Explicit Kummer Varieties for Hyperelliptic Curves of Genus 3

Michael Stoll
Universität Bayreuth

Théorie des nombres et applications
CIRM, Luminy

January 17, 2012
Application / Motivation

We would like to determine the set of integral points on a curve like

\[ C : Y^2 - Y = X^7 - X. \]

**Bugeaud, Mignotte, Siksek, St., Tengely (2008):**

Can be done if we know generators of the Mordell-Weil Group \( J(\mathbb{Q}) \) (where \( J \) is the Jacobian of \( C \)).

Existing technology gives \( J(\mathbb{Q}) \cong \mathbb{Z}^4 \)

and generators of a finite-index subgroup \( G \).

**Theorem** (St., yesterday).

\( J(\mathbb{Q}) \) is generated by the classes of the divisors

\[ (0,0) - \infty, \quad (1,0) - \infty, \quad (-1,0) - \infty \quad \text{and} \quad (\omega,0) + (\omega^2,0) - 2 \cdot \infty \]

where \( \omega^2 + \omega + 1 = 0. \)
Requirements

What do we need to be able to saturate $G$?

We need to be able to

- Compute canonical heights on $J(\mathbb{Q})$.
- Bound the difference between naïve and canonical height.

Reason:

- We can enumerate points with bounded naïve height.
- We want to enumerate points with bounded canonical height.
Let $C'$ be a hyperelliptic curve of genus 3 over $\mathbb{Q}$:

$$C' : Y^2 = F(X, Z) = f_8 X^8 + f_7 X^7 Z + \ldots + f_1 XZ^7 + f_0 Z^8$$

with $F \in \mathbb{Z}[X, Z]$ such that $\text{disc}(F) \neq 0$; $C'$ is a smooth curve in $\mathbb{P}^2_{1,4,1}$.

Let $J$ be the Jacobian variety of $C'$.

The quotient of $J$ by the action of $\{\pm 1\}$ is the Kummer Variety $K$.

There is an embedding $J \xrightarrow{\kappa} K \hookrightarrow \mathbb{P}^7$ that gives rise to a naïve height $h$ on $K$ and $J$ and consequently to the canonical height $\hat{h}(P) = \lim_{n \to \infty} 4^{-n} h(2^n P)$. 
The Objects

We want:

- The embedding $K \hookrightarrow \mathbb{P}^7$.
- Equations for its image.
- The duplication map $\delta : K \to K$, $\kappa(P) \mapsto \kappa(2P)$.
- The sum and difference map $\quad \quad B : \text{Sym}^2 K \to \text{Sym}^2 K, \quad \{\kappa(P), \kappa(Q)\} \mapsto \{\kappa(P + Q), \kappa(P - Q)\}$.

The embedding defines the naïve height $h$.
The duplication map can be used to compute the canonical height $\hat{h}$ and to bound the height difference.
Previous Work

For the case $f_8 = 0$:

- **A. Stubbs** (2000): Embedding and many (but not all) equations.
- **J.S. Müller** (2010): All equations.
- **Duquesne and Müller**: Conjectural $\delta$, preliminary results on $B$.

Computation of $\tilde{h}$:

- **Müller and D. Holmes**: General algorithms.
Overview of Results

For the general case \((f_8 \neq 0 \text{ not excluded})\) I get:

- The embedding (in the most natural coordinates \(\xi_1, \ldots, \xi_8\);
  \(\kappa(O) = (0 : 0 : 0 : 0 : 0 : 0 : 0 : 1)\)).
- The equations describing \(K \subset \mathbb{P}^7\):
  \(\xi_1\xi_8 - \xi_2\xi_7 + \xi_3\xi_6 - \xi_4\xi_5 = 0\) plus 34 quartic relations.
- The action of \(J[2]\) (taken from Duquesne).
- The duplication map \(\delta\)
  (quartic polynomials \(\delta_1, \ldots, \delta_8 \in \mathbb{Z}[f_0, \ldots, f_8][\xi_1, \ldots, \xi_8]\)
  such that \(\delta(0, 0, 0, 0, 0, 0, 0, 1) = (0, 0, 0, 0, 0, 0, 0, 1)\).
- The sum and difference map \(B\)
  (bilinear forms in \(\xi_i\xi_j\) and \(\Xi\) where \(4\Xi^2 = \delta_1\)).
- Results on heights.
The Action of Two-Torsion

Assume that $f_8 \neq 0$ and let $f = F(x, 1) \in \mathbb{Z}[x]$. Let $\Omega$ denote the set of roots of $f$.

A point $T \in J[2]$ corresponds to a partition $\{\Omega_1, \Omega_2\}$ of $\Omega$ with $\#\Omega_1$ and $\#\Omega_2$ even. Define $\sigma(T) = (-1)^{\#\Omega_1/2}$ (OK since $\#\Omega_1 \equiv \#\Omega_2 \mod 4$). Then $e_2(T, T') = \sigma(T)\sigma(T')\sigma(T + T')$.

There is an extension

$$0 \longrightarrow \mu_2 \longrightarrow \Gamma \overset{\pi}{\longrightarrow} J[2] \longrightarrow 0$$

with $\Gamma \subset SL(8)$ such that $\gamma^2 = \sigma(\pi(\gamma))I_8$ and such that $\gamma$ acts on $K \subset \mathbb{P}^7$ as translation by $\pi(\gamma)$. 
The First Representation

Let $V_n$ denote the space of homogeneous polynomials of degree $n$ in $\xi_1, \ldots, \xi_8$.

Then $\Gamma$ acts on $V_n$: $\rho_n : \Gamma \to \text{Aut}(V_n)$.
Let $\chi_n$ be the character of $\rho_n$.

$$\chi_1(\gamma) = \text{Tr}(\gamma) = \begin{cases} \pm 8 & \text{if } \pi(\gamma) = O, \\ 0 & \text{else.} \end{cases}$$

It follows that $\rho_1$ is irreducible.

