Applying modular Galois representations to the Inverse Galois Problem

Gabor Wiese[1], 5 February 2014

For many finite groups the Inverse Galois Problem (IGP) can be approached through modular/automorphic Galois representations. This report is about the **ideas** and the **methods** that my coauthors and I have used so far, and their **limitations** (in my experience).
In this report I will mostly stick to the case of 2-dimensional Galois representations because it is technically much simpler and already exhibits essential features; occasionally I'll mention n-dimensional symplectic representations; details on that case can be found in Sara Arias-de-Reyna's report on our joint work with Dieulefait and Shin.

Basics of the approach

The link between the IGP and Galois representations. Let $K/\mathbb{Q}$ be a finite Galois extension such that $G := \mathrm{Gal}(K/\mathbb{Q}) \subset \mathrm{GL}_n(\overline{\mathbb{F}}_\ell)$ is a subgroup. Then $G_\mathbb{Q} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \twoheadrightarrow \mathrm{Gal}(K/\mathbb{Q}) \hookrightarrow \mathrm{GL}_n(\overline{\mathbb{F}}_\ell)$ is an n-dimensional continuous Galois representation with image G. Conversely, given a Galois representation $\rho : G_\mathbb{Q} \to \mathrm{GL}_n(\overline{\mathbb{F}}_\ell)$ (all our Galois representations are assumed continuous), then $\mathrm{im}(\rho) \subset \mathrm{GL}_n(\overline{\mathbb{F}}_\ell)$ is the Galois group of the Galois extension $\overline{\mathbb{Q}}^{\ker(\rho)}/\mathbb{Q}$.

Source of Galois representations: abelian varieties. Let A be a GL_2-type abelian variety over $\mathbb{Q}$ of dimension d with multiplication by the number field $F/\mathbb{Q}$ (of degree d) with integer ring $\mathcal{O}_F$. Then for every prime ideal $\lambda \lhd \mathcal{O}_F$, the λ-adic Tate module of A gives rise to $\rho_{A,\lambda} : G_\mathbb{Q} \to \mathrm{GL}_2(\mathcal{O}_{F,\lambda})$. These representations are a special case of those presented next (due to work of Ribet and the proof of Serre's modularity conjecture).

Source of Galois representations: modular/automorphic forms. Let $f = \sum_{n=1}^\infty a_n e^{2\pi i n z}$ be a normalised Hecke eigenform of level N and weight k without CM (or, more generally, an automorphic representation of a certain type over $\mathbb{Q}$). The coefficients a_n are algebraic integers and $\mathbb{Q}_f = \mathbb{Q}(a_n \mid n \in \mathbb{N})$ is a number field, the **coefficient field** of f. Denote by $\mathbb{Z}_f$ its ring of integers. The eigenform f gives rise to a **compatible system of Galois representations**, that is, for every prime λ of $\mathbb{Q}_f$ a Galois representation $\rho_{f,\lambda} : G_\mathbb{Q} \to \mathrm{GL}_2(\mathbb{Z}_{f,\lambda})$ such that $\rho_{f,\lambda}$ is unramified outside $N\ell$ (where $(\ell) = \mathbb{Z} \cap \lambda$) and for all $p \nmid N\ell$ we have $\mathrm{Tr}(\rho_{f,\lambda}(\mathrm{Frob}_p)) = a_p$. All representations thus obtained are odd (determinant of complex conjugation equals -1).

Reduction and projectivisation. We consider the representations $\overline{\rho}_{f,\lambda} : G_\mathbb{Q} \xrightarrow{\rho_{f,\lambda}} \mathrm{GL}_2(\mathbb{Z}_{f,\lambda}) \twoheadrightarrow \mathrm{GL}_2(\mathbb{F}_{f,\lambda})$ and $\overline{\rho}^{\mathrm{proj}}_{f,\lambda} : G_\mathbb{Q} \xrightarrow{\overline{\rho}_{f,\lambda}} \mathrm{GL}_2(\mathbb{F}_{f,\lambda}) \twoheadrightarrow \mathrm{PGL}_2(\mathbb{F}_{f,\lambda})$, where $\mathbb{F}_{f,\lambda} = \mathbb{Z}_{f,\lambda}/\lambda$. In our research we focus on projective representations because the groups $\mathrm{PSL}_2(\mathbb{F}_{\ell^d})$ are simple for $\ell^d \geq 4$.
Main idea: By varying f and λ (and thus ℓ), realise as many finite subgroups of $\mathrm{PGL}_2(\overline{\mathbb{F}}_\ell)$ as possible.

