Explicit descent on elliptic curves, II

Cathy O'Neil

12th July 2005

Let E be an elliptic curve over the perfect field K. For an integer $n \geq 2$, fix an embedding $f : E \to \mathbb{P}^{n-1}$ defined over K given by the divisor $n \cdot O_E$.

As Tom has explained, a typical element of $H^1(K, E[n])$ can be viewed as a diagram of the form $f^\xi : C \to S$ where S is a Brauer-Severi variety of dimension $n-1$. There is no chance therefore to find a model in $\mathbb{P}^{n-1}$ for every element in $H^1(K, E[n])$. There are two basic tricks we will use: First, every element in $H^1(K, E[n])$ has a model in $\mathbb{P}^{n^2-1}$ (look at the obstruction maps with respect to $H^1(K, E[n]) \to H^1(K, E[n^2])$ sending $C \to S \mapsto C \to \mathbb{P}^{n^2-1}$ or, with respenct to divisor classes, $(C, [D]) \mapsto (C, n[D])$), and second, any element of the Selmer group always looks like $C \to \mathbb{P}^{n-1}$. In fact let us denote the subset of $H^1(K, E[n])$ which has $S \cong \mathbb{P}^{n-1}$ by $H_{Ob}(K)$.

Our basic question then is, starting with an element of H_{Ob}, how do we *reverse* the map $C \to \mathbb{P}^{n-1} \mapsto C \to \mathbb{P}^{n^2-1}$?

First, a description of what works over algebraically closed fields. Then, given f as above, there is a notion of a dual curve embedding $f^\vee : E \to (\mathbb{P}^{n-1})^\vee$. Therefore we get a map to the product $\mathbb{P}^{n-1} \times (\mathbb{P}^{n-1})^\vee$. We can compose that map with the Segre embedding to get a map:

$$h : E \to \mathbb{P}^{n-1} \times (\mathbb{P}^{n-1})^\vee \to \mathbb{P}^{n^2-1}.$$

We will prove that g is an embedding of E via the *nearly* full linear series associated to $n^2 \cdot O_E$.

In fact we construct the following commutative diagram:

$$\begin{tikzcd}
x \arrow[rrrr, mapsto] & & & & (a_x : T \mapsto a_T(x)) \\
E \arrow[r, "nO"] \arrow[drrr, "n^2 O"] & \mathbb{P}^{n-1} \times \check{\mathbb{P}}^{n-1} \arrow[r, "\text{Segre}"] & \mathbb{P}(\mathrm{Mat}(n,K)) \cong & \mathbb{P}^{n^2-1} \arrow[r] & \mathbb{P}(\mathcal{R}) \\
& & & \mathbb{P}^{n^2-1} \arrow[u, dotted] &
\end{tikzcd}$$

where $\mathcal{R} = \mathrm{Res}_{R/K}\mathbb{A}^1$, $\mathbb{P}(\mathcal{R}) = (\mathcal{R} \setminus \{0\})/\mathbf{G_m}$. Note that the vertical arrow will be projection away from one coordinate of the n^2-dimensional vector space $\Gamma = \Gamma(E, n^2 \cdot O)$ of global sections of $|n^2 \cdot O|$ on E.

How do we define these functions a_T, and how do we know they are sections of Γ? We use the fact that the image of $E[n]$ generates $\mathrm{Mat}(n, K)$ as a K-vector space under the following map (defined by Tom):

$$\begin{tikzcd}
E[n] \arrow[r] \arrow[ddr] & \mathrm{PGL}_n \\
T \arrow[ddr, mapsto] & \\
& \mathrm{GL}_n \arrow[uu] \\
& M_T
\end{tikzcd}$$

We then define the a_T as the coefficient functions of the M_T for the function h:

$h(x) = \sum_{T \in E[n]} a_T(x) M_{-T}^{-1}$. We can solve for $a_T : n a_T = \mathrm{Tr}(h(x) M_{-T}) = \mathrm{Tr}(X T_X M_{-T}) = \mathrm{Tr}(T_X M_{-T} X) = T_X(X - T)$.

