EXPLICIT ASPECTS OF GEOMETRIC GALOIS REPRESENTATIONS

GABRIEL CHÊNEVERT

McGill University Ph.D. thesis summary

Since the 90s, we know that all elliptic curves defined over $\mathbf{Q}$ are modular, and the (almost proven) Serre conjectures imply that the same is true more generally for every odd 2-dimensional Galois representation coming from the cohomology of varieties defined over $\mathbf{Q}$. However, even if this gives in theory a finite method to determine the relevant modular form from defining equations for the variety, in practice it is rarely feasible in reasonable time. So this raises two main issues: 1) how to specify, and "compute", Galois representations arising in the cohomology of arithmetic varieties; and 2) how to determine the automorphic (modular) forms corresponding (conjecturally in the general case) to these representations. Some results and leads are discussed here, illustrated on an example related to the distribution of certain exponential sums.

General setting

Let X be an arithmetic variety defined over a number field K; here we assume X is smooth and proper for simplicity. For any constructible E_λ-sheaf $\mathcal{F}_\lambda$ on X, where E_λ is a finite extension of $\mathbf{Q}_\ell$, the *étale cohomology groups*

$$H^\bullet(X, \mathcal{F}_\lambda) := \bigoplus_{i=0}^{2\dim X} H^i_{\text{ét}}(X_{\overline{K}}, \mathcal{F}_\lambda)$$

are finite-dimensional graded E_λ-vector spaces on which the absolute Galois group G_K acts linearly. For example, if X is an abelian variety (e.g. an elliptic curve), then

$$H^i(X, \mathbf{Q}_\ell) = \wedge^i H^1(X, \mathbf{Q}_\ell) = \wedge^i V_\ell(X)^\vee,$$

where $V_\ell(X) = T_\ell(X) \otimes_{\mathbf{Z}_\ell} \mathbf{Q}_\ell$ is the ℓ-adic Tate module of X, of dimension $2\dim X$.

Now let E be another number field and $\mathcal{F}$ an E-constructible sheaf on X. For every finite place λ of E, we denote by E_λ the completion of E with respect to the λ-adic norm. Then $\mathcal{F}_\lambda := \mathcal{F} \otimes E_\lambda$ is an E_λ-constructible sheaf, and the trace formula of Grothendieck implies that

$$H^\bullet(X, \mathcal{F}) := \big(H^\bullet(X, \mathcal{F}_\lambda)\big)_\lambda$$

is a *compatible system of E-rational λ-adic Galois representations*: for every prime $\mathfrak{p}$ at which X has good reduction, and for every λ away from $\mathfrak{p}$, the λ-adic representation $H^\bullet(X, \mathcal{F}_\lambda)$ is unramified at $\mathfrak{p}$ and the (graded) characteristic polynomial

$$\det(1 - t\mathrm{Frob}_\mathfrak{p} \mid H^\bullet(X, \mathcal{F}_\lambda)) \in E_\lambda(t)$$

of the Frobenius substitution $\mathrm{Frob}_\mathfrak{p}$ at $\mathfrak{p}$ has coefficients in E, and is independent of λ.

This allows one to define the *Hasse-Weil zeta function*

$$\zeta(X, \mathcal{F}; s) := \prod_{\mathfrak{p} \notin \mathrm{Ram}\, X} \det(1 - N\mathfrak{p}^{-s}\mathrm{Frob}_\mathfrak{p} \mid H^\bullet(X, \mathcal{F}))^{-1},$$

which converges for $\Re s > \dim X + 1$ and encodes the information about the number of points of X over (most) finite fields.

Modularity

For example, if X is an elliptic curve over $\mathbf{Q}$, then

$$\zeta(X, \mathbf{Q}; s) = \zeta(s)\zeta(s-1)\prod_p (1 - a_p(X)p^{-s} + p^{1-s})$$

where $a_p(X)$ is the number of points of X over $\mathbf{F}_p$ when it has good reduction. By the celebrated Modularity Theorem [2, 19], the coefficients $a_p(X)$ are the Hecke eigenvalues $a_p(f)$ of a rational modular form f of weight 2 and level the conductor N_X of X.

