Some improvements to 4-descent on an elliptic curve

Tom Fisher
(University of Cambridge)

ANTS VIII 19th May 2008

K a number field (often $K = \mathbb{Q}$)

E/K an elliptic curve

n-covering

$$\begin{tikzcd} C \arrow[d, "\text{(over } \overline{K}\text{)}"', "\cong"] \arrow[dr, "\text{(over } K\text{)}"] & \\ E \arrow[r, "\times n"] & E \end{tikzcd}$$

ELS 4-coverings ELS 2-coverings

$$\begin{tikzcd}[row sep=small] C_4 \arrow[dr] & & \\ C_4' \arrow[r] & C_2 \arrow[ddr] & \\ \vdots & & \\ {} \arrow[r] & C_2' \arrow[r] & E \\ {} \arrow[ur] & C_2'' \arrow[ur] & \\ \vdots & \vdots & \end{tikzcd}$$

$$E(K)[2] \to S^{(2)}(E/K) \to S^{(4)}(E/K) \longrightarrow S^{(2)}(E/K)$$

4-descent developed in PhD theses of

Siksek (1995) $\leftarrow$ see also (Merriman, Siksek, Smart 1996)

Womack (2003) $\leftarrow$ MAGMA implementation

Stamminger (2005) $\leftarrow$ also 8-descent.

Background on 2-descent

$E: \quad y^2 = f(x) \qquad f \in K[x]$ monic, cubic (assume irreducible)

$$L = K(\varphi) = \frac{K[x]}{(f(x))}$$

There is a group homomorphism

$$E(K) \longrightarrow \underbrace{\ker\left(L^*/(L^*)^2 \xrightarrow{N_{L/K}} K^*/(K^*)^2 \right)}_{= H^1(K, E[2])}$$

$$(x,y) \longmapsto x - \varphi$$

To decide whether $\alpha \in L^*$ (representing an element of $H^1(K, E[2])$) comes from $E(K)$, consider

$$x - \varphi = \alpha (u + v\varphi + w\varphi^2)^2$$

The coefficients of φ and φ^2 give equations for a 2-covering

$$\left\{ \begin{array}{l} -t^2 = Q_1(u,v,w) \\ \;\;\; 0 = Q_2(u,v,w) \end{array} \right\} \subset \mathbb{P}^3_{t,u,v,w}$$

Obstruction map

$$\mathrm{Ob}_2 : H^1(K, E[2]) \longrightarrow \mathrm{Br}(K)$$

$$\alpha \longmapsto \left(\begin{array}{c} \text{class of the conic} \\ \{Q_2 = 0\} \end{array} \right)$$

Note $\mathrm{Ob}_2(\alpha) = 0 \iff \alpha (L^*)^2$ contains an element linear in φ.

Good representatives for $K^*/(K^*)^n$

Example $K = \mathbb{Q}(t)$ where $t = \sqrt[3]{7823}$

Fundamental unit $\alpha = a + bt + ct^2$

where $a, b, c \in \mathbb{Z}$ each have $\simeq 1400$ decimal digits

But
$$\begin{aligned}
\alpha &\equiv t^2 - t + 113 && \bmod (K^*)^2 \\
\alpha &\equiv 3 && \bmod (K^*)^3 \\
\alpha &\equiv 9t^2 + 72t + 1359 && \bmod (K^*)^4 \\
\alpha &\equiv 518t^2 - 5922t - 76801 && \bmod (K^*)^5
\end{aligned}$$

How to find good representatives?

"<u>MINIMISE</u>" Write $(\alpha) = \underline{\underline{b}}\, \underline{\underline{c}}^n$

where $\underline{\underline{b}} = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_k^{r_k}$ $\quad 0 < r_i < n$

"<u>REDUCE</u>" Find $\gamma \in \underline{\underline{c}}^{-1}$ that is short

w.r.t. the inner product

$$\langle \gamma, \gamma' \rangle = \sum_{i=1}^{d} |\sigma_i(\alpha)|^{2/n} \sigma_i(\gamma) \overline{\sigma_i(\gamma')}$$

where $\sigma_1, \ldots, \sigma_d : K \hookrightarrow \mathbb{C}$, $\quad [K:\mathbb{Q}] = d$.

