

Some improvements to 4-descent
on an elliptic curve

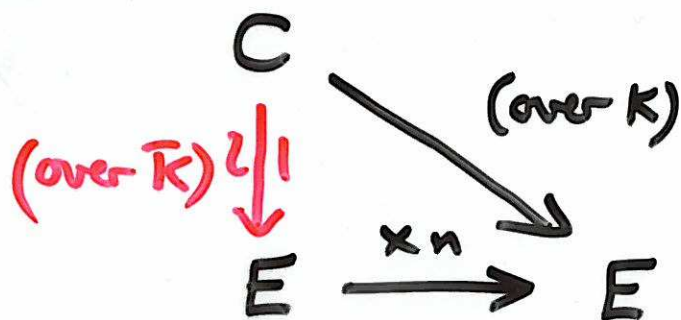
Tom Fisher
(University of Cambridge)

ANTS VIII 19th May 2008

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

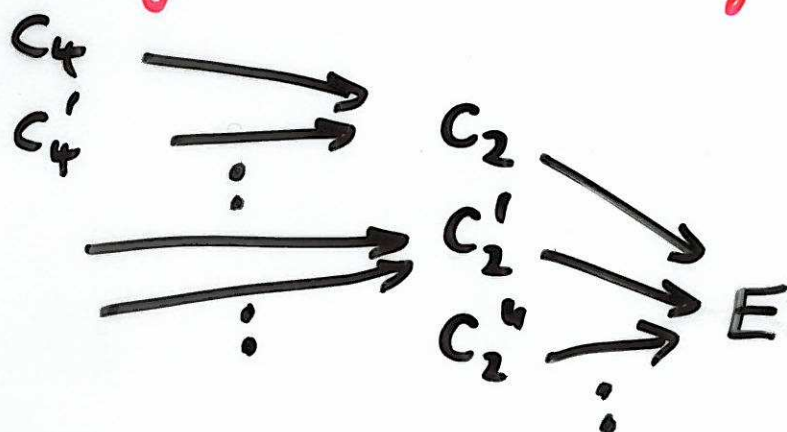
E/K an elliptic curve

n -covering



ELS 4-coverings

ELS 2-coverings



$$E(K)[2] \rightarrow S^{(2)}(E/K) \rightarrow S^{(4)}(E/K) \rightarrow S^{(2)}(E/K) \rightarrow \dots$$

4-descent developed in PhD theses of

Siksek (1995) ← see also (Membran, Siksek, Smart 1996)

Winnak (2003) ← MAGMA implementation

Stumminger (2005) ← also 8-descent.

Background on 2-descent

$E: y^2 = f(x) \quad f \in K[x] \text{ monic, cubic}$

(assume irreducible)

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

$H^1(K, E[2])$

There is a group homomorphism

$E(K) \rightarrow \ker \left(L^* / (L^*)^2 \xrightarrow{N_{L/K}} K^* / (K^*)^2 \right)$

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

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

$Ob_2: H^1(K, E[2]) \rightarrow Br(K)$

$\alpha \mapsto \left(\text{class of the conic} \right) \left\{ Q_2 = 0 \right\}$

Note $Ob_2(\alpha) = 0 \iff \alpha(L^*)^2$ 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 ≈ 1400 decimal digits

But $\alpha \equiv t^2 - t + 113 \pmod{(K^*)^2}$

$\alpha \equiv 3 \pmod{(K^*)^3}$

$\alpha \equiv 9t^2 + 72t + 1359 \pmod{(K^*)^4}$

$\alpha \equiv 518t^2 - 5922t - 76801 \pmod{(K^*)^5}$

How to find good representatives?

"MINIMISE"

write $(\alpha) = \underline{\underline{\zeta}} \underline{\underline{\zeta}}^n$

where $\underline{\underline{\zeta}} = \prod_{i=1}^{r_1} p_i^{r_i} \dots \prod_{i=1}^{r_k} p_i^{r_k}$ $0 < r_i < n$

"REDUCE"

Find $\delta \in \underline{\underline{\zeta}}^{-1}$ that is short

w.r.t. the inner product

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

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

Then replace α by $\alpha \delta^n$

MAGMA function: **Nice Representative Modulo Powers**

Background on 4-descent

Start with a 2-covering (with trivial obstruction)

$$C_2: y^2 = g(x)$$

$g \in K[x]$ quartic
leading coeff a (say)
(assume irreducible)

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

There is a map

$$C_2(K) \longrightarrow \left\{ \xi \in F^* \mid N_{F/K}(\xi) \equiv a \pmod{(K^*)^2} \right\}$$

