Isogenies and the Discrete Logarithm Problem in Genus Three

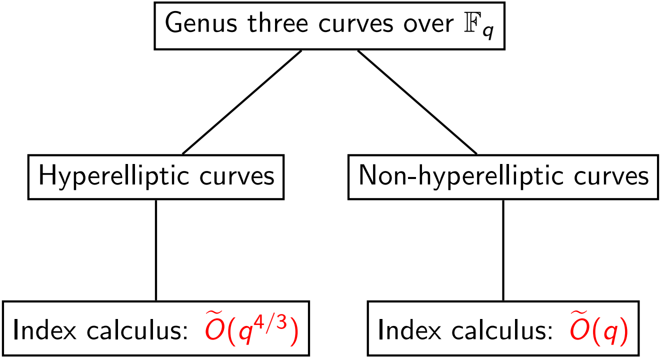
Benjamin Smith

Royal Holloway, University of London

September 6, 2007

q is odd!

Curves of genus three



Index calculus on hyperelliptic curves: Gaudry–Thomé–Theriault–Diem
Index calculus on non-hyperelliptic curves: Diem

Hyperelliptic and non-hyperelliptic curves of genus three

Hyperelliptic curves $H/\mathbb{F}_q$:
Defining equation:

$$H : y^2 = F(x, z),$$

where F is a squarefree homogeneous polynomial of degree 8
($\longrightarrow$ projective model in $\mathbb{P}(1, 4, 1)$).
Canonical map: $\pi : H \longrightarrow \mathbb{P}^1$, $(x : y : z) \longmapsto (x : z)$.
Involution: $\iota : (x : y : z) \mapsto (x : -y : z)$.

Hyperelliptic and non-hyperelliptic curves of genus three

Hyperelliptic curves $H/\mathbb{F}_q$:
Defining equation:

$$H : y^2 = F(x, z),$$

where F is a squarefree homogeneous polynomial of degree 8
($\longrightarrow$ projective model in $\mathbb{P}(1, 4, 1)$).
Canonical map: $\pi : H \longrightarrow \mathbb{P}^1$, $(x : y : z) \longmapsto (x : z)$.
Involution: $\iota : (x : y : z) \mapsto (x : -y : z)$.

Non-hyperelliptic curves $C/\mathbb{F}_q$:
Defining equation:

$$C : F(x, y, z) = 0,$$

where F is a homogeneous polynomial of degree 4
(Plane Quartic Model in $\mathbb{P}^2$).
Canonical map: embedding $C \hookrightarrow \mathbb{P}^2$.

More on genus three curves

Throughout, we adopt these conventions:

- X always denotes a curve of genus three
- H always denotes a hyperelliptic curve of genus three
- C always denotes a non-hyperelliptic curve of genus three (with a plane quartic model).

More on genus three curves

Throughout, we adopt these conventions:

- X always denotes a curve of genus three
- H always denotes a hyperelliptic curve of genus three
- C always denotes a non-hyperelliptic curve of genus three (with a plane quartic model).

The **Jacobian** J_X of X is a three-dimensional PPAV.

Points of J_X correspond to divisor classes on X (elements of $\mathrm{Pic}^0(X)$); that is, equivalence classes of formal sums $\sum_i P_i$ of points on X.

Nonsingular projective embeddings of J_X are too hard to work with, so we always work with $\mathrm{Pic}^0(X)$ and X instead.

Homomorphisms and the DLP

Hyperelliptic and non-hyperelliptic curves
have completely different geometries.

H **cannot** be isomorphic to C

$\implies$ J_H **cannot** be isomorphic to J_C (as PPAVs)

...so we can't translate Index Calculus algorithms between J_C and J_H.

But we **can** have homomorphisms $J_H \to J_C$
— so we should be able to translate DLPs from J_H to J_C:

$$Q = [m]P \implies \phi(Q) = [m]\phi(P).$$

A surjective homomorphism with finite kernel is called an **isogeny**.

Our aim

Aim: explicit isogenies from hyperelliptic to non-hyperelliptic Jacobians.

Oort and Ueno:

every 3-dimensional PPAV is isomorphic (over $\mathbb{F}_{q^2}$) to a Jacobian.

