Research report:
Compatible systems of symplectic Galois representations and the inverse Galois problem

Sara Arias-de-Reyna

February 2014

Together with L. Dieulefait, S.W. Shin and G. Wiese, we have completed a project on the realization of (projective) symplectic groups over finite fields as Galois groups over $\mathbb{Q}$, making use of the compatible systems of Galois representations attached to certain automorphic forms (cf. [1], [2], [3]).

As a motivation for our work, consider a principally polarized n-dimensional abelian variety A defined over $\mathbb{Q}$. Then, for all prime numbers ℓ, we can consider the ℓ-torsion Galois representation

$$\overline{\rho}_{A,\ell} : G_{\mathbb{Q}} \to \mathrm{GSp}(A[\ell], e_\ell) \simeq \mathrm{GSp}_{2n}(\mathbb{F}_\ell),$$

where $G_{\mathbb{Q}}$ denotes the absolute Galois group of $\mathbb{Q}$ and e_ℓ is the Weil pairing on $A[\ell]$. If $\overline{\rho}_{A,\ell}$ is surjective, we obtain a realization of $\mathrm{GSp}_{2n}(\mathbb{F}_\ell)$ as a Galois group over $\mathbb{Q}$. Choosing a suitable abelian variety (e.g. [7]), it can be proven that, for all sufficiently large ℓ, $\mathrm{GSp}_{2n}(\mathbb{F}_\ell)$ can be realized as the Galois group of an extension $K/\mathbb{Q}$. Moreover, $K/\mathbb{Q}$ ramifies only at ℓ and the primes dividing the conductor of A.

We could try to replace the field $\mathbb{F}_\ell$ by $\mathbb{F}_{\ell^d}$, for some fixed integer $d \geq 1$. This naturally leads us to consider compatible systems of symplectic Galois representations $\rho_\bullet = (\rho_\lambda)_\lambda$, where λ runs through the primes of a number field L, and

$$\rho_\lambda : G_{\mathbb{Q}} \to \mathrm{GSp}_{2n}(\overline{L}_\lambda),$$

where $\overline{L}_\lambda$ denotes an algebraic closure of the completion of L at the prime λ, and ℓ denotes the rational prime below λ. The result we obtain is the following.

Theorem 1 (A., Dieulefait, Shin, Wiese). *Let $n, d \in \mathbb{N}$. There exists a positive density set $\mathcal{L}$ of rational primes such that, for every prime $\ell \in \mathcal{L}$, the group $\mathrm{PGSp}_{2n}(\mathbb{F}_{\ell^d})$ or $\mathrm{PSp}_{2n}(\mathbb{F}_{\ell^d})$ can be realized as a Galois group over $\mathbb{Q}$. The corresponding number field ramifies at most at ℓ and two more primes, which are independent of ℓ.*

This result generalizes to the n-dimensional setting the work of Dieulefait and Wiese on the realization of groups of the form $\mathrm{PGL}_2(\mathbb{F}_{\ell^d})$ and $\mathrm{PSL}_2(\mathbb{F}_{\ell^d})$ (see [6]). In the terminology introduced in Gabor Wiese's report on applications of modular Galois representations to the inverse Galois problem, the theorem presented above can be encompassed in the *horizontal direction*, complementing the results in the *vertical direction* due to Wiese in the 2-dimensional setting (cf. [10]) and Khare, Larsen and Savin for symplectic groups of arbitrary dimension (cf. [8]).

I want to thank Gabor Wiese for his remarks on a first version of this report.

To prove this result, we need to address the following questions:

1: Find conditions ensuring that the image of the residual Galois representation $\overline{\rho}_\lambda : G_\mathbb{Q} \to \mathrm{GSp}_{2n}(\overline{\mathbb{F}}_\ell)$ is *huge*, i.e., contains the subgroup $\mathrm{Sp}_{2n}(\mathbb{F}_\ell)$ (note that if $\mathrm{Im}\overline{\rho}_\lambda$ is huge, then the projective image of $\overline{\rho}_\lambda$ is $\mathrm{PGSp}_{2n}(\mathbb{F}_{\ell^r})$ or $\mathrm{PSp}_{2n}(\mathbb{F}_{\ell^r})$ for some $r \in \mathbb{N}$).

