Genus 3 curves and the inverse Galois problem

Samuele Anni
joint with Pedro Lemos and Samir Siksek

University of Warwick

Modular Forms and Curves of Low Genus: Computational Aspects
ICERM, Providence, 29th September 2015
1. The inverse Galois problem

2. Abelian varieties and the inverse Galois problem

3. The main result

4. An “algorithm” for the genus 3 case
The inverse Galois problem

Let $G$ be a finite group. Does there exist a Galois extension $K/\mathbb{Q}$ such that $\text{Gal}(K/\mathbb{Q}) \cong G$?

For example, let $G$ be $S_n$, the symmetric group of $n$ letters. Then $G$ is a Galois group over $\mathbb{Q}$. Moreover, for all positive integer $n$ we can realize $G$ as the Galois group of the splitting field $x^n - x - 1$.

Galois representations may answer the inverse Galois problem for finite linear groups.
1. **The inverse Galois problem**

2. **Abelian varieties and the inverse Galois problem**
   - Back to the inverse Galois problem

3. **The main result**

4. **An “algorithm” for the genus 3 case**
Let $\overline{\mathbb{Q}}$ be an algebraic closure of $\mathbb{Q}$ and let $G_{\mathbb{Q}} = \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

Let $A$ be a principally polarized abelian variety over $\mathbb{Q}$ of dimension $d$.

Let $\ell$ be a prime and $A[\ell]$ the $\ell$-torsion subgroup:

$$A[\ell] := \{ P \in A(\overline{\mathbb{Q}}) \mid [\ell]P = 0 \} \cong (\mathbb{Z}/\ell\mathbb{Z})^{2d}.$$ 

$A[\ell]$ is a $2d$-dimensional $\mathbb{F}_\ell$-vector space, as well as a $G_{\mathbb{Q}}$-module.
The polarization induces a symplectic pairing, the mod $\ell$ Weil pairing on $A[\ell]$, which is a bilinear, alternating, non-degenerate pairing:

$$\langle \ , \ \rangle : A[\ell] \times A[\ell] \to \mu_\ell$$

that is Galois invariant: $\forall \sigma \in G_\mathbb{Q}, \forall v, w \in A[\ell]$,

$$\langle \sigma v, \sigma w \rangle = \chi(\sigma) \langle v, w \rangle,$$

where $\chi : G_\mathbb{Q} \to \mathbb{F}_\ell^\times$ is the mod $\ell$ cyclotomic character.

$(A[\ell], \langle \ , \ \rangle)$ is a symplectic $\mathbb{F}_\ell$-vector space of dimension $2d$. This gives a representation

$$\bar{\rho}_{A,\ell} : G_\mathbb{Q} \to \text{GSp}(A[\ell], \langle \ , \ \rangle) \cong \text{GSp}_{2d}(\mathbb{F}_\ell).$$
Theorem (Serre)

Let $A$ be a principally polarized abelian variety of dimension $d$, defined over $\mathbb{Q}$. Assume that $d = 2, 6$ or $d$ is odd and, furthermore, assume that $\text{End}_\mathbb{Q}(A) = \mathbb{Z}$. Then there exists a bound $B_A$ such that for all primes $\ell > B_A$ the representation $\bar{\rho}_{A,\ell}$ is surjective.

The conclusion of the theorem is known to be false for general $d$ (counterexample by Mumford for $d = 4$).
**Open Question**

Given $d$ as in the theorem, is there a uniform bound $B_d$ depending only on $d$, such that for all principally polarized abelian varieties $A$ over $\mathbb{Q}$ of dimension $d$ with $\text{End}_\mathbb{Q}(A) = \mathbb{Z}$, and all $\ell > B_d$, the representation $\overline{\rho}_{A,\ell}$ is surjective?

For elliptic curves an affirmative answer is expected, and this is known as Serre’s Uniformity Question.

Much easier for semistable elliptic curves:

**Theorem (Serre)**

Let $E/\mathbb{Q}$ be a semistable elliptic curve, and $\ell \geq 11$ be a prime. Then $\overline{\rho}_{E,\ell}$ is surjective.
The Galois representation attached to the $\ell$-torsion of the elliptic curve $y^2 + y = x^3 - x$ is surjective for all prime $\ell$. This gives a realization $\text{GL}_2(\mathbb{F}_\ell)$ as Galois group for all $\ell$.