This is a purely representation-theoretic statement, since Deligne [4] described how to attach to every cusp eigenform $f \in S_k^{\mathrm{new}}(N, \varepsilon)$, $k \geq 2$, a 2-dimensional compatible system ρ_f of $\mathbf{Q}(f)$-rational ℓ-adic representations, unramified outside N, satisfying

$$\det \rho_f = \varepsilon \chi^{k-1} \qquad \text{and} \qquad \operatorname{tr} \rho_f(\mathrm{Frob}_p) = a_p(f) \quad \text{for } p \not| N,$$

where $\chi = (\chi_\ell)_\ell$ is the cyclotomic character. Thus the Modularity Theorem can be rephrased as: the compatible system of representations $H^1(X, \mathbf{Q})$ is isomorphic to ρ_f for some rational $f \in S_2^{\mathrm{new}}(N_X, 1)$.

Assuming the full Serre conjectures (proved at least for odd conductor [11]), the following more general result holds.

Theorem 1 ([10, 17])**.** *Let ρ be an odd irreducible 2-dimensional subquotient of $H^\bullet(X, \mathbf{Q})$ of Hodge-Tate weights $a < b$, where X is defined over $\mathbf{Q}$. Then*

$$\rho \simeq \chi^{-a} \otimes \rho_f,$$

where f is a newform of weight $b - a + 1$, character $\varepsilon = \chi^{2a} \det \rho$, and level dividing $N := \prod_{p \in \mathrm{Ram}\, \rho} N_p$ with

$$N_p = \begin{cases} 2^8 & \text{if } p = 2 \notin \mathrm{Ram}\,(\det \rho) \\ 2^{11} & \text{if } p = 2 \in \mathrm{Ram}\,(\det \rho) \\ 3^5 & \text{if } p = 3 \\ p^2 & \text{if } p > 5. \end{cases}$$

Thus if ρ is known explicitely (in the sense that for every unramified prime p we know how to compute $\operatorname{tr} \rho(\mathrm{Frob}_p)$), and k, N, ε are given by the theorem, we can determine precisely which eigenform $f \in S_k(N, \varepsilon)$ corresponds to ρ by computing the traces of ρ for primes up to [14]

$$\frac{k}{12} N \prod_{p|N} \left(1 + \frac{1}{p}\right).$$

The problem with that approach is that often we do not know the precise ramification set $\mathrm{Ram}\, \rho$ of the representation; in that situation the best we can do is replace $\mathrm{Ram}\, \rho$ with the (possibly bigger) set $\mathrm{Ram}\, X$ of primes of bad reduction for X to get a (possibly much bigger) bound $\prod_{p \in \mathrm{Ram}\, X} N_p$ on the level of the modular form, which can render this algorithm inapplicable in practice.

The best way around this would be able to read more information about the ramification of ρ from the geometry of X. For instance, if X admits a semistable model, then the Galois representation on its cohomology is tamely ramified and this allows one to improve the bound in the theorem.

Another approach is to make an educated guess (from numerical evidence) for the modular form f, and then proceed to show directly that the compatible system ρ is isomorphic to ρ_f.

The Faltings-Serre method

Faltings [5] remarked, and Serre [16] turned into a working tool, the fact that the equivalence of two continuous λ-adic Galois representations is something which can in principle be determined on some finite extension of the base field (even though the representations themselves need not factor through a finite quotient).

Let $\mathcal{O}_\lambda$ be the ring of integers in a finite extension of $\mathbf{Q}_\ell$ and consider $\rho_1, \rho_2 : G \to \mathrm{GL}_n(\mathcal{O}_\lambda)$ two semisimple representations of a group G. Denote by M the image of $\mathcal{O}_\lambda[G]$ in $\mathrm{M}_n(\mathcal{O}_\lambda) \times \mathrm{M}_n(\mathcal{O}_\lambda)$ by the linear map induced by $\rho_1 \times \rho_2$, and $\delta(G)$ the image of G in $(M/\lambda M)^\times$. We call $\delta(G)$ the *deviation group* of the pair (ρ_1, ρ_2).

