Constructing hyperelliptic curves with surjective Galois representations

Samuele Anni
joint with Vladimir Dokchitser

University of Warwick

Automorphic Forms: theory and computation
King's College London, 6th September 2016

1. Abelian varieties and the inverse Galois problem
2. Subgroups of $\mathsf{GSp}_{2g}(\mathbb{F}_\ell)$
3. Semistable abelian varieties
4. Irreducibility and Goldbach
5. Primitivity

The inverse Galois problem

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

Aim of this talk

Show that it is possible to **explicitly** realise for all* $g \in \mathbb{Z}_{\geq 1}$, the group $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$, simultaneously for all odd primes ℓ, using the ℓ-torsion of the Jacobian of the same hyperelliptic curve.

Let $\overline{\mathbb{Q}}$ be an algebraic closure of $\mathbb{Q}$ and let $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

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

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

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

$A[\ell]$ is a $2g$-dimensional $\mathbb{F}_\ell$-vector space, as well as a $G_{\mathbb{Q}}$-module.

The polarization induces a symplectic pairing, the mod ℓ **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 ℓ cyclotomic character.

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

$$\overline{\rho}_{A,\ell}: G_{\mathbb{Q}}\to \mathrm{GSp}(A[\ell],\langle\ ,\ \rangle)\cong\mathrm{GSp}_{2g}(\mathbb{F}_\ell).$$

Theorem (Serre)

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

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

Open question

Is it possble to have a **uniform bound** B_g depending only on g?

Genus 1

The Galois representation attached to the ℓ-torsion of the **elliptic curve**

$$y^2 + y = x^3 - x \qquad (37a1)$$

is surjective for all prime ℓ. This gives a realization $\mathrm{GL}_2(\mathbb{F}_\ell)$ as Galois group for all prime ℓ.

Genus 2 (Dieulefait)

Let C be the **genus** 2 **hyperelliptic curve** given by

$$y^2 = x^5 - x + 1 \qquad (45904.d.734464.1)$$

and let J denotes its Jacobian. Dieulefait proved that $\overline{\rho}_{J,\ell}$ is surjective for all odd prime ℓ. This gives a realization $\mathrm{GSp}_4(\mathbb{F}_\ell)$ as Galois group for all odd prime ℓ.

Genus 3 (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. Then

$$\overline{\rho}_{J,\ell}(G_{\mathbb{Q}}) = \mathrm{GSp}_6(\mathbb{F}_\ell)$$

for all odd prime ℓ. Moreover, $\overline{\rho}_{J,2}(G_{\mathbb{Q}}) \cong S_5 \times C_2 \subseteq S_8$.

Higher genera

What about $g \geq 4$?

Goldbach pairs

Let $g \in \mathbb{Z}_{\geq 0}$.

Hypothesis $(2\mathrm{G} + \epsilon)$

There exist primes q_1, q_2, q_3, q_4, q_5 such that:
$2g + 2 = q_1 + q_2 = q_4 + q_5, \qquad 2g + 2 > q_3 > q_5 > q_2 \geq q_1 > q_4$.

Hypothesis $(2\mathrm{G} + \epsilon)$ has been verified for g up to 10^7: the only exceptions are $0, 1, 2, 3, 4, 5, 7$ and 13.

Main result

Theorem (A., Dokchitser)

Let g be a positive integer such that $(2\mathrm{G}+\epsilon)$ is satisfied. Then there exist an explicit $N \in \mathbb{Z}$ and an explicit $f_0 \in \mathbb{Z}[x]$ monic of degree $2g+2$ such that if

1. $f(x) \equiv f_0 \bmod N$, *and*
2. $C : y^2 = f(x)$ *is semistable at all primes* $p \nmid N$

then $\mathrm{Gal}(\mathbb{Q}(\mathrm{Jac}(C)[\ell])/\mathbb{Q}) \cong \begin{cases} \mathrm{GSp}_{2g}(\mathbb{F}_\ell) & \text{for all primes } \ell \neq 2 \\ S_{2g+2} & \text{for } \ell = 2. \end{cases}$

In the rest of the talk I will explain the role of hypothesis $(2\mathrm{G}+\epsilon)$ and sketch some ideas of the proof of the theorem.