A key observation is that the classification of the finite subgroups of $\mathrm{GSp}_{2n}(\overline{\mathbb{F}}_\ell)$ containing a transvection is quite simple.

Theorem 2. *Let $G \subset \mathrm{GSp}_{2n}(\overline{\mathbb{F}}_\ell)$ be a finite subgroup containing a transvection. Then G is either reducible, imprimitive, or it contains $\mathrm{Sp}_{2n}(\mathbb{F}_\ell)$.*

If $G = \mathrm{Im}\overline{\rho}_\lambda$, this theorem implies that $\overline{\rho}_\lambda$ is either reducible, induced from an open subgroup of $G_\mathbb{Q}$, or has huge image. We assume that $\mathrm{Im}\overline{\rho}_\lambda$ contains a transvection, and look for conditions ensuring that the other two possibilities cannot occur. The reducible case can be ruled out if the compatible system possesses a maximally induced place of order p, which is a generalization to the n-dimensional setting, due to Khare, Larsen and Savin (cf. [8]), of the notion of good-dihedral prime appearing in the work of Khare and Wintenberger on Serre's Modularity Conjecture. To rule out the induced case for ℓ sufficiently large, we need to assume some regularity condition for the restriction of $\overline{\rho}_\lambda$ to a decomposition group at ℓ.

2: Determine the smallest field $\mathbb{F}(\lambda)$ such that the image of the composition $\overline{\rho}_\lambda^{\mathrm{proj}}$ of $\overline{\rho}_\lambda$ with the projection $\mathrm{GSp}_{2n}(\overline{\mathbb{F}}_\ell) \to \mathrm{PGSp}_{2n}(\overline{\mathbb{F}}_\ell)$ can be defined over $\mathbb{F}(\lambda)$.

Assume that ρ_λ is (absolutely) residually irreducible. Then ρ_λ can be conjugated (in $\mathrm{GL}_{2n}(\overline{L}_\lambda)$) to take values in $\mathrm{GL}_{2n}(L_\lambda)$. Enlarging L if necessary, we may assume that $L/\mathbb{Q}$ is a Galois extension. The key ingredient to address this question is the notion of *inner twist*. Namely, a pair (γ, ε) consisting of an element $\gamma \in \mathrm{Gal}(L_\lambda/\mathbb{Q}_\ell)$ and a character $\varepsilon : G_\mathbb{Q} \to L_\lambda^\times$ is called an inner twist of ρ_λ if the representations ${}^\gamma\rho_\lambda$ and $\rho_\lambda \otimes \varepsilon$ are conjugated. Let $\Gamma_{\rho_\lambda} \subset \mathrm{Gal}(L_\lambda/\mathbb{Q}_\ell)$ be the subgroup of elements appearing in inner twists of ρ_λ, and $K_{\rho_\lambda} := L_\lambda^{\Gamma_{\rho_\lambda}}$. If $\rho_\bullet$ satisfies several conditions (e.g. huge residual image, bounded inertial weights), then for all except finitely many primes λ the residue field $\mathbb{F}(\lambda)$ of K_{ρ_λ} is the smallest field on which $\overline{\rho}_\lambda^{\mathrm{proj}}$ can be defined. Moreover, there exists a global field $K_{\rho_\bullet} \subset L$ such that K_{ρ_λ} is the completion of $K_{\rho_\bullet}$ at the prime below λ (except for finitely many λ).