$\Longrightarrow$ quotients of J_H by small subgroups give isogenies to other Jacobians.

Naïve picture of moduli spaces:

(It's on the board!)

If we start from J_H and take an arbitrary isogeny $J_H \to J_X$,
then with overwhelming probability we will have an isomorphism $X \cong C$,
and hence an isogeny $J_H \to J_C$.

Computing explicit isogenies

For almost all choices of kernel, no explicit construction of the isogenies are known.

We will give a general construction for $(2, 2, 2)$-isogenies.

Computing explicit isogenies

For almost all choices of kernel, no explicit construction of the isogenies are known.

We will give a general construction for $(2,2,2)$-isogenies.

The **Weierstrass points** of $H : y^2 = F(x,z)$
are the eight points $W_1, \ldots, W_8$ of $H(\overline{\mathbb{F}_q})$ where $y(W_i) = 0$.

The divisor classes $[W_1 - W_2]$, $[W_3 - W_4]$, $[W_5 - W_6]$, and $[W_7 - W_8]$
generate a subgroup $S \cong (\mathbb{Z}/2\mathbb{Z})^3$ of J_H.
We call such subgroups **tractable subgroups**.

We have derived algorithms to compute isogenies with tractable kernels.

Geometric methods

Suppose we are given H and $S = \langle [W_i - W_{i+1}] : i \in \{1, 3, 5, 7\} \rangle$.

Let $g : \mathbb{P}^1 \to \mathbb{P}^1$ be a 3-to-1 (**trigonal**) map such that

$$g(W_i) = g(W_{i+1}) \text{ for each } [W_i - W_{i+1}] \in S.$$

Geometric methods

Suppose we are given H and $S = \langle [W_i - W_{i+1}] : i \in \{1,3,5,7\} \rangle$.

Let $g : \mathbb{P}^1 \to \mathbb{P}^1$ be a 3-to-1 (**trigonal**) map such that

$$g(W_i) = g(W_{i+1}) \text{ for each } [W_i - W_{i+1}] \in S.$$

Recillas' **trigonal construction**, applied to $\pi : H \to \mathbb{P}^1$ and $g : \mathbb{P}^1 \to \mathbb{P}^1$, yields a curve X of genus three and a 4-to-1 map $f : X \to \mathbb{P}^1$.
Donagi and Livné: there is an isogeny $\phi : J_H \to J_X$ with kernel S.

If Q is a point on $\mathbb{P}^1$, then

$$(g \circ \pi)^{-1}(Q) = \{P_1, P_2, P_3, \iota(P_1), \iota(P_2), \iota(P_3)\}$$

$$f^{-1}(Q) = \left\{ \begin{array}{c} Q_1 \leftrightarrow \{P_1, P_2, P_3 | \iota(P_1), \iota(P_2), \iota(P_3)\}, \\ Q_2 \leftrightarrow \{P_1, \iota(P_2), \iota(P_3) | \iota(P_1), P_2, P_3\}, \\ Q_3 \leftrightarrow \{\iota(P_1), P_2, \iota(P_3) | P_1, \iota(P_2), P_3\}, \\ Q_4 \leftrightarrow \{\iota(P_1), \iota(P_2), P_3 | P_1, P_2, \iota(P_3)\} \end{array} \right\}$$

Everybody loves commutative diagrams...

$$
\begin{tikzcd}
 & R \arrow[dl, "\pi_H"', "2"] \arrow[dr, "\pi_X", "3"'] & & \\
H \arrow[d, "\pi"', "2"] & & X \arrow[r, "\cong", "??"'] \arrow[ddl, "4"', "f"'] & C \\
\mathbb{P}^1 \arrow[dr, "3", "g"'] & & & \\
 & \mathbb{P}^1 & &
\end{tikzcd}
$$

$$
\begin{tikzcd}
 & J_R \arrow[dr, "(\pi_X)_*"] & & \\
J_H \arrow[ur, "(\pi_H)^*"] \arrow[rrr, bend right, "\phi"'] & & J_X \arrow[r, "\cong"] & J_C
\end{tikzcd}
$$

Explicit trigonal constructions

Given S (over $\mathbb{F}_q$), we can compute g using basic linear algebra.
this requires solving a quadratic equation over $\mathbb{F}_q$.