Remarks

- If $(2\mathrm{G}+\epsilon)$ does not hold, it is still possible to obtain the same conclusion except for a finite list of primes ℓ (work in progress).

Genus	primes excluded
2	$3, 5$
3	$3, 5, 7$
4	$5, 7$
5	$5, 7, 11$
7	$5, 11, 13$
13	$11, 17, 23$

- Generalization to higher degree number fields does hold.
- It is possible to prove that for each g which satisfies $(2\mathrm{G}+\epsilon)$ there exists a **positive density** of $f(x) \in \mathbb{Z}[x]$ as in the previous theorem.

Notation: let $C : y^2 = f(x)$ be an hyperelliptic curve over $\mathbb{Q}$ with $f(x) \in \mathbb{Z}[x]$ monic and squarefree of degree $2g+2$ and let $J = \mathrm{Jac}(C)$.

Example: $g = 6$

$$
\begin{aligned}
f_0(x) = {} & x^{14} + 4296083454237577386357617132812 4x^{13} + 2439929119918282243103447454687 52x^{12} + \\
& + 3707073508994624455055086470312 56x^{11} + 3742171491997544285937621694531 20x^{10} + \\
& + 1534893172469251001860492988046 880x^{9} + 8238770649084606799319573145312 64x^{8} + \\
& + 6534612109199198379970793990468 736x^{7} + 2180022624141109179697804398671 872x^{6} + \\
& + 1863946231663073928236023445820 3136x^{5} + 3531469707604255992350756791468 7488x^{4} + \\
& + 1210994917128439969393182861315 62496x^{3} + 2120805092919664051353866276284 37504x^{2} + \\
& + 3208860953573448313306191691715 62496x + 7353483150956662361516268240000 00000
\end{aligned}
$$

$$
N = p_t^2 \cdot p_t'^2 \cdot p_{lin} \cdot p_{irr} \cdot p_2^3 \cdot p_2'^3 \cdot p_3^3 \cdot p_3'^3 \cdot 2^{2g+2} \cdot \prod_{3 \leq p \leq g} p^{g+1} =
$$

$$
= 7^2 \cdot 11^2 \cdot 23 \cdot 29 \cdot 19^3 \cdot 41^3 \cdot 37^3 \cdot 17^3 \cdot 2^{14} \cdot 3^7 \cdot 5^7 = 1302357892577232237180900238080000000
$$

For all $f(x) \in \mathbb{Z}[x]$ such that

1. $f(x) \equiv f_0 \bmod N$, and
2. C is semistable at all primes $p \nmid N$ (e.g. $f = f_0$).

$$
\mathrm{Gal}(\mathbb{Q}(J[\ell])/\mathbb{Q}) \cong \begin{cases} \mathrm{GSp}_{12}(\mathbb{F}_\ell) & \text{for all primes } \ell \neq 2 \\ S_{14} & \text{for } \ell = 2. \end{cases}
$$

1. Abelian varieties and the inverse Galois problem
2. Subgroups of $\mathsf{GSp}_{2g}(\mathbb{F}_\ell)$
3. Semistable abelian varieties
4. Irreducibility and Goldbach
5. Primitivity

Transvection

Definition

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

Therefore, a transvection is a unipotent element $\sigma \in \mathrm{GSp}(V, \langle\ ,\ \rangle)$ such that $\sigma - I$ has rank 1.

When does $\overline{\rho}_{J,\ell}(G_{\mathbb{Q}})$ 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 monic squarefree polynomial.

Let $p \neq \ell$ be an odd prime such that p does not divide the discriminant of f and 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 J at p has toric dimension 1, i.e. $\overline{\rho}_{J,\ell}(G_{\mathbb{Q}})$ contains a transvection (Grothendieck, Hall).

Classification of subgroups of $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$ with a transvection

Theorem (Arias-de-Reyna, Dieulefait and Wiese; Hall)

Let $\ell \geq 5$ be a prime and let V a symplectic $\mathbb{F}_\ell$-vector space of dimension $2g$. Let G be a subgroup of $\mathrm{GSp}(V)$ such that:

(i) G contains a transvection;

(ii) V is an $\mathbb{F}_\ell$ irreducible G-module;

(iii) V is a primitive G-module.