Let $C$ be the genus 2 hyperelliptic curve given by $y^2 = x^5 - x + 1$ and let $J$ denote its Jacobian. Dieulefait proved that $\bar{\rho}_{J,\ell}$ is surjective for all odd prime $\ell$. This gives a realization $\text{GSp}_4(\mathbb{F}_\ell)$ as Galois group for all odd $\ell$.

What about genus 3 curves?
1 **The inverse Galois problem**

2 **Abelian varieties and the inverse Galois problem**

3 **The main result**
   - Transvection
   - Ingredients of the proof of the main theorem
   - Idea of the proof

4 **An “algorithm” for the genus 3 case**
Theorem (A., Lemos and Siksek)

Let $A$ be a semistable principally polarized abelian variety of dimension $d \geq 1$ over $\mathbb{Q}$ and let $\ell \geq \max(5, d + 2)$ be prime. Suppose the image of $\bar{\rho}_{A, \ell} : G_{\mathbb{Q}} \to \text{GSp}_{2d}(\overline{\mathbb{F}}_{\ell})$ contains a transvection. Then $\bar{\rho}_{A, \ell}$ is either reducible or surjective.
Theorem (A., Lemos and Siksek)

Let $A$ be a semistable principally polarized abelian variety of dimension $d \geq 1$ over $\mathbb{Q}$ and let $\ell \geq \max(5, d + 2)$ be prime. Suppose the image of $\overline{\rho}_{A,\ell} : G_\mathbb{Q} \to \text{GSp}_{2d}(\mathbb{F}_\ell)$ contains a transvection. Then $\overline{\rho}_{A,\ell}$ is either reducible or surjective.
**Transvection**

**Definition**

Let $(V, \langle , \rangle)$ be a finite-dimensional symplectic vector space over $\mathbb{F}_\ell$. A **transvection** is an element $T \in \text{GSp}(V, \langle , \rangle)$ which fixes a hyperplane $H \subset V$.

Therefore, a transvection is a unipotent element $\sigma \in \text{GSp}(V, \langle , \rangle)$ such that $\sigma - I$ has rank 1.
When does $\overline{\rho}_{A,\ell}(G_{\mathbb{Q}})$ contain a transvection?

Let $q \neq \ell$ be a prime and suppose that the following two conditions are satisfied:

- the special fibre of the Néron model for $A$ at $q$ has toric dimension 1;
- $\ell \nmid \#\Phi_q$, where $\Phi_q$ is the group of connected components of the special fibre of the Néron model at $q$.

Then the image of $\overline{\rho}_{A,\ell}$ contains a transvection (Hall).
When does $\overline{\rho}_{A,\ell}(G_{\mathbb{Q}})$ contain a transvection?

Let $C/\mathbb{Q}$ be a hyperelliptic curve of genus $d$:

$$C : y^2 = f(x)$$

where $f \in \mathbb{Z}[x]$ is a squarefree polynomial.

Let $p$ be an odd prime not dividing the leading coefficient of $f$ such that $f$ modulo $p$ has one root in $\overline{\mathbb{F}}_p$ having multiplicity precisely 2, with all other roots simple.

Then the Néron model of the Jacobian at $p$ has toric dimension 1 (Hall).
In the proof of this theorem we rely on:

- the classification due to Arias-de-Reyna, Dieulefait and Wiese of subgroups of $\text{GSp}_{2d}(\mathbb{F}_\ell)$ containing a transvection;

- results of Raynaud on the image of the inertia subgroup.
Classification of subgroups of $GSp_{2d}(\mathbb{F}_\ell)$ with a transvection

**Theorem (Arias-de-Reyna, Dieulefait and Wiese)**

Let $\ell \geq 5$ be a prime and let $V$ a symplectic $\mathbb{F}_\ell$-vector space of dimension $2d$. Any subgroup $G$ of $GSp(V)$ which contains a transvection satisfies one of the following:

1. There is a non-trivial proper $G$-stable subspace $W \subset V$.
2. There are non-singular symplectic subspaces $V_i \subset V$ with $i = 1, \ldots, h$, of dimension $2m < 2d$ and a homomorphism $\phi : G \to S_h$ such that $V = \bigoplus_{i=1}^h V_i$ and $\sigma(V_i) = V_{\phi(\sigma)(i)}$ for $\sigma \in G$ and $1 \leq i \leq h$. Moreover, $\phi(G)$ is a transitive subgroup of $S_h$.
3. $Sp(V) \subseteq G$.