In other words, a_T vanishes on x exactly when the point $x - T$ lies on the hyperosculating plane of x. When $T \neq O$, this means: $a_T = 0 \Leftrightarrow n \cdot x = T$. This implies that $a_T \in \Gamma$ whenever $T \neq O$, and it's not hard (using character theory) to see that the various a_T are independent in Γ. We like to think of the a_T as 'secondary Hessians,' in that they are polynomials of degree n (because the dual map can be seen as coming from the vector space of global sections of $|n \cdot O|^{\otimes(n-1)}$ and because E is a normal curve) in the original embedding $f : E \to \mathbb{P}^{n-1}$ and in that embedding a_T intersects E exactly at the n^2 points Q such that $n \cdot Q = T$.

Note that when $T = O$, the condition that x vanishes on its own tangent line is the empty condition, which is why we project away from the coordinate corresponding to O.

Now for C, we can do almost the same thing:

$$
\begin{tikzcd}
C \arrow[r] & \mathbb{P}^{n-1} \times \check{\mathbb{P}}^{n-1} \arrow[r] \arrow[d, "\cong"'] & \mathbb{P}(\mathrm{Mat}(n, K)) \arrow[d, "\cong"'] & & \\
C \arrow[r] & S \times \check{S} \arrow[r] & \mathbb{P}(A) & \cong & \mathbb{P}(\mathcal{R})
\end{tikzcd}
$$

$$
\begin{tikzcd}
x \arrow[r, mapsto] \arrow[rrd, mapsto] & \sum_T a_T(x) i(-T)^{-1} & \\
& & (a_x : T \mapsto a_T(x))
\end{tikzcd}
$$

Note that Tom also explained that the image of $E[n]$ will generate the central simple algebra associated to $C \to S$ as follows:

$$
\begin{tikzcd}
E[n] \arrow[r] \arrow[dr, "i"'] & A^*/K^* \\
& A^* \arrow[u]
\end{tikzcd}
$$

Therefore we can still define the a_Ts as coefficient functions, now not of matrices but of these distinguished elements of the central simple algebra A. We will again find as above that the a_T are elements of the vector space of global sections of $n|D|$, if $C \to S$ corresponds to the pair $(C, |D|)$.

Now we have carefully defined two maps: one from E to $\mathbb{P}(\mathcal{R})$, and the other from C to $\mathbb{P}(\mathcal{R})$. How are these related? We have:

$$
\begin{tikzcd}
E \arrow[r] \arrow[d] & \mathbb{P}(\mathcal{R}) \arrow[d, "\gamma"'] \\
C \arrow[r] & \mathbb{P}(\mathcal{R}),
\end{tikzcd}
$$

where $\partial\gamma = \rho \in R \otimes R$, $\gamma^n \in R^*/R^{*n}$. This means that we can use the underlying algebra structure of R to literally 'multiply' every point of E to get a point of C. Note that the map 'multiplication by γ' is not K-rational. However, both $\partial\gamma = \rho \in R \otimes R =$ and $\gamma^n \in R^*/R^{*n}$ *are.*

In some sense this means γ is nearly rational, and only differs from an actual rational element of R by an $E[n]$-action.

The Algorithm

So the story is as follows: Say we had actual equations for $E \to \mathbb{P}(\mathcal{R})$. Then we can modify those equations by point-wise multiplication by γ to get equations for C inside $\mathbb{P}(\mathcal{R})$.

Then we project away from the O-coordinate. In the case that $C \to S \cong \mathbb{P}^{n-1}$ (equivalently when we can explicitly compute an isomorphism $A \cong \mathrm{Mat}(n, K)$) we can then project onto the first factor in the above diagram to recover a model for C.

A final ingredient to find the equations for E is to compute the map r, coming from the connecting map in cohomology:

$$\begin{tikzcd}
E(K)/nE(K) \arrow[r] \arrow[dr, "r"] & H^1(K, E[n]) \arrow[d] & \\
P \arrow[dr, mapsto] & H & \subset (R \otimes R)^*/\partial R \\
 & \partial a_Q &
\end{tikzcd}$$

Theorem. $r(P) = \partial a_Q$, where $nQ = P$.