Trust in the approach. If $\ell > 2$, the oddness of the representations leads to $\overline{\mathbb{Q}}^{\ker(\overline{\rho}^{\mathrm{proj}}_{f,\ell})}$ being totally imaginary. **The approach through modular Galois representations for the groups $\mathrm{PSL}_2(\mathbb{F}_{\ell^d})$ and $\mathrm{PGL}_2(\mathbb{F}_{\ell^d})$ to the IGP should in principle work** for the following reason: If $\mathrm{Gal}(K/\mathbb{Q}) \subset \mathrm{PGL}_2(\overline{\mathbb{F}}_\ell)$ is a finite (irreducible) subgroup and $K/\mathbb{Q}$ is totally imaginary (which is 'much more likely' than being totally real), then Serre's modularity conjecture implies that K can be obtained from some f and λ. In more general contexts, there are generalisations of Serre's modularity conjecture (however, unproved!) and I am inclined to believe that the approach is promising in more general contexts than just GL_2.

The two directions. We have so far explored two directions for the realisation of $\mathrm{PSL}_2(\mathbb{F}_{\ell^d})$ and $\mathrm{PSp}_n(\mathbb{F}_{\ell^d})$. **Vertical direction:** fix ℓ, let d run (results by me for PSL_2 [Wie08], generalised by Khare-Larsen-Savin for PSp_n [KLS08]); **horizontal direction:** fix d, let ℓ run (results by Dieulefait and me for PSL_2 [DW11] and by Arias-de-Reyna, Dieulefait, Shin and me for PSp_n [AdDSW13]).

Main challenges

In approaching the IGP through modular forms for specific groups, in my experience one is faced with two challenges:

(1) Control/predetermine the type of the image $\overline{\rho}^{\mathrm{proj}}_{f,\lambda}(G_\mathbb{Q})$.
(2) Control/predetermine the coefficient field $\mathbb{Q}_f$.

Problem (2) appears harder to me.

Controlling the type of the images. By a classical theorem of Dickson, if $\overline{\rho}_{f,\lambda}$ is irreducible, then it is either induced from a lower dimensional representation (only possiblity: a character) or $\overline{\rho}^{\mathrm{proj}}_{f,\lambda}(G_\mathbb{Q}) \in \{\mathrm{PSL}_2(\mathbb{F}_{\ell^d}), \mathrm{PGL}_2(\mathbb{F}_{\ell^d})\}$

[1]Université du Luxembourg, Faculté des Sciences, de la Technologie et de la Communication, 6, rue Richard Coudenhove-Kalergi, L-1359 Luxembourg, Luxembourg, gabor.wiese@uni.lu

for some d (we call this case **huge/big image**). Under the assumption of a transvection in the image, we have generalised this result to symplectic representations. In our applications we want to exclude reducibility and induction. One can expect a **generic huge image result** (for GL_2 this is classical work of Ribet; for other cases e.g. recent work of Larsen and Chin Yin Hui in this direction [HL13]).

Inner twists. If one has e.g. determined that $\overline{\rho}_{f,\lambda}^{\mathrm{proj}}(G_{\mathbb{Q}})$ is huge, one still needs to compute which $d \in \mathbb{N}$ and which of the two cases $\mathrm{PSL}_2(\mathbb{F}_{\ell^d})$, $\mathrm{PGL}_2(\mathbb{F}_{\ell^d})$ occurs. The answer is given by **inner twists**. For GL_2 these are well-understood (with Dieulefait we exclude them by a good choice of f); for PSp_n we proved a generalisation allowing us to describe d by means of a number field, but, as to now we are unable to distinguish between the two cases.

Coefficient field

One knows that $\mathbb{Q}_f$ is either totally real or totally imaginary (depending on the nebentype of f). Moreover, $[\mathbb{Q}_f : \mathbb{Q}] \leq \dim S_k(N)$, where $S_k(N)$ is the space of cusp forms of level N and weight k. Furthermore, a result of Serre says that for any sequence $(N_n, k_n)_n$ such that $N_n + k_n$ tends to infinity, there is $f_n \in S_{k_n}(N_n)$ such that $[\mathbb{Q}_{f_n} : \mathbb{Q}]$ tends to infinity. However, to the best of my knowledge, almost **nothing is known about the arithmetic of the coefficient fields and the Galois groups of their normal closures over** $\mathbb{Q}$. In my experience, this is the **biggest obstacle** preventing us from obtaining very strong results on the IGP.