We apply this to $G = \overline{\rho}_{A,\ell}(G_{\mathbb{Q}})$ where $A$ and $\ell$ are as in the main theorem. If $Sp_{2d}(\mathbb{F}_\ell) \subseteq G$ then $G = GSp_{2d}(\mathbb{F}_\ell)$, since the mod $\ell$ cyclotomic character is surjective.
The main result

Ingredients of the proof of the main theorem

Inertia and a theorem of Raynaud

**Theorem (Raynaud)**

Let $A$ be an abelian variety over $\mathbb{Q}$. Let $\ell$ be a prime of semistable reduction for $A$. Regard $A[\ell]$ as an $I_\ell$-module and let $V$ be a Jordan-Hölder factor of dimension $n$ over $\mathbb{F}_\ell$. Let $\psi_n : I_\ell \to \mathbb{F}_\ell^\times$ be a fundamental character of level $n$. Then $V$ has the structure of a $1$-dimensional $\mathbb{F}_\ell^n$-vector space and the action of $I_\ell$ on it is given by a character $\varpi : I_\ell \to \mathbb{F}_\ell^n$, where $\varpi = \psi_n \sum_{i=0}^{n-1} a_i \ell^i$ with $a_i = 0$ or $1$. 
Idea of the proof

Denote $\bar{\rho} = \bar{\rho}_{A, \ell}$. Let $G = \bar{\rho}(G_{\mathbb{Q}}) \subseteq \text{GSp}_{2d}(\mathbb{F}_{\ell})$.

Since $G$ contains a transvection, it is sufficient to show that the induced case does not arise.

Suppose otherwise. Write $V = \bigoplus_{i=1}^{h} V_i$ where $V_i$ are non-singular symplectic subspaces of dimension $2m < 2d$. Then there is some $\phi : G \to S_h$ with transitive image such that $\sigma(V_i) = V_{\phi(\sigma)(i)}$. Let

$$
\begin{array}{ccc}
G_{\mathbb{Q}} & \xrightarrow{\pi} & G \\
\bar{\rho} & \xrightarrow{\phi} & S_h
\end{array}
$$
Let $H = \ker(\pi)$. Then $H = G_K$ for some number field $K/\mathbb{Q}$. Moreover, $\overline{\rho}|_{G_K}$ is reducible as the $V_i$ are stable under the action of $G_K$.

In the proof we show that for $\ell \geq \max(5, d + 2)$ the extension $K/\mathbb{Q}$ is unramified at the finite places, and thus $K$ has discriminant $\pm 1$

$\Rightarrow K = \mathbb{Q} \Rightarrow \pi$ is trivial $\Rightarrow$ contradiction

The bound on $\ell$ is obtained considering the image of inertia subgroup and applying Raynaud’s result.
1 THE INVERSE GALOIS PROBLEM

2 ABELIAN VARIETIES AND THE INVERSE GALOIS PROBLEM

3 THE MAIN RESULT

4 AN “ALGORITHM” FOR THE GENUS 3 CASE
   - 1-dimensional Jordan–Hölder factors
   - 2-dimensional Jordan–Hölder factors
   - 3-dimensional Jordan–Hölder factors
   - Example
We now let $A/\mathbb{Q}$ be a **principally polarized abelian threefold**.