One can prove that $\delta(G)$ is a finite quotient of G (of order no more than $N(\lambda)^{2n^2}$), unramified outside $\mathrm{Ram}\, \rho_1 \cup \mathrm{Ram}\, \rho_2$, and having the property that for any $\Sigma \subseteq G$ surjecting onto $\delta(G)$,

$$\rho_1 \simeq \rho_2 \iff \operatorname{tr} \rho_1|_\Sigma = \operatorname{tr} \rho_2|_\Sigma.$$

In special cases, it is possible to turn this into a usable criterion, e.g. Serre's method of quartic fields [16] or the following in the case of 2-adic representations *with even trace* [13].

Theorem 2. *Let K be a number field, E_λ a finite extension of $\mathbf{Q}_2$, $\rho_1, \rho_2 : G_K \to \mathrm{GL}_2(E_\lambda)$ two semisimple representations with even trace, same determinant, and unramified outside S. Let $\Sigma \subseteq G_K$ be a set surjecting onto $\mathrm{Gal}(K_S^{(2)}/K)$, where $K_S^{(2)}$ is the compositum of all quadratic extensions of K which are unramified outside S. Then*

$$\rho_1 \simeq \rho_2 \iff \operatorname{tr} \rho_1|_\Sigma = \operatorname{tr} \rho_2|_\Sigma.$$

In this form, the Faltings-Serre method was used to explicitly prove many instances of modularity over $\mathbf{Q}$: Schoen's singular quintic 3-fold [15, 17], Livné's singular cubic 7-fold [13], and more recently for a lot of K3 surfaces and rigid Calabi-Yau manifolds [8]. It was also used recently for Hilbert modular forms [18].

For $K = \mathbf{Q}$, this criterion involves at most $2^{|S|+1}$ checks. In my thesis I proved the following result, which generalizes Serre's original quartic fields method to the case where the above criterion fails.

Theorem 3. *Let K be a number field, $\rho_1, \rho_2 : G_K \to \mathrm{GL}_2(\mathbf{Z}_2)$ two semisimple representations with traces of the same parity but not identically even, having the same determinant, and unramified outside a set S of primes of K. Let L be the Galois extension of K cut out by the kernel of the modulo 2 representations, and $\Sigma \subseteq G_K$ be a set surjecting onto $\mathrm{Gal}(L'/K)$ for every Galois extension L'/K containing L, unramified outside S, and such that, as $\mathrm{Gal}(L/K)$-modules,*

$$\mathrm{Gal}(L'/K) \simeq \mathbf{Z}/2\mathbf{Z} \text{ or } V_4^r, \quad \text{with } r \leq \begin{cases} 1 & \text{if } \mathrm{Gal}(L/K) \simeq S_3, \\ 5 & \text{if } \mathrm{Gal}(L/K) \simeq \mathbf{Z}/3\mathbf{Z}. \end{cases}$$

Then $\rho_1 \simeq \rho_2 \iff \operatorname{tr} \rho_1|_\Sigma = \operatorname{tr} \rho_2|_\Sigma$.

Notice that this criterion is strictly more efficient than first establishing the equivalence of ρ_1 and ρ_2 as representations of G_L using the original Faltings-Serre method, and then arguing using Frobenius reciprocity that they agree as representations of G_K, as was done in [18]. The proof uses a delicate bootstrap argument involving the deviation group.

A modular cubic 4-fold

Consider the variety $W_n \subseteq \mathbf{P}^{n-1}$ defined by

$$\sum_{i=1}^n x_i = \sum_{i=1}^n x_i^3 = 0.$$

For $n > 5$, W_n is an irreducible variety of dimension $n-3$ admitting an action of S_n by permutation of the coordinates. This family was studied by Livné in connection with Birch's conjecture on the distribution of cubic exponential sums [12]. In particular, it was proven in [13], using the Faltings-Serre-Livné criterion for even trace representations, that W_{10} is modular (the only interesting piece of its cohomology is 2-dimensional).

Using my generalization of the Faltings-Serre-Livné criterion (Theorem 3), I was able to prove the following.