Almost complete control through Maeda's conjecture. A conjecture of Maeda gives us some control on the coefficient field by claiming that for any $f \in S_k(1)$ one has $[\mathbb{Q}_f : \mathbb{Q}] = \dim S_k(1) =: m_k$ and that the Galois group of the normal closure of $\mathbb{Q}_f$ over $\mathbb{Q}$ is S_{m_k}, the symmetric group. The conjecture has been numerically tested for quite high values of k, but to my knowledge a proof is out of sight at the moment and there's no generalisation to higher dimensions either. Assuming Maeda's conjecture I was able to prove in [Wie13] that for even d the groups $\mathrm{PSL}_2(\mathbb{F}_{\ell^d})$ occur as Galois groups over $\mathbb{Q}$ with only ℓ ramifying for all ℓ, except possibly a density-0 set. In a nutshell, for the proof I choose a sequence f_n of forms of level 1 such that $[\mathbb{Q}_{f_n} : \mathbb{Q}]$ strictly increases. That the Galois group is the symmetric group ensures two things: firstly, every $\mathbb{Q}_{f_n}$ possesses a degree-d prime; secondly, the fields $\mathbb{Q}_{f_n}$ and $\mathbb{Q}_{f_m}$ for $m \neq n$ are almost disjoint (in the sense that their intersection is at most quadratic) and thus the sets of primes of degree d in the two fields are almost independent, so that their density adds up to 1 when $n \to \infty$. This illustrates that **some control on the coefficient field promises strong results on the IGP**.

A conjecture of Coleman on GL_2-type abelian varieties. The modular form f corresponding to a GL_2-type abelian variety with multiplication by F has coefficient field $\mathbb{Q}_f = F$. However, I don't know of any method to construct a GL_2-type abelian variety with multiplication by a given field. Indeed, a conjecture attributed to Coleman (see [BFGR06]) predicts that for a given dimension, only finitely many number fields occur. In other words, for weight-2 modular forms in all levels, there are only finitely many $\mathbb{Q}_f$ of a given degree. Under the assumption of Coleman's conjecture, it is impossible to obtain $\mathrm{PSL}_2(\mathbb{F}_{\ell^2})$ for all ℓ from GL_2-type abelian surfaces because there will be a positive density set of ℓ that are split in all number fields of degree 2 that occur as multiplication fields. Although I don't know if there are finitely or infinitely many quadratic fields occuring as $\mathbb{Q}_f$ for f of arbitrary level and arbitrary weight, this nevertheless suggests to me that one should make use of modular forms of **arbitrary coefficient degrees** for approaching $\mathrm{PSL}_2(\mathbb{F}_{\ell^d})$ for fixed d (as we did when we assumed Maeda's conjecture).

Numerical data. Some very simple computer calculations for $p = 2$ during my PhD have very quickly revealed that all $\mathrm{PSL}_2(\mathbb{F}_{2^d})$ with $1 \leq d \leq 77$ occur over $\mathbb{Q}$. With Marcel Mohyla we plotted $\mathbb{F}_{f,\lambda}$ for small fixed weight and f having prime levels [MW11]. The computations suggest that the maximum and the average degrees (for f in $S_k(N)$ for N prime) of $\mathbb{F}_{f,\lambda}$ are roughly proportional to the dimension of $S_k(N)$.

The local 'bad primes' approach to the main challenges

We need to gain some control on the coefficient fields and in the absence of a generic huge image result, we also need to force huge image of the Galois representation. In all our work (like in that of Khare-Larsen-Savin [KLS08]), we approach this by choosing suitable inertial types, or in the language of abelian varieties, by choosing certain types of bad reduction. The basic idea appeared in the work of Khare-Wintenberger on Serre's modularity conjecture. More precisely, one chooses inertial types at some primes q guaranteeing that $\overline{\rho}_{f,\lambda}(I_q)$ contains certain elements (I_q denotes the inertia group at q) . For instance, if an element that is conjugate to $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ is contained, the representation cannot be induced. In the n-dimensional symplectic case, we use this to obtain a transvection in the image, allowing us to apply our classification (see above). We also employ Khare-Larsen-Savin's generalisation of Khare-Wintenberger's good-dihedral primes. More precisely, for GL_2 we impose $\overline{\rho}_{f,\lambda}|G_{\mathbb{Q}_q} = \mathrm{Ind}_{\mathbb{Q}_{q^2}}^{\mathbb{Q}_q}(\alpha)$ where α is a character of $\mathbb{Q}_{q^2}^\times$ of prime order t not descending to $\mathbb{Q}_q^\times$. This has two uses: (1) As the representation is **irreducible** locally at q, so it is globally. (2) $\mathbb{Q}_f$ contains $\zeta_t + \zeta_t^{-1}$ (this follows from an explicit description of the induction). This **cyclotomic field in the coefficient field** can be exploited in two ways. (2a) By making t big, $[\mathbb{F}_{f,\lambda} : \mathbb{F}_\ell]$ becomes big. **This leads to the results in the vertical direction.** (2b) Given d, by choosing t suitably, $\mathbb{Q}(\zeta_t + \zeta_t^{-1})$