### Assumptions

<table>
<thead>
<tr>
<th>Assumption</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>(A)</td>
<td>$A$ is semistable;</td>
</tr>
<tr>
<td>(B)</td>
<td>$\ell \geq 5$;</td>
</tr>
<tr>
<td>(C)</td>
<td>There is a prime $q$ such that the special fibre of the Néron model for $A$ at $q$ has toric dimension 1.</td>
</tr>
<tr>
<td>(D)</td>
<td>$\ell$ does not divide $\gcd{q \cdot #\Phi_q : q \in S}$, where $S$ is the set of primes $q$ satisfying (C) and $\Phi_q$ is the group of connected components of the special fibre of the Néron model of $A$ at $q$.</td>
</tr>
</tbody>
</table>

Under these assumptions the image of $\overline{\rho}_{A,\ell}$ contains a transvection. Then $\overline{\rho}_{A,\ell}$ is either reducible or surjective.
“Algorithm”

Practical method which should, in most cases, produce a small integer $B$ (depending on $A$) such that for $\ell \mid B$, the representation $\bar{\rho}_{A,\ell}$ is irreducible and, hence, surjective.

We will apply this procedure to the Jacobian of the hyperelliptic curve:

$$C : y^2 + (x^4 + x^3 + x + 1)y = x^6 + x^5$$

(look at the glassboard for the computations).
Let \( \chi : G_Q \to \mathbb{F}_\ell^\times \) denote the mod \( \ell \) cyclotomic character.

We will study the Jordan–Hölder factors \( W \) of the \( G_Q \)-module \( A[\ell] \). By the determinant of such a \( W \) we mean the determinant of the induced representation \( G_Q \to \text{GL}(W) \).

**Lemma**

Any Jordan–Hölder factor \( W \) of the \( G_Q \)-module \( A[\ell] \) has determinant \( \chi^r \) for some \( 0 \leq r \leq \dim(W) \).
Weil polynomials

From a prime $p \neq \ell$ of good reduction for $A$, we will denote by

$$P_p(x) = x^6 + \alpha_p x^5 + \beta_p x^4 + \gamma_p x^3 + p\beta_p x^2 + p^2 \alpha_p + p^3 \in \mathbb{Z}[x]$$

the characteristic polynomial of Frobenius $\sigma_p \in G_\mathbb{Q}$ at $p$ acting on the Tate module $T_\ell(A)$ (also known as the Weil polynomial of $A$ mod $p$). The polynomial $P_p$ is independent of $\ell$.

Its roots in $\overline{\mathbb{F}}_\ell$ have the form $u$, $v$, $w$, $p/u$, $p/v$, $p/w$. 
1-dimensional Jordan–Hölder factors

Let $T$ be a non-empty set of primes of good reduction for $A$. Let

$$B_1(T) = \gcd\{p \cdot \# A(F_p) : p \in T\}.$$

**Lemma**

Suppose $\ell \nmid B_1(T)$. The $G_{\mathbb{Q}}$-module $A[\ell]$ does not have any 1-dimensional or 5-dimensional Jordan–Hölder factors.
Suppose the $\mathbb{G}_Q$-module $A[\ell]$ does not have any 1-dimensional Jordan–Hölder factors, but has either a 2-dimensional or 4-dimensional irreducible subspace $U$. Then $A[\ell]$ has a 2-dimensional Jordan–Hölder factor $W$ with determinant $\chi$. 
Let $N$ be the conductor of $A$. Let $W$ be a 2-dimensional Jordan–Hölder factor of $A[\ell]$ with determinant $\chi$. The representation

$$\tau : \mathbb{G}_Q \to \text{GL}(W) \cong \text{GL}_2(\mathbb{F}_\ell)$$

is odd (as the determinant is $\chi$), irreducible (as $W$ is a Jordan–Hölder factor) and 2-dimensional. By Serre’s modularity conjecture (Khare, Wintenberger, Dieulefait, Kisin Theorem), this representation is modular:

$$\tau \cong \overline{\rho}_f,\ell$$

it is equivalent to the mod $\ell$ representation attached to a newform $f$ of level $M \mid N$ and weight 2.
Let $O_f$ be the ring of integers of the number field generated by the Hecke eigenvalues of $f$. Then there is a prime $\lambda \mid \ell$ of $O_f$ such that for all primes $p \nmid \ell N$,

$$\text{Tr}(\tau(\sigma_p)) \equiv c_p(f) \pmod{\lambda}$$

where $\sigma_p \in G_{\mathbb{Q}}$ is a Frobenius element at $p$ and $c_p(f)$ is the $p$-th Hecke eigenvalue of $f$.