Then G contains $\mathrm{Sp}(V)$. The same holds true for $\ell = 3$, provided that $V \otimes \overline{\mathbb{F}}_3$ is an irreducible and primitive G-module.

1. Abelian varieties and the inverse Galois problem
2. Subgroups of $\mathsf{GSp}_{2g}(\mathbb{F}_\ell)$
3. Semistable abelian varieties
4. Irreducibility and Goldbach
5. Primitivity

The semistable case

Theorem (A., Lemos and Siksek)

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

Genus 3

We now let $A/\mathbb{Q}$ be a **principally polarized abelian threefold**.

Assumptions

(A) A is semistable;

(B) $\ell \geq 5$;

(C) $\overline{\rho}_{A,\ell}(G_{\mathbb{Q}})$ contains a transvection for all ℓ.

Then $\overline{\rho}_{A,\ell}$ is either reducible or surjective.

"Algorithm" (A., Lemos and Siksek)

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

One step: deal with $\boxed{2-\textit{dimensional}}$ Jordan–Hölder factors.

Lemma

Suppose the $G_{\mathbb{Q}}$-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 χ.

Let N be the conductor of A. Let W be a 2-dimensional Jordan–Hölder factor of $A[\ell]$ with determinant χ.
The representation

$$\tau : G_{\mathbb{Q}} \to \mathrm{GL}(W) \cong \mathrm{GL}_2(\mathbb{F}_\ell)$$

is odd (as the determinant is χ), 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 ℓ representation attached to a newform f of level $M \mid N$ and weight 2.

Modularity gives us a criterion to rule out 2-dimensional Jordan–Hölder factors **but** we need to compute $S_2^{\mathrm{new}}(M)$ for all $M \mid \mathrm{cond}(A)$.

The approach for genus 3 do not generalize: increasing g the conductor increases (at least 10.323^g) and the computation of the newform of such levels is not currently available.

On the other hand, dealing with higher dimensional Jordan–Hölder factors is even more "challenging".

New approach

Remove the semistability assumption and introduce primes of bad reduction such that the local inertia has a specific behaviour.

1. Abelian varieties and the inverse Galois problem
2. Subgroups of $\mathsf{GSp}_{2g}(\mathbb{F}_\ell)$
3. Semistable abelian varieties
4. Irreducibility and Goldbach
5. Primitivity

Definition

*Let $t \in \mathbb{Z}_{>0}$. We say that $f(x) = \sum_{i=0}^{m} a_i x^i \in \mathbb{Z}_p[x]$ is a t-***Eisenstein polynomial** *of degree $m \in \mathbb{Z}_{>0}$ if it is monic and $\mathrm{ord}_p(a_i) \geq t$ for all $i \neq m$, while $\mathrm{ord}_p(a_0) = t$.*

Definition

Let $q_1, \ldots, q_k$ be prime numbers and let $t \in \mathbb{Z}_{>0}$.
Let $f(x) \in \mathbb{Z}_p[x]$ be a monic squarefree polynomial. Then $f(x)$ is of **type** *$t - \{q_1, \ldots, q_k\}$ if*

$$f(x) = h(x) \prod_{i=1}^{k} g_i(x - \alpha_i)$$

over $\mathbb{Z}_p[x]$, for some $\alpha_i \in \mathbb{Z}_p$ with $\overline{\alpha}_i \neq \overline{\alpha}_j$ (reduction) for all $i \neq j$, where $g_i(x) \in \mathbb{Z}_p[x]$ is a t-Eisenstein polynomial of degree q_i and $\overline{h}(x)$ is separable and such that $\overline{h}(\alpha_i) \neq 0$ for all i.

Definition

Let $f(x) \in \mathbb{Z}[x]$ be a monic squarefree polynomial. We say that f is of **type** $t - \{q_1, \ldots, q_k\}$ *at a prime p if $f(x) \in \mathbb{Z}_p[x]$ is of type $t - \{q_1, \ldots, q_k\}$.*

The notion of type can be expressed in terms of congruence conditions.