Theorem 4. *The zeta function of the smooth variety W_7 of dimension 4 is given by*

$$\zeta(W_7, s) = \zeta(s)\zeta(s-1)\zeta(s-3)\zeta(s-4)\zeta(s-2)^{15} L(\varepsilon_5, s-2)^6 L(f, s-1)$$

where $f \in S^{\mathrm{new}}(35, \varepsilon_{35})$, and ε_d denotes the quadratic character of conductor d.

To prove this, the first step is to decompose the cohomology of W_7 into isotypical components for the action of S_7. The following fact is needed, which is implicitly present in [6, 7] but stated here in a more precise and general form.

Theorem 5. *Let X be a variety defined over a number field K, G a finite group of automorphims of X such that the quotient X/G exists, and $\mathcal{F}$ a G-equivariant E-constructible sheaf on X, where E is a finite extension of $\mathbf{Q}$. As a $G \times G_K$-module, the cohomology decomposes into G-isotopical components*

$$H^\bullet(\overline{X}, \mathcal{F}) = \bigoplus_{\phi \in \mathrm{Irr}_E(G)} H^\bullet(\overline{X}, \mathcal{F})_\phi \otimes_{E_\phi} W_\phi$$

where the sum ranges over all irreducible representations ϕ of G over E, W_ϕ is a vector space on which G acts via ϕ, and $E_\phi = \mathrm{End}_E(W_\phi)$. Then each "multiplicity"

$$H^\bullet(\overline{X},\mathcal{F})_\phi = \mathrm{Hom}_G(W_\phi, H^\bullet(\overline{X},\mathcal{F}))$$

is an E-rational compatible system of λ-adic representations.

To compute this isotypical decomposition, it is sometimes possible to obtain the character of the action using the Lefschetz fixed point formula. In the case of S_n acting on $H^\bullet(W_n)$, I proved the following.

Theorem 6. *Let $n > 5$ be an odd integer (so that W_n is smooth) and let χ_{pr} denote the character of the symmetric group S_n acting on the primitive cohomology of W_n. For $\sigma \in S_n$, write $m_d(\sigma)$ for the number cycles of order divisible by d in its disjoint cycles decomposition. Then*

$$\chi_{\mathrm{pr}}(\sigma) = \frac{(-2)^{m_1(\sigma)-1} - (-2)^{m_3(\sigma)+1}}{3}.$$

For example, for $\sigma = (123)(456)(78) \in S_9$, we have $m_1(\sigma) = 4$, $m_2(\sigma) = 1$, $m_3(\sigma) = 2$ and $m_d(\sigma) = 0$ for $d \geq 4$, so that $\chi_{\mathrm{pr}}(\sigma) = 0$. I got similar formulas involving the class functions m_d for other representations of the symmetric groups on families of symmetric hypersurfaces of varying dimension. A careful analysis of these formulas seems both subtle and interesting from a combinatorical point of view.

For W_7, it turns out that all irreducible representations which appear occur with multiplicity 1, and the corresponding linear Galois characters are easily computed, except for the alternating representation which occurs with multiplicity 2 in the primitive cohomology.

Theorem 7. *Let ρ denote the representation of $G_{\mathbf{Q}}$ on $H^4_{\mathrm{pr}}(W_7,\mathbf{Q})(-1)$. Then $\mathrm{Ram}\,\rho \subseteq \{3,5,7\}$, $\det\rho = \varepsilon_{35}\chi^2$ and*

$$\mathrm{tr}\,\rho(\mathrm{Frob}_p) = \frac{V_7(p)}{p^3(p-1)} - 14p - 6\left(\frac{p}{5}\right)p$$

for $p \neq 3,5,7$, where

$$V_n(p) = \sum_{\substack{a,b\in\mathbf{F}_p\\ a\neq 0}} \left\{\sum_{x\in\mathbf{F}_p} \exp\left(\frac{2\pi i}{p}(ax^3+bx)\right)\right\}^n.$$

From the Serre conjecture (unconditionally here because 2 is not ramified), we get that ρ comes from a newform $g \in S_3(N,\varepsilon_{35})$ with $35 \mid N \mid 3^5 5^2 7^2 = 297675$. Thus, to find the exact modular form would involve computing the traces for primes up to 119070. However, an application of the generalized Faltings-Serre-Livné criterion requires significatively less computations.