contains prime ideals of degree d, thus $\mathbb{Q}_f$ **contains prime ideals of degree d, which makes the results in the horizontal direction work**. In the absence of any knowledge on the Galois closure of $\mathbb{Q}_f$ over $\mathbb{Q}$ in general, I do not know of any other way to guarantee that degree-d primes exist at all (we need them to realise $\mathrm{PSL}_2(\mathbb{F}_{\ell^d})$).
My feeling is that the cyclotomic field $\mathbb{Q}(\zeta_t + \zeta_t^{-1})$ only makes up a very small part of the coefficient field, i.e. that $[\mathbb{Q}_f : \mathbb{Q}]$ will be much bigger than $[\mathbb{Q}(\zeta_t + \zeta_t^{-1}) : \mathbb{Q}]$. Thus, in our results in the horizontal direction, for given d and f, we only obtain very small densities. Moreover, I cannot prove that by varying f for fixed d, the sets of primes of residue degree d are not contained in each other. Any information, for instance, on the ramification of $\mathbb{Q}_f$ changing with f or on the Galois group would probably enable us to obtain a big density by taking the union of the sets of degree-d primes for many f.

Constructing the relevant modular/automorphic forms

For finishing the approach, one must finally construct or show the existence of modular/automorphic forms having the required inertial types. For modular forms one can do this in quite a down-to-earth way by using level raising. This approach was taken in the work by Dieulefait and me. In the symplectic case, we exploit work of Shin, as well as level-lowering results of Barnet-Lamb, Gee, Geraghty and Taylor [BLGGT13]. Khare-Larsen-Savin [KLS08] use other automorphic techniques.

Conclusion

The presented approach to the IGP for many families of finite groups through automorphic representations seems in principle promising. In my opinion, the main obstacle is a poor understanding of the coefficient fields.
The approach has the advantage that it allows **full control on the ramification**. A disadvantage is that one does not obtain a regular realisation.

Acknowledgements. I thank Sara Arias-de-Reyna for valuable comments on a first draft of this report.

References

[AdDSW13] 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 (2013).

[BFGR06] Nils Bruin, E. Victor Flynn, Josep González, and Victor Rotger, *On finiteness conjectures for endomorphism algebras of abelian surfaces*, Math. Proc. Cambridge Philos. Soc. **141** (2006), no. 3, 383–408. MR 2281405 (2008b:14076)

[BLGGT13] Thomas Barnet-Lamb, Toby Gee, David Geraghty, and Richard Taylor, *Potential automorphy and change of weight*, Annals of Mathematics, to appear (2013).

[DW11] Luis Dieulefait and Gabor Wiese, *On modular forms and the inverse Galois problem*, Trans. Amer. Math. Soc. **363** (2011), no. 9, 4569–4584.

[HL13] C. Y. Hui and M. Larsen, *Adelic openness without the Mumford-Tate conjecture*, arXiv:1312.3812 (2013).

[KLS08] Chandrashekhar Khare, Michael Larsen, and Gordan Savin, *Functoriality and the inverse Galois problem*, Compos. Math. **144** (2008), no. 3, 541–564.

[MW11] Marcel Mohyla and Gabor Wiese, *A computational study of the asymptotic behaviour of coefficient fields of modular forms*, Actes de la Conférence "Théorie des Nombres et Applications", Publ. Math. Besançon Algèbre Théorie Nr., Presses Univ. Franche-Comté, Besançon, 2011, pp. 75–98. MR 2894269

[Wie08] Gabor Wiese, *On projective linear groups over finite fields as Galois groups over the rational numbers*, Modular forms on Schiermonnikoog, Cambridge Univ. Press, Cambridge, 2008, pp. 343–350. MR 2530980 (2010i:11079)

[Wie13] ______, *An application of Maeda's Conjecture to the Inverse Galois Problem*, arXiv:1210.7157v3 (2013).