Theorem

Suppose that $f \in \mathbb{Z}_p[x]$ has type $t - \{q_1, \ldots, q_k\}$ with $q_i \neq 2, p$ for all i. Then for every $\ell \neq p$, the inertia group $I_{\mathbb{Q}_p}$ acts tamely on $H^1_{\acute{e}t}(C/\overline{\mathbb{Q}}_p, \mathbb{Q}_\ell)$ and on $J[\ell]$ through a quotient of order $2\prod_i q_i$. Moreover, the non-trivial eigenvalues (with multiplicity) of any generator τ of tame inertia are either

$$-\zeta_{q_1}, -\zeta_{q_1}^2, \ldots, -\zeta_{q_1}^{q_1-1}, \ldots, -\zeta_{q_k}, -\zeta_{q_k}^2, \ldots, -\zeta_{q_k}^{q_k-1} \quad \text{if } t \text{ is odd}$$

or

$$\zeta_{q_1}, \zeta_{q_1}^2, \ldots, \zeta_{q_1}^{q_1-1}, \ldots, \zeta_{q_k}, \zeta_{q_k}^2, \ldots, \zeta_{q_k}^{q_k-1} \quad \text{if } t \text{ is even.}$$

The main ingredient for the proof is the theory of clusters (Dokchitser T., Dokchitser V., Maistret and Morgan).

Lemma

Let p be an odd prime. Suppose that $f \in \mathbb{Z}_p[x]$ has type $t - \{q_1, \ldots, q_k\}$ where $q_1, \ldots, q_k$ are odd primes, coprime to pt. Suppose moreover that p is a primitive root modulo each of the q_i.
Then for every prime $\ell \neq p, q_1, \ldots, q_k$, the representation $V = (J[\ell] \otimes_{\mathbb{F}_\ell} \overline{\mathbb{F}}_\ell)_{ss}$ decomposes as a direct sum of one $(q_1 - 1)$-dimensional, one $(q_2 - 1)$-dimensional, ..., one $(q_k - 1)$-dimensional irreducible $G_{\mathbb{Q}}$-subrepresentation, and all other irreducible constituents being 1-dimensional.

Lemma

Let q_1, q_2 and q_3 be primes such that $q_1 < q_2 < q_3 < 2g + 2$ and $q_1 + q_2 = 2g + 2$.
Suppose $f \in \mathbb{Z}[x]$ has type $1 - \{q_1, q_2\}$ at an odd prime p_2 and type $2 - \{q_3\}$ at an odd prime p_3, where p_2 is a primitive root modulo q_1 and q_2; and p_3 is a primitive root modulo q_3.
Then for every prime $\ell \neq q_1, q_2, q_3, p_2, p_3$, the $G_{\mathbb{Q}}$-module $J[\ell]$ is absolutely irreducible.

Theorem

Let g be a positive which satisfies $(2\mathrm{G}+\epsilon)$

$$2g+2 = q_1 + q_2 = q_4 + q_5 \qquad 2g+2 > q_3 > q_5 > q_2 \geq q_1 > q_4.$$

Suppose $f \in \mathbb{Z}[x]$ has type $1-\{q_1, q_2\}$ at an odd prime p_2, type $1-\{q_4, q_5\}$ at an odd prime p_2', type $2-\{q_3\}$ at an odd prime p_3 and type $2-\{q_5\}$ at an odd prime p_3', where:

- *p_2 is a primitive root modulo q_1 and q_2;*
- *p_2' is a primitive root modulo q_4 and q_5;*
- *p_3 is a primitive root modulo q_3;*
- *p_3' is a primitive root modulo q_5.*

Then for every prime ℓ, the $G_{\mathbb{Q}}$-module $J[\ell]$ is absolutely irreducible.

Proof.