I will not prove this theorem, but I want to mention that we can modify the map r by a scalar (namely divide by a choice of a 'primary Hessian' a_O) and we have the following explicit definition of r:

$r(P)(T_1, T_2) = \frac{a_{T_1}(Q)a_{T_2}(Q)}{a_{T_1+T_2}(Q)a_O(Q)}$

We can now deduce the equations (i.e. a huge bunch of quadrics) defining E by the following *formula*:

$$\{z \in \mathbb{P}(\mathcal{R}) | r(P) = \partial z \text{ for some } P \in E\}$$

Note that this formula is tautological: a point P of E maps to a point in $\mathbb{P}(\mathcal{R})$ via r, so a point in $\mathbb{P}(\mathcal{R})$ lies on E exactly when it's in the image of r. However, the formula can be explicitly written out for any two elements $T_1, T_2 \in E[n](\overline{K})$:

$$r(P)(T_1, T_2) = \partial z(T_1, T_2) = \frac{z(T_1)z(T_2)}{z(T_1 + T_2)}.$$

We now fix $T = T_1 + T_2$ in order to remove the dependency on r and to get quadrics in terms of the $z(T)$'s. We will use:

Claim: $P \mapsto r(P)(T_1, T_2)$ has poles at $P = 0$ and $P = T_1 + T_2 = T$.
Proof. By the explicit formula for r above and the fact that a_T and a_O are Hessians.

Note that the vector space of functions on E with two fixed poles has dimension 2, by Riemann-Roch. Therefore, fix two sets of Ts whose sum is fixed: $T_{11} + T_{12} = T$ and $T_{21} + T_{22} = T$.

Then we have in particular that $r(P)(T_{11}, T_{12})z(T) = z(T_{11})z(T_{12})$ and $r(P)(T_{21}, T_{22})z(T) = z(T_{21})z(T_{22})$. However by the above Claim, for any *other* pair T_1, T_2 whose sum is T, there exist scalars (which we can easily solve for) α and β such that $r(P)(T_1, T_2) = \alpha r(P)(T_{11}, T_{12}) + \beta r(P)(T_{21}, T_{22})$.

Finally we deduce $\alpha z(T_{11})z(T_{12}) + \beta z(T_{21})z(T_{22}) = z(T_1)z(T_2)$.

Hey, look, a quadric! A counting argument will show that we get all of the quadrics defining E inside $\mathbb{P}(\mathcal{R})$. Note that it's actually a tricky point that, once we project away from the O coordinate, that the resulting curve is still defined by quadrics (namely, the quadrics that don't involve the coordinate $z(O)$). This fact was supplied by the algebraic geometer Michnea Popa. Also, note that in the algorithm itself, Michael finds the quadrics in a slightly different (but equivalent) way. Indeed, the above quadrics won't be K-rational but will generate a K-rational vector space of quadrics, which we then know will descend to a K-rational basis. In Michael's algorithm, he goes immediately to the K-rational basis. In fact, he goes straight to the equations for C. From the point of view of explaining, it seems to make more sense to do it this way.

In any case, we now have a bunch of quadrics defining E and we now modify our approach slightly to find equations for C, namely using a modified formula:

$C \to \mathbb{P}(\mathcal{R})$ is the set $\{z \in \mathbb{P}(\mathcal{R}) | r(P) = \rho \partial z = \partial(\gamma z) \text{ for some } P \in E\}$.

Remember, this formula determines the image of C because of the relationship between the two models.

Finally, I'd like to end with a suggested way of looking at what we've done. I'd like to think of the various choices for C as points on some scheme. As we've seen, we can basically represent C by the element γ, which is not quite rational. However, it *is* defined 'up to $E[n]$ action,' or in other words it corresponds to an honest point of the scheme $\mathbb{P}(\mathcal{R})/E[n]$. I claim we should think then of this scheme $\mathbb{P}(\mathcal{R})/E[n]$ as a kind of arithmetic parameter space. Indeed it is an example of what I call a sampling space for the functor $H^1(K, E[n])$, which I will discuss in the next half hour. For now, note that the following diagram commutes, which gives us the impression that this is a natural choice.

$$
\begin{tikzcd}
x \arrow[r, mapsto] & a_x \\
E \arrow[r] \arrow[d] & \mathbb{P}(\mathcal{R}) \arrow[dd] \\
E/E[n] \arrow[d, "\cong"'] & \\
E \arrow[r] \arrow[d, twoheadrightarrow] & \mathbb{P}(\mathcal{R})/E[n] \arrow[d, twoheadrightarrow] \\
E(K)/nE(K) \arrow[r] & H^1(K, E[n]) = H \subset R \otimes R/\partial R
\end{tikzcd}
$$

The diagrams were drawn with Paul Taylor's commutative diagrams package.