For $n$ even, $\rho_n$ will factor through $J[2]$ and therefore split into one-dimensional representations.
The Second Representation

We can compute $\chi_2$ and deduce that

$$\rho_2 \cong \bigoplus_{\sigma(T)=1} \rho_T$$

where $\rho_T$ is given by $\gamma \mapsto e_2(T, \pi(\gamma))$.

Since $\sigma(O) = 1$, there is a copy of the trivial representation; it is generated by $\xi_1\xi_8 - \xi_2\xi_7 + \xi_3\xi_6 - \xi_4\xi_5$.

For $T \neq O$, $\sigma(T) = 1$, let $y_T$ denote the generator of the $T$-eigenspace with coefficient 1 at $\xi^2_8$. Then the coefficients of $y_T$ are integral over $\mathbb{Z}[f_0, \ldots, f_8]$.

**Lemma.** $8\xi^2_j$ is an integral linear combination of the $y_T/R(T)$, where $R(T)$ is the resultant of the two factors of $F$ corresponding to $T$. 
The Third Representation

We now consider $\rho_4$. In the same way as before, we find that

$$\rho_4 \cong \rho_O^{\oplus 15} \oplus \bigoplus_{T \neq O} \rho_T^{\oplus 5}.$$  

Lemma.  
The invariant subspace of $V_4$ intersects $I(K)$ in a seven-dimensional space. The quotient is spanned by the images of $\delta_1, \ldots, \delta_8$. 

For $T \neq O$ with $\sigma(T) = 1$,

$$y_T^2 \equiv \delta_8 - \tau_2 \delta_7 + \tau_3 \delta_6 - \tau_4 \delta_5 - \tau_5 \delta_4 + \tau_6 \delta_3 - \tau_7 \delta_2 + \tau_8 \delta_1 \mod I(K)$$

where $\kappa(T) = (1 : \tau_2 : \ldots : \tau_8)$ and the $\tau_j$ are integral.

Corollary. For $\mathbb{P}(\xi) \in K(\mathbb{Q}_v)$ and $v$ a non-arch. valuation,

$$0 \leq v(\delta(\xi)) - 4v(\xi) \leq v(2^6 \text{disc}(F)).$$
The Height

Recall:

- \( h(\mathbb{P}(\xi)) = \sum_v \log \max\{|\xi_j|_v : 1 \leq j \leq 8\}. \)
- \( \hat{h}(P) = \lim_{n \to \infty} 4^{-n}h(2^n P) = h(P) + \sum_{n=0}^{\infty} 4^{-n-1}(h(2^{n+1} P) - 4h(2^n P)). \)

Define, for \( P \in J(\mathbb{Q}_v) \) with \( \kappa(P) = \mathbb{P}(\xi) \),

\[ \varepsilon_v(P) = \log \max_j\{|\delta_j(\xi)|_v\} - 4 \log \max_j\{|\xi_j|_v\}. \]

and \( \gamma_v = -\min_{P \in J(\mathbb{Q}_v)} \varepsilon_v(P). \)

Then for \( v = p \) non-archimedean,

\[ -v(2^6 \text{disc}(F)) \log p \leq -\gamma_p \leq \varepsilon_p(P) \leq 0. \]

For \( v = \infty \), lower and upper bounds \( -\gamma_\infty \) and \( \gamma'_\infty \) for \( \varepsilon_\infty(P) \) can also be computed (using the Lemmas above).
Bounding the Height Difference

Since
\[ h(P) - \hat{h}(P) = - \sum_{v} \sum_{n=0}^{\infty} 4^{-n-1} \varepsilon_v(P), \]
we obtain
\[ -\frac{1}{3} \gamma' \leq h(P) - \hat{h}(P) \leq \frac{1}{3} \left( \gamma_{\infty} + \sum_{p|2\text{disc}(F')} \gamma_p \right) \leq \frac{1}{3} (\gamma_{\infty} + \log |2^6\text{disc}(F')|). \]

Improvements are possible, for example for non-arch. odd \( v = p \):
\[ v(\text{disc}(F')) = 1 \implies \gamma_p = 0. \]

The bounds on \( \varepsilon_v \) allow us
- to compute canonical heights, and
- to saturate subgroups.
The Example

We come back to our original example

\[ C : Y^2 - Y = X^7 - X. \]

This is isomorphic to \( Y^2 = 4X^7Z - 4XZ^7 + Z^8; \) the discriminant of the right hand side is \( 2^{16} \cdot 19 \cdot 223 \cdot 44909. \)

We therefore obtain

\[ h(P) - \hat{h}(P) \leq \frac{22}{3} \log 2 + \frac{1}{3} \gamma_\infty < 6.2345. \]

Looking at the lattice corresponding to the known subgroup, we can conclude that \( J(\mathbb{Q}) \) is generated by the known points together with points \( P \) such that

\[ H(P) = \exp h(P) \leq 847. \]

No new generators exist in this range.
Concluding Remarks

• The action of $\Gamma$ can be used to find the sum and difference map.

• A more detailed study of the $\varepsilon_p$ leads to an efficient algorithm that computes

$$\mu_p(P) = \sum_{n=0}^{\infty} 4^{-n-1} \varepsilon_p(2^n P) \in \mathbb{Q} \log p$$

exactly.

• The construction of the embedding $K \subset \mathbb{P}^7$ is based on the Mumford representation of effective divisors of degree 4 in general position. It leads to an explicit description of the form $K \setminus \kappa(\Theta) \cong V/G$ with an affine variety $V$ on which a group $G$ acts.