As $W$ is a Jordan–Hölder factor of $A[\ell]$ we see that $x^2 - c_p(f)x + p$ is a factor modulo $\lambda$ of $P_p$. 
Now let $H_{M,p}$ be the $p$-th Hecke polynomial for the new subspace $S_{2}^{\text{new}}(M)$ of cusp forms of weight 2 and level $M$. This has the form

$$H_{M,p} = \prod (x - c_{p}(g)),$$

where $g$ runs through the newforms of weight 2 and level $M$. Write

$$H'_{M,p}(x) = x^{d}H_{M,p}(x + p/x) \in \mathbb{Z}[x],$$

where $d = \deg(H_{M,p}) = \dim(S_{2}^{\text{new}}(M))$.

It follows that $x^{2} - c_{p}(f)x + p$ divides $H'_{M,p}$. 
Let

$$R(M, p) = \text{Res}(P_p, H'_M, p) \in \mathbb{Z},$$

where Res denotes resultant. If $R(M, p) \neq 0$ then we have a bound on $\ell$.

The integers $R(M, p)$ can be very large. Given a non-empty set $T$ of rational primes $p$ of good reduction for $A$, let

$$R(M, T) = \gcd\left\{ p \cdot R(M, p) : p \in T \right\}.$$ 

In practice, we have found that for a suitable choice of $T$, the value $R(M, T)$ is fairly small.
Let

\[ B_2'(T) = \text{lcm}(R(M, T)) \]

where \( M \) runs through the divisors of \( N \) such that \( \dim(S_{2}^{\text{new}}(M)) \neq 0 \), and let

\[ B_2(T) = \text{lcm}(B_1(T), B_2'(T)) \]

where \( B_1(T) \) is given as before.

**Lemma**

Let \( T \) be a non-empty set of rational primes of good reduction for \( A \), and suppose \( \ell \nmid B_2(T) \). Then \( A[\ell] \) does not have 1-dimensional Jordan–Hölder factors, and does not have irreducible 2- or 4-dimensional subspaces.
We fail to bound \( \ell \) in the above lemma if \( R(M, p) = 0 \) for all primes \( p \) of good reduction.

Here are two situations where this can happen:

- Suppose \( A \cong_{\mathbb{Q}} E \times A' \) where \( E \) is an elliptic curve and \( A' \) an abelian surface. Let \( M \mid N \) be the conductor of the elliptic curve, and \( f \) to be the newform associated to \( E \) by modularity, then \( x^2 - c_p(f)x + p \) is a factor of \( P_p(x) \Rightarrow R(M, p) = 0 \) for all \( p \nmid N \).

- Suppose \( A \) is of \( \text{GL}_2 \)-type. Let \( f \) be the corresponding eigenform, then again \( x^2 - c_p(f)x + p \) is a factor of \( P_p(x) \) in \( \mathcal{O}_f[x] \) \( \Rightarrow R(M, p) = 0 \) for all \( p \nmid N \).
Note that in both these situations $\text{End}_{\mathbb{Q}}(A) \neq \mathbb{Z}$.

We expect, but are unable to prove, that if $\text{End}_{\mathbb{Q}}(A) = \mathbb{Z}$ then there will be primes $p$ such that $R(M, p) \neq 0$. 
An “algorithm” for the genus 3 case

3-dimensional Jordan–Hölder factors

**Lemma**

Suppose $A[\ell]$ has Jordan–Hölder filtration $0 \subset U \subset A[\ell]$ where both $U$ and $A[\ell]/U$ are irreducible and 3-dimensional. Moreover, let $u_1, u_2, u_3$ be a basis for $U$, and let

$$G_Q \to \text{GL}_3(\mathbb{F}_\ell), \quad \sigma \mapsto M(\sigma)$$

give the action of $G_Q$ on $U$ with respect to this basis. Then we can extend $u_1, u_2, u_3$ to a symplectic basis $u_1, u_2, u_3, w_1, w_2, w_3$ for $A[\ell]$ so that the action of $G_Q$ on $A[\ell]$ with respect to this basis is given by

$$G_Q \to \text{GSp}_6(\mathbb{F}_\ell), \quad \sigma \mapsto \begin{pmatrix} M(\sigma) & * \\ 0 & \chi(\sigma)(M(\sigma)^t)^{-1} \end{pmatrix}.$$ 

