Isomorphisms of modular Galois representations and graphs

Samuele Anni

Seminair Lithe and Fast Algorithmic Number Theory

3 November 2020 - Bordeaux

Université d'Aix-Marseille, Institut de Mathématiques

Congruence graphs

joint with Vandita Patel (Manchester University)

Modular forms

Let n be a positive integer, the congruence subgroup $\Gamma_0(n)$ is a subgroup of $\mathrm{SL}_2(\mathbb{Z})$ given by

$$\Gamma_0(n) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : n \mid c \right\}.$$

Given a pair of positive integers n (level) and k (weight), a **modular form** f for $\Gamma_0(n)$ is an holomorphic function on the complex upper half-plane $\mathbb{H}$ satisfying

$$f(\gamma z) = f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z) \quad \forall \gamma \in \Gamma_0(n), z \in \mathbb{H}$$

and a growth condition for the coefficients of its power series expansion

$$f(z) = \sum_0^\infty a_m q^m, \qquad \text{where} \qquad q = e^{2\pi i z}.$$

Newforms

There are families of operators acting on the space of modular forms. In particular, the **Hecke operators** T_p for every prime p. These operators describe the interplay between different group actions on the complex upper half-plane.

We will consider only cuspidal **newforms**: cuspidal modular forms ($a_0 = 0$), normalized ($a_1 = 1$), which are eigenforms for the Hecke operators and arise from level n.

We will denote by $S_k(n)_{\mathbb{C}}$ the space of cuspforms and by $S_k(n)_{\mathbb{C}}^{new}$ the subspace of newforms.

Congruence between newforms

Let f and g be two newforms.

$$f = \sum a_m q^m \qquad g = \sum b_m q^m.$$

Then $\mathbb{Q}_f = \mathbb{Q}(\{a_m\})$ is a number field, the **Hecke eigenvalue field** of f.

Definition

We say that f and g are **congruent** *mod p, if there exists an ideal $\mathfrak{p}$ dividing p in the compositum of the Hecke eigenvalue fields of f and g such that*

$$a_m \equiv b_m \bmod \mathfrak{p} \quad \textit{for all } m.$$

Example: $S_2(77)^{new}_{\mathbb{C}}$

$$f_0(q) = q - 3q^3 - 2q^4 - q^5 - q^7 + 6q^9 - q^{11} + 6q^{12} - 4q^{13} + 3q^{15} + \dots$$
$$f_1(q) = q + q^3 - 2q^4 + 3q^5 + q^7 - 2q^9 - q^{11} - 2q^{12} - 4q^{13} + 3q^{15} + \dots$$
$$f_2(q) = q + q^2 + 2q^3 - q^4 - 2q^5 + 2q^6 - q^7 - 3q^8 + q^9 - 2q^{10} + q^{11} + \dots$$
$$f_{3,4}(q) = q + \alpha q^2 + (-\alpha + 1)\, q^3 + 3q^4 - 2q^5 + (\alpha - 5)\, q^6 + q^7 + \dots$$

where α satisfies $x^2 - 5 = 0$.

The Hecke eigenvalue fields are $\mathbb{Q}$ for f_0, f_1, f_2 and $\mathbb{Q}(\sqrt{5})$ for $f_{3,4}$. The following congruences hold:

$f_0 \equiv f_1 \bmod 2$, $\quad f_1 \equiv f_{3,4} \bmod \mathfrak{p}_5$, $\quad f_2 \equiv f_{3,4} \bmod \mathfrak{p}_2$,

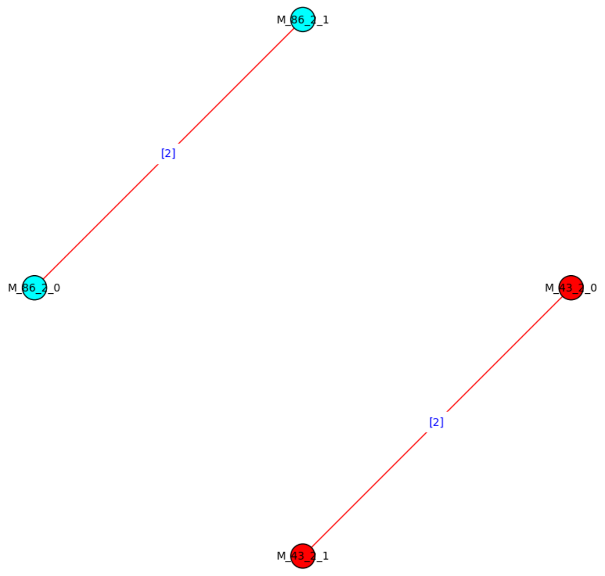
where $\mathfrak{p}_2 = (2)$, $\mathfrak{p}_5 \mid 5$ are primes in $\mathbb{Q}(\sqrt{5})$. This is the **complete** list of possible congruences!

