliptic curves*, Math. Comp. **81** (2012), no. 279, 1635–1662, DOI 10.1090/S0025-5718-2012-02587-7. MR2904595

[21] T.A. Fisher, *Elements of order* 3 *in the Tate-Shafarevich group*, online tables at `http://www.dpmms.cam.ac.uk/~taf1000/g1data/order3.html`.

[22] T.A. Fisher, *Explicit 5-descent on elliptic curves*, in ANTS X: Proceedings of the Tenth Algorithmic Number Theory Symposium, San Diego, 2012, Everett W. Howe, Kiran S. Kedlaya (eds.), Open Book Series, Vol. 1. Mathematical Sciences Publishers, Berkeley, 2013.

[23] C. Friedrichs, *Berechnung von Maximalordnungen über Dedekindringen*, Dissertation, Technische Universität Berlin, 2000. Available at `http://opus.kobv.de/tuberlin/volltexte/2001/40/pdf/friedrichs_carsten.pdf`.

[24] Willem A. de Graaf, Michael Harrison, Jana Pílniková, and Josef Schicho, *A Lie algebra method for rational parametrization of Severi-Brauer surfaces*, J. Algebra **303** (2006), no. 2, 514–529, DOI 10.1016/j.jalgebra.2005.06.022. MR2255120 (2007e:14058)

[25] John Hunter, *The minimum discriminants of quintic fields*, Proc. Glasgow Math. Assoc. **3** (1957), 57–67. MR0091309 (19,944b)

[26] Gábor Ivanyos and Lajos Rónyai, *Finding maximal orders in semisimple algebras over* $\mathbf{Q}$, Comput. Complexity **3** (1993), no. 3, 245–261, DOI 10.1007/BF01271370. MR1246219 (95c:11154)

[27] Gábor Ivanyos, Lajos Rónyai, and Josef Schicho, *Splitting full matrix algebras over algebraic number fields*, J. Algebra **354** (2012), 211–223, DOI 10.1016/j.jalgebra.2012.01.008. MR2879232

[28] J. R. Merriman, S. Siksek, and N. P. Smart, *Explicit* 4*-descents on an elliptic curve*, Acta Arith. **77** (1996), no. 4, 385–404. MR1414518 (97j:11027)

[29] Victor S. Miller, *The Weil pairing, and its efficient calculation*, J. Cryptology **17** (2004), no. 4, 235–261, DOI 10.1007/s00145-004-0315-8. MR2090556 (2005g:11112)

[30] David Mumford, *Varieties defined by quadratic equations*, Questions on Algebraic Varieties (C.I.M.E., III Ciclo, Varenna, 1969), Edizioni Cremonese, Rome, 1970, pp. 29–100. MR0282975 (44 #209)

[31] I. Reiner, *Maximal orders*, London Mathematical Society Monographs. New Series, vol. 28, The Clarendon Press Oxford University Press, Oxford, 2003. Corrected reprint of the 1975 original; With a foreword by M. J. Taylor. MR1972204 (2004c:16026)

[32] Lajos Rónyai, *Computing the structure of finite algebras*, J. Symbolic Comput. **9** (1990), no. 3, 355–373, DOI 10.1016/S0747-7171(08)80017-X. MR1056632 (91h:68093)

[33] Edward F. Schaefer, *Computing a Selmer group of a Jacobian using functions on the curve*, Math. Ann. **310** (1998), no. 3, 447–471, DOI 10.1007/s002080050156. MR1612262 (99h:11063)

[34] Edward F. Schaefer and Michael Stoll, *How to do a p-descent on an elliptic curve*, Trans. Amer. Math. Soc. **356** (2004), no. 3, 1209–1231, DOI 10.1090/S0002-9947-03-03366-X. MR2021618 (2004g:11045)

[35] S. Siksek, *Descent on curves of genus one*, Ph.D. thesis, University of Exeter, 1995. Available at `http://hdl.handle.net/10871/8323`.

[36] S. Stamminger, *Explicit 8-descent on elliptic curves*, PhD thesis, International University Bremen, 2005. Available at `http://www.jacobs-university.de/phd/files/1135329284.pdf`.

[37] M. Stoll, *Descent on elliptic curves*, to appear in Panoramas et Synthéses **36**, Société Mathématique de France. Available at `http://www.mathe2.uni-bayreuth.de/stoll/talks/short-course-descent.pdf`.

[38] André Weil, *Basic number theory*, 3rd ed., Springer-Verlag, New York, 1974. Die Grundlehren der Mathematischen Wissenschaften, Band 144. MR0427267 (55 #302)

[39] T.O. Womack, *Explicit descent on elliptic curves*, Ph.D. thesis, University of Nottingham, 2003. Available at `http://www.warwick.ac.uk/staff/J.E.Cremona/theses/womack.pdf`.

Mathematics Institute, University of Warwick, Coventry CV4 7AL, United Kingdom
E-mail address: J.E.Cremona@warwick.ac.uk

University of Cambridge, DPMMS, Centre for Mathematical Sciences, Wilberforce Road, Cambridge CB3 0WB, United Kingdom
E-mail address: T.A.Fisher@dpmms.cam.ac.uk

505 Pulitzer Hall, Columbia University Graduate School of Journalism, 2950 Broadway, New York, New York 10027
E-mail address: cathy.oneil@gmail.com

Université de Caen, Campus II - Boulevard Maréchal Juin, BP 5186–14032, Caen, France
E-mail address: Denis.Simon@math.unicaen.fr

Mathematisches Institut, Universität Bayreuth, 95440 Bayreuth, Germany
E-mail address: Michael.Stoll@uni-bayreuth.de