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

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

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

— a quadric intersection (QI)

Remarks

- (i) Multiplying ξ by an element of K^* or $(F^*)^2$
gives equivalent QI's
- (ii) C_4 ELS $\iff \xi \in \left(\begin{array}{l} \text{a finite subset} \\ \text{of } F^*/K^*(F^*)^2 \end{array} \right)$

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

Testing Equivalence of 4-coverings

$$C_4 = \{Q_1 = Q_2 = 0\} \begin{cases} \rightarrow C_2 = \{y^2 = g(x)\} \\ \text{(intermediate 2-covering)} \\ \rightarrow \exists \in F^* / (K^*(F^*)^2) \end{cases}$$

classical formulae

Given QI's C_4 and C_4'

- Test whether C_2 and C_2' are equivalent (Gemara, 2001)
- If so, C_2 and C_2' determine the same field F . Compute $\exists, \exists' \in F^*$
- Test whether $\exists \equiv \exists' \pmod{K^*(F^*)^2}$

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

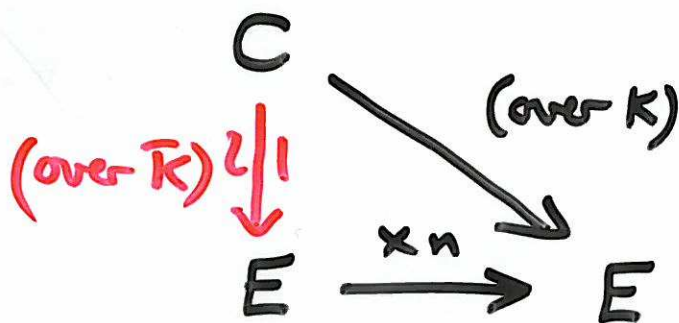
IsEquivalent(<Model G1>, <Model G1>)

- If true also returns the transformation in $GL_2(\mathbb{Q}) \times GL_4(\mathbb{Q})$.

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

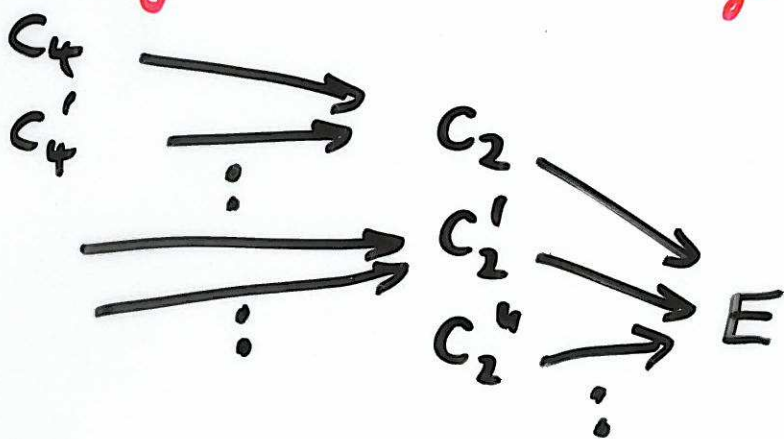
E/K an
elliptic curve

n -covering



ELS 4-coverings

ELS 2-coverings



$$E(K)[2] \rightarrow S^{(2)}(E/K) \rightarrow S^{(4)}(E/K) \rightarrow S^{(2)}(E/K) \rightarrow \dots$$

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

Why is this difficult?

representing elements
as QI's

A 4-covering $\mathfrak{F} \in H^1(K, E[4])$ can be
written as a QI $\iff \text{ob}_4(\mathfrak{F}) = 0$

where $\text{ob}_4: H^1(K, E[4]) \rightarrow \text{Br}(K)$
(quadratic map)

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

A general method (Cremers, F., O'Neil, Simer, 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 $A \cong \text{Mat}_4(K)$ find such an isomorphism explicitly } (Pillniková 2007)

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

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

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

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

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

$$\beta \mapsto \text{Obs}_2(\alpha) + \text{Obs}_2(\beta) + \text{Obs}_2(\alpha\beta)$$

$$\beta \mapsto \text{Tr}_{L/F} \left(\frac{\sqrt{\alpha}}{f'(\varphi)} \right) \text{Tr}_{L/F} \left(\frac{\sqrt{\beta\delta}}{f'(\varphi)} \right)$$

where $\alpha, \beta, \delta \in L^*$ are linear in φ
and $\alpha\beta\delta \in (L^*)^2$