Applying the previous Lemma with q_1, q_2, q_3, proves the claim for all $\ell \neq p_2, p_3, q_1, q_2, q_3$. Applying the lemma again with q_4, q_5, q_3 and with q_1, q_2, q_5 prove the result for all ℓ. □

Back to the example

$$
\begin{aligned}
f_0(x) = {} & x^{14} + 4296083454237577386357617132812 4x^{13} + 24399291199182822431034474546875 2x^{12} + \\
& + 37070735089946244550550864703125 6x^{11} + 37421714919975442859376216945312 0x^{10} + \\
& + 15348931724692510018604929880468 80x^{9} + 82387706490846067993195731453126 4x^{8} + \\
& + 65346121091991983799707939904687 36x^{7} + 21800226241411091796978043986718 72x^{6} + \\
& + 18639462316630739282360234458203 136x^{5} + 35314697076042559923507567914687 488x^{4} + \\
& + 12109949171284399693931828613156 2496x^{3} + 21208050929196640513538662762843 7504x^{2} + \\
& + 32088609535734483133061916917156 2496x + 73534831509566623615162682400000 0000
\end{aligned}
$$

$$N = p_t^2 \cdot p_t'^2 \cdot p_{lin} \cdot p_{irr} \cdot p_2^3 \cdot p_2'^3 \cdot p_3^3 \cdot p_3'^3 \cdot 2^{2g+2} \cdot \prod_{3 \le p \le g} p^{g+1} =$$

$$= 7^2 \cdot 11^2 \cdot 23 \cdot 29 \cdot 19^3 \cdot 41^3 \cdot 37^3 \cdot 17^3 \cdot 2^{14} \cdot 3^7 \cdot 5^7 = 1302357892577232237180900238080000000$$

$f_0 \equiv (x^7 - 19) \cdot ((x-1)^7 - 19) \bmod 19^3$	type 1 − $\{7, 7\}$	at 19
$f_0 \equiv (x^{11} - 41) \cdot ((x-1)^3 - 41) \bmod 41^3$	type 1 − $\{3, 11\}$	at 41
$f_0 \equiv (x^{13} - 37^2) \cdot (x+1) \bmod 37^3$	type 2 − $\{13\}$	at 37
$f_0 \equiv (x^{11} - 17^2) \cdot (x^3 + x + 14) \bmod 17^3$	type 2 − $\{11\}$	at 17

1. Abelian varieties and the inverse Galois problem
2. Subgroups of $\mathsf{GSp}_{2g}(\mathbb{F}_\ell)$
3. Semistable abelian varieties
4. Irreducibility and Goldbach
5. Primitivity

Definition

A symplectic representation V of $G_{\mathbb{Q}}$ is **quasi-unramified** *if for every $G_{\mathbb{Q}}$-stable decomposition $V = \oplus_{i=1}^{k} V_i$ into symplectic $\mathbb{F}_\ell$-subspaces, the permutation action of $G_{\mathbb{Q}}$ on $\{V_1, \ldots, V_k\}$ is unramified at every prime.*

Proposition

If $\ell \geq 5$ and V is an irreducible quasi-unramified symplectic representation of $G_{\mathbb{Q}}$, then $G_{\mathbb{Q}}$ has full image in $\mathrm{GSp}(V)$ provided that some element of $G_{\mathbb{Q}}$ acts as a transvection.

Proof.

The lemma follows from the Hermite-Minkowski theorem combined with the classification theorem.
Assume V is imprimitive and write $V = \oplus_{i=1}^{h} V_i$ where V_i are non-singular symplectic subspaces of dimension $2m < 2g$. Then there is some $\phi : G \to S_h$ with transitive image such that $\sigma(V_i) = V_{\phi(\sigma)(i)}$. Let

$$G_{\mathbb{Q}} \xrightarrow[\bar{\rho}]{} G \xrightarrow[\phi]{} S_h, \qquad \pi = \phi \circ \bar{\rho} : G_{\mathbb{Q}} \to S_h$$

Let $H = \ker(\pi)$. Then $H = G_K$ for some number field $K/\mathbb{Q}$. By hypothesis 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. □

Constructing hyperelliptic curves with surjective Galois representations

Samuele Anni
joint with Vladimir Dokchitser

University of Warwick

Automorphic Forms: theory and computation
King's College London, 6th September 2016

Thanks!