Then replace α by $\alpha \gamma^n$

MAGMA function: NiceRepresentativeModuloPowers

Background on 4-descent

Start with a 2-covering (with trivial obstruction)

$C_2 : \quad y^2 = g(x)$ $\qquad g \in K[x]$ quartic, leading coeff a (say) (assume irreducible)

$$F = K(\theta) = \frac{K[x]}{(g(x))}$$

There is a map

$$C_2(K) \longrightarrow \{ \xi \in F^* \mid N_{F/K}(\xi) \equiv a \bmod (K^*)^2 \}$$
$$(x, y) \longmapsto x - \theta$$

To decide whether $\xi \in F^*$ comes from $C_2(K)$ we consider

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

The coefficients of θ^2 and θ^3 give equations for a 4-covering

$$C_4 = \{Q_1 = Q_2 = 0\} \subset \mathbb{P}^3_{x_1, x_2, x_3, x_4}$$

— a quadric intersection (QI)

Remarks

(i) Multiplying ξ by an element of K^* or $(F^*)^2$ gives equivalent QI's

(ii) C_4 ELS $\Longleftrightarrow \xi \in \left(\text{a finite subset of } F^*/K^*(F^*)^2 \right)$

computing this requires knowledge of the class group & units of F.

Testing Equivalence of 4-coverings

$C_2 = \{ y^2 = g(x) \}$ (intermediate 2-covering)

$C_4 = \{ Q_1 = Q_2 = 0 \}$

classical formulae

$\xi \in F^* / (K^*)(F^*)^2$

Given QI's C_4 and C_4'

- Test whether C_2 and C_2' are equivalent (Cremona, 2001)
- If so, C_2 and C_2' determine the same field F. Compute $\xi, \xi' \in F^*$
- Test whether $\xi \equiv \xi' \mod K^*(F^*)^2$

Magma implementation (with $K = \mathbb{Q}$)

IsEquivalent(<Model G1>,<Model G1>)

– if true also returns the transformation in

$$GL_2(\mathbb{Q}) \times GL_4(\mathbb{Q}).$$

K a number field (often $K = \mathbb{Q}$)

E/K an elliptic curve

<u>n-covering</u>

$$\begin{tikzcd} C \arrow[d, "\cong"', "\text{(over } \bar{K}\text{)}"] \arrow[dr, "\text{(over } K\text{)}"] & \\ E \arrow[r, "\times n"] & E \end{tikzcd}$$

ELS 4-coverings   ELS 2-coverings

$$\begin{tikzcd}[row sep=small] C_4 \arrow[dr] & & \\ C_4' \arrow[r] & C_2 \arrow[ddr] & \\ \vdots & & \\ {} \arrow[r] & C_2' \arrow[r] & E \\ {} \arrow[ur] & & \\ \vdots & C_2'' \arrow[uur] & \\ & \vdots & \end{tikzcd}$$

$$E(K)[2] \to S^{(2)}(E/K) \to S^{(4)}(E/K) \longrightarrow S^{(2)}(E/K)$$

<u>Problem</u> Implement the group law on $\underline{S^{(4)}(E/K)}$

Why is this difficult?   representing elements as QI's

A 4-covering $\xi \in H^1(K, E[4])$ can be written as a QI $\Longleftrightarrow$ $\mathrm{Ob}_4(\xi) = 0$

where $\mathrm{Ob}_4 : H^1(K, E[4]) \longrightarrow \mathrm{Br}(K)$ (quadratic map)

Problem Implement the group law on $S^{(4)}(E|K)$

A general method (Cremona, F., O'Neil, Simon, Stoll) developed for 3-descent can be applied provided we can

(i) Compute matrices in $GL_4(\bar{K})$ describing the action of $E[4]$ on $C_4 \subset \mathbb{P}^3$ } see §7

(ii) Given a c.s.a. A over K with $A \cong \mathrm{Mat}_4(K)$ find such an isomorphism explicitly } (Pílniková 2007)

A special case I give a formula for adding 2-Selmer and 4-Selmer elements

$$S^{(2)}(E|K) \subset H^1(K, E[2]) = \ker\left(L^*/(L^*)^2 \xrightarrow{N_{L|K}} K^*/(K^*)^2 \right)$$

$$\{C_2 : y^2 = g(x)\} \longmapsto \alpha$$

$F = K[x]/(g(x))$

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

$$\beta \longmapsto Ob_2(\alpha) + Ob_2(\beta) + Ob_2(\alpha\beta)$$

$$\beta \longmapsto \mathrm{Tr}_{LF/F}\left(\frac{\sqrt{\alpha}}{f'(\varphi)} \right) \mathrm{Tr}_{LF/F}\left(\frac{\sqrt{\beta\gamma}}{f'(\varphi)} \right)$$

where $\alpha, \beta, \gamma \in L^*$ are <u>linear</u> in φ and $\alpha\beta\gamma \in (L^*)^2$