3: Force the field $K_{\rho_\bullet}$ to contain as many primes λ of residue degree d as possible. Let p, q be two rational primes, let $\zeta_p \in \overline{\mathbb{Q}}$ be a primitive p-th root of unity, and let $\xi_p = \sum_{i=0}^{2n-1} \zeta_p^{q^i}$. The key observation is that the presence of a maximally induced place of order p at a prime $\mathfrak{q}$ above q implies that the cyclotomic field $\mathbb{Q}(\xi_p)$ is contained in $K_{\rho_\bullet}$. This implies that, for all $d | \frac{p-1}{2n}$, there exists a positive density set of rational primes ℓ such that $K_{\rho_\bullet}$ contains a prime λ above ℓ of residue degree d.

Once these three points have been addressed, we can formulate sufficient conditions on a compatible system $\rho_\bullet$ of symplectic Galois representations ensuring that the projective image of the residual representation $\overline{\rho}_\lambda$ will equal $\mathrm{PGSp}_{2n}(\mathbb{F}_{\ell^d})$ or $\mathrm{PSp}_{2n}(\mathbb{F}_{\ell^d})$, where ℓ runs through a positive density set $\mathcal{L}$ of rational primes as λ runs through the primes of L.

4: Find some object giving rise to a compatible system satisfying all the conditions above.

We exploit the compatible systems of Galois representations attached to regular, algebraic, essentially self-dual, cuspidal automorphic representations π of $\mathrm{GL}_{2n}(\mathbb{A}_{\mathbb{Q}})$. An additional condition on π ensures that these Galois representations have symplectic images (cf. [5]). We have to specify local conditions at two auxiliary primes (one to obtain a transvection in the image of ρ_λ, the other to obtain a maximally induced place of order p). Equivalently (via the Local Langlands Correspondence) we need to specify the local components of π at two finite places. The results of Shin on equidistribution of local components at a fixed prime in the unitary dual with respect to the Plancherel measure (cf. [9]) ensure the existence of the desired π. We still have to take care of the fact that the transvection contained in the image of ρ_λ may become trivial when we reduce mod λ. To ensure that this can occur only at a density zero set of rational primes ℓ, we use a level-lowering argument based on results of [4] over imaginary quadratic fields.

References

[1] Sara Arias-de-Reyna, Luis Dieulefait and Gabor Wiese. *Compatible systems of symplectic Galois representations and the inverse Galois problem I. Images of projective representations*. Preprint arXiv:1203.6546 (2013).

[2] Sara Arias-de-Reyna, Luis Dieulefait and Gabor Wiese. *Compatible systems of symplectic Galois representations and the inverse Galois problem II. Transvections and huge image*. Preprint arXiv:1203.6552 (2013).

[3] Sara Arias-de-Reyna, Luis Dieulefait, Sug Woo Shin and Gabor Wiese. *Compatible systems of symplectic Galois representations and the inverse Galois problem III. Automorphic construction of compatible systems with suitable local properties*. Preprint arXiv:1308.2192 (2013).

[4] Thomas Barnet-Lamb, Toby Gee, David Geraghty and Richard Taylor. *Potential automorphy and change of weight*. Annals of Mathematics, to appear (2013).

[5] Joël Bellaïche and Gaëtan Chenevier, *The sign of Galois representations attached to automorphic forms for unitary groups*, Compos. Math. **147** (2011), no. 5, 1337–1352.

[6] Luis Dieulefait and Gabor Wiese. *On modular forms and the inverse Galois problem*. Trans. Amer. Math. Soc. **363** (2011), no. 9, 4569–4584.

[7] Chris Hall. *An open-image theorem for a general class of abelian varieties*. With an appendix by Emmanuel Kowalski. Bull. Lond. Math. Soc. **43** (2011), no. 4, 703–711.

[8] Chandrashekhar Khare, Michael Larsen and Gordan Savin. *Functoriality and the inverse Galois problem*. Compos. Math. **144** (2008), no. 3, 541–564.

[9] Sug Woo Shin. *Automorphic Plancherel density theorem*. Israel J. Math. **192** (2012), no. 1, 83–120.

[10] Gabor Wiese. *On projective linear groups over finite fields as Galois groups over the rational numbers*. Modular forms on Schiermonnikoog, 343–350, Cambridge Univ. Press, Cambridge, 2008.