Equidistribution of exponential sums

For any fixed degree $k > 1$, one can consider the average limit distribution as $p \to \infty$ of the exponential sums

$$B_k(a,b;p) := \sum_{x=0}^{p-1} \exp\left(\frac{2\pi}{p}(ax^k+bx)\right), \qquad a \neq 0.$$

In his paper [13], Livné proves an analogue of the Sato-Tate conjecture, first formulated by Birch [1], in the case $k = 3$. He achieved this by relating these exponential sums with the number of points over finite fields, hence the étale cohomology, of the varieties W_n introduced above. For a general k, the moments of the limit distribution are related to the number of points of the projective varieties $W_k^{m,n} \subseteq \mathbf{P}^{m+n-1}$ defined in the homogeneous coordinates $x_1,\ldots,x_m,y_1,\ldots,y_n$ by

$$\sum_{i=1}^m x_i = \sum_{j=1}^n y_j, \qquad \sum_{i=1}^m x_i^k = \sum_{j=1}^n y_j^k.$$

The situation becomes considerably more complicated, but using the fact that these varieties admit $S_m \times S_n$ as automorphisms, I was able in many cases to compute the Galois representation supported by the cohomology groups of these varieties (or their desingularization). This yields asymptotics for the corresponding moments of the distribution of the sums $B_k(a,b;p)$ along certain families of primes. However, I am not aware of a simple description of the limit distributions like in the case $k = 3$.

References

[1] B. Birch, *How the number of points of an elliptic curve over a fixed prime field varies*, J. London Math. Soc. **43** (1968), 57–60.

[2] C. Breuil, B. Conrad, F. Diamond, R. Taylor, *On the modularity of elliptic curves over* $\mathbf{Q}$*: Wild 3-adic exercises*, Journ. AMS 14 (2001), 843–939.

[3] C. Consani, J. Scholten, *Arithmetic on a quintic threefold*, International Journal of Mathematics **12**, n° 8 (2001), 943–972.

[4] P. Deligne, *Formes modulaires et représentations* ℓ*-adiques*, Séminaire Bourbaki, **11** (1968-1969), exposé no. 355, 34 p.

[5] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (1983), 349–366.

[6] A. Grothendieck, *Formule de Lefschetz et rationalité des fonctions L*, Sém. Bourbaki 1964/65, 279, 15 p.

[7] P. Deligne, G. Lusztig, *Representations of reductive groups over finite fields*, Ann. Math. 2 **103** (1976), no. 1, 103–161.

[8] K. Hulek, R. Kloosterman, M. Schütt, *Modularity of Calabi-Yau varieties* in Global aspects of complex geometry, Springer (2006), 271–309.

[9] A. J. de Jong, *Smoothness, semi-stability and alterations*, Publ. Math. IHÉS, **83** (1996), 51–93.

[10] C. Khare, *Modularity of Galois representations and motives with good reduction properties*, J. Ramanujan Math. Soc. **22**, n° 1 (2007), 1–26.

[11] C. Khare, J.-P. Wintemberger, *Serre's modularity conjecture (I)*, preprint.

[12] R. Livné, *The average distribution of cubic exponential sums*, J. Reine Angew. Math. **375/376** (1987), 362–379.

[13] R. Livné, *Cubic exponential sums and Galois representations*, Contemp. Math. **67** (1987), 247–261.

[14] R. Murty, *Congruences between modular forms* in Analytic Number Theory, London Math. Soc. Lecture Notes **247** (1997), 313–320.

[15] C. Schoen, *Algebraic cycles on certain desingularized nodal hypersurfaces*, Math. Ann. **270** (1985), no. 1, 17–27.

[16] J.-P. Serre, *Résumé des cours de 1984 – 1985*, Annuaire du Collège de France (1985), 85–90.

[17] J.-P. Serre, *Sur les représentations modulaires de degré 2 de* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, Duke Math. J. **54** (1987) 179–230.

[18] J. Socrates, D. Whitehouse, *Unramified Hilbert modular forms, with examples relating to elliptic curves*, Pacific J. Math. **219** (2005), no. 2, 333–364.

[19] A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. Math. 2 **141** (1995), no. 3, 443–551.