$$\text{det}(U) = \chi^r \text{ and } \text{det}(A[\ell]/U) = \chi^s \text{ where } 0 \leq r, s \leq 3 \text{ with } r + s = 3.$$
Let $p$ be a prime of good reduction for $A$. For ease write $\alpha$, $\beta$ and $\gamma$ for the coefficients $\alpha_p$, $\beta_p$, $\gamma_p$ in the equation of the Weil polynomial. Suppose $p + 1 \neq \alpha$. Let

$$\delta = \frac{-p^2\alpha + p^2 + p\alpha^2 - p\alpha - p\beta + p - \beta + \gamma}{(p - 1)(p + 1 - \alpha)} \in \mathbb{Q}, \quad \epsilon = \delta + \alpha \in \mathbb{Q}.$$ 

Let $g(x) = (x^3 + \epsilon x^2 + \delta x - p)(x^3 - \delta x^2 - p\epsilon x - p^2) \in \mathbb{Q}[x]$. Write $k$ for the greatest common divisor of the numerators of the coefficients in $P_p - g$. Let

$$K_p = p(p - 1)(p + 1 - \alpha)k.$$ 

Then $K_p \neq 0$. Moreover, if $\ell \nmid K_p$ then $A[\ell]$ does not have a Jordan–Hölder filtration as in the previous Lemma with $\det(U) = \chi$ or $\chi^2$. 
Lemma

Let $p$ be a prime of good reduction for $A$. Write $\alpha$, $\beta$ and $\gamma$ for the coefficients $\alpha_p$, $\beta_p$, $\gamma_p$ in the equation of the Weil polynomial. Suppose $p^3 + 1 \neq p\alpha$. Let $\epsilon' = p\delta' + \alpha \in \mathbb{Q}$ where

$$\delta' = \frac{-p^5\alpha + p^4 + p^3\alpha^2 - p^3\beta - p^2\alpha + p\gamma + p - \beta}{(p^3 - 1)(p^3 + 1 - p\alpha)} \in \mathbb{Q}.$$ 

Let $g'(x) = (x^3 + \epsilon'x^2 + \delta'x - 1)(x^3 - p\delta'x^2 - p^2\epsilon'x - p^3) \in \mathbb{Q}[x]$. Write $k'$ for the greatest common divisor of the numerators of the coefficients in $P_p - g'$. Let

$$K'_p = p(p^3 - 1)(p^3 + 1 - p\alpha)k'.$$

Then $K'_p \neq 0$. Moreover, if $\ell \nmid K'_p$ then $A[\ell]$ does not have a Jordan–Hölder filtration as in the above Lemma with $\det(U) = 1$ or $\chi^3$. 
The following theorem summarizes all the lemmas:

**Theorem (A., Lemos and Siksek)**

Let $A$ and $\ell$ satisfy conditions (A)–(D). Let $T$ be a non-empty set of primes of good reduction for $A$. Let

$$B_3(T) = \gcd(\{K_p : p \in T\}), \quad B_4(T) = \gcd(\{K'_p : p \in T\}),$$

where $K_p$ and $K'_p$ are defined in the last two Lemmas. Let

$$B(T) = \text{lcm}(B_2(T), B_3(T), B_4(T)).$$

If $\ell \nmid B(T)$ then $\rho_{A,\ell}$ is surjective.
Example

Theorem (A., Lemos and Siksek)

Let $C/\mathbb{Q}$ be the following genus 3 hyperelliptic curve,

$$C : y^2 + (x^4 + x^3 + x + 1)y = x^6 + x^5.$$ 

and write $J$ for its Jacobian. Let $\ell \geq 3$ be a prime. Then $\overline{\rho}_{J,\ell}(G_{\mathbb{Q}}) = \text{GSp}_6(\mathbb{F}_\ell)$.

Proof.

For $\ell \geq 5$ we apply the algorithm, look at the glassboard for the computations. For $\ell = 3$, we prove the result by direct computations.
Genus 3 curves and the inverse Galois problem

Samuele Anni
joint with Pedro Lemos and Samir Siksek

University of Warwick

Modular Forms and Curves of Low Genus: Computational Aspects
ICERM, Providence, 29th September 2015

Thanks!