Given g and H, we can compute a model of X in $\mathbb{A}^1 \times \mathbb{A}^3$ using linear algebra and modular polynomial arithmetic. (The computation is involved, but essentially easy.)
Again, we need to solve a quadratic equation over $\mathbb{F}_q$.

The map $f : X \to \mathbb{A}^1$ is projection onto the first factor.

Having computed g, f, and X, we get R, π_H and π_X "for free".

Finally, the canonical map of X (for the isomorphism to C) can be computed quickly using standard algorithms.

Rationality

It is important that our isogenies be $\mathbb{F}_q$-rational
— otherwise they map $J_H(\mathbb{F}_q)$ into $J_C(\mathbb{F}_{q^d})$;
Index Calculus in $J_C(\mathbb{F}_{q^d})$ requires $\widetilde{O}(q^d)$ time, so we gain nothing!

We therefore need

1. A rational kernel subgroup S
2. A rational trigonal map g
   $\longrightarrow 1/2$ probability for a given rational S
3. A rational model for X
   $\longrightarrow 1/2$ probability for a given rational S and g

We should be able to use descent to deal with irrational trigonal maps g.

How many kernel subgroups are there?

$H : y^2 = F(x, z)$, F homogeneous, squarefree, $\deg F = 8$.
$\mathcal{S}(H) :=$ set of $\mathbb{F}_q$-rational tractable subgroups of J_H.

Degrees of k-irreducible factors of F	$\#\mathcal{S}(H)$
$(8), (6, 2), (6, 1, 1), (4, 2, 1, 1)$	1
$(4, 4)$	5
$(4, 2, 2), (4, 1, 1, 1, 1), (3, 3, 2), (3, 3, 1, 1)$	3
$(2, 2, 2, 1, 1)$	7
$(2, 2, 1, 1, 1, 1)$	9
$(2, 1, 1, 1, 1, 1, 1)$	15
$(2, 2, 2, 2)$	25
$(1, 1, 1, 1, 1, 1, 1, 1)$	105
Other	0

How often do we have a rational isogeny?

Summing over probabilities of the different factorization types, we find that for a randomly chosen $H : y^2 = F(x, z)$, there is an expectation of

$$\sim 18.57\%$$

that our methods will produce a rational isogeny from $J_H \to J_C$.

If we can use descent to account for the square root in computing g, we obtain an even better expectation:

$$\sim 31.13\%$$

Remarks

1. This approach is independent of the size of the DLP subgroup.

Remarks

1. This approach is independent of the size of the DLP subgroup.
2. These algorithms are "very fast".

Remarks

1. This approach is independent of the size of the DLP subgroup.
2. These algorithms are "very fast".
3. With more general methods for isogenies, more hyperelliptic curves will be vulnerable to $\widetilde{O}(q)$ index calculus (including characteristic 2).

Remarks

1. This approach is independent of the size of the DLP subgroup.
2. These algorithms are "very fast".
3. With more general methods for isogenies, more hyperelliptic curves will be vulnerable to $\widetilde{O}(q)$ index calculus (including characteristic 2).
4. This approach is not generally applicable in lower genus...

Remarks

1. This approach is independent of the size of the DLP subgroup.
2. These algorithms are "very fast".
3. With more general methods for isogenies, more hyperelliptic curves will be vulnerable to $\widetilde{O}(q)$ index calculus (including characteristic 2).
4. This approach is not generally applicable in lower genus...
5. ...and probably will not work in higher genus either.

Remarks

1. This approach is independent of the size of the DLP subgroup.
2. These algorithms are "very fast".
3. With more general methods for isogenies, more hyperelliptic curves will be vulnerable to $\widetilde{O}(q)$ index calculus (including characteristic 2).
4. This approach is not generally applicable in lower genus...
5. ...and probably will not work in higher genus either.
6. As things stand, "security" of genus three hyperelliptic Jacobians depends on the factorization of the hyperelliptic polynomial.

Thanks

Thanks: to Roger Oyono and Christophe Ritzenthaler