Congruence Graphs

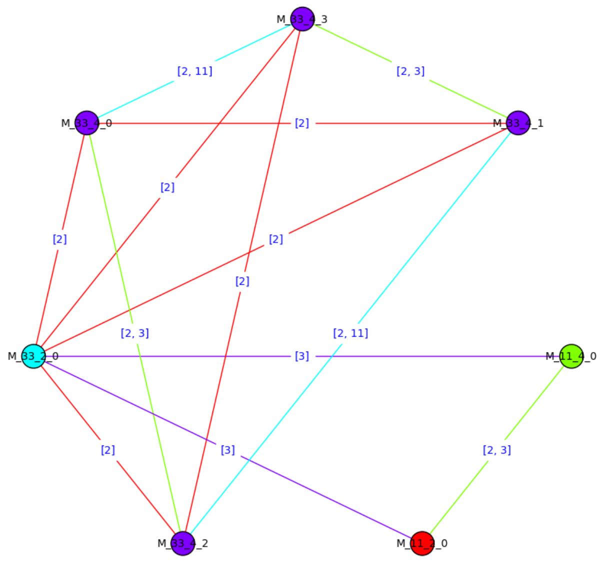
- $\boxed{\textbf{Nodes}}$ correspond to Hecke orbits of newforms of level and weight in a given set (for $f \in S_k(n)^{\mathrm{new}}$ a Hecke orbit is the set of forms $\tau(f)$ for $\tau : \mathbb{Q}_f \to \overline{\mathbb{Q}}$).
- We draw an $\boxed{\textbf{edge}}$ between two nodes whenever there is a prime ℓ for which there is a congruence mod ℓ between forms in the orbits.

Let S be the set of **divisors of a positive integer** and let W be a **finite set of weights**, $\boxed{\mathcal{G}_{S,W}}$ denotes the associated graph.

$\mathcal{G}_{[1,2,43,86],[2]}$



$\mathcal{G}_{[1,3,11,33],[2,4]}$



Checking congruences

How do we check congruence?

Sturm Theorem

Let $n \geq 1$ be an integer. Let $f(q) = \sum a_m q^m$ be a modular form of level n and weight k, with coefficients in the ring of integers of a number field, and let λ be a maximal ideal herein.

Suppose that the reduction of the q-expansion of f modulo λ satisfies

$$a_m \equiv 0 \mod \lambda \quad \text{for all } m \leq \frac{k}{12}[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(n)].$$

Then $a_m \equiv 0 \mod \lambda$ for all m.

Hecke algebras and congruence graphs

Hecke algebra: connectedness

Definition

The **Hecke algebra** $\mathbb{T}(n,k)$ *is the* $\mathbb{Z}$*-subalgebra of* $\mathrm{End}_{\mathbb{C}}(S(n,k)_{\mathbb{C}})$ *generated by Hecke operators* T_p *for every prime* p.

Question (Ash, Mazur)

Is $\operatorname{Spec} \mathbb{T}(n,k)$ connected?

The congruence graphs are related to the dual graphs of the spectrum of the Hecke algebra.

Theorem

$\operatorname{Spec}\mathbb{T}(p,k)$ *is connected for*

- p *prime* ≤ 997 *with* $k=4$,
- p *prime* ≤ 293 *with* $k=6,8$,
- p *prime* ≤ 97 *with* $k=10,12$.

This follows from $\mathcal{G}_{[p],[k]}$ being a connected graphs for p and k as above.

Theorem

$\mathcal{G}_{[p],[4]}$ *is a complete graph for* p *prime* ≤ 997.

Residual modular Galois representations & Isomorphism graphs

Theorem (Deligne, Serre, Shimura)

Let n and k be positive integers. Let $\mathbb{F}$ be a finite field of characteristic ℓ, with $\ell \nmid n$, and $f : \mathbb{T}(n,k) \twoheadrightarrow \mathbb{F}$ a surjective ring homomorphism. Then there is a (unique) continuous semi-simple representation:

$$\rho_f : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}),$$

unramified outside $n\ell$, such that for all p not dividing $n\ell$ we have:

$$\mathrm{Tr}(\rho_f(\mathrm{Frob}_p)) = f(T_p) \text{ and } \det(\rho_f(\mathrm{Frob}_p)) = f(\langle p \rangle)p^{k-1} \text{ in } \mathbb{F}.$$

Remark

If f and g are congruent modulo ℓ then there exists primes $\lambda, \lambda' \mid \ell$ in $\mathbb{Q}_f$ and $\mathbb{Q}_g$, such that $\overline{\rho}_{f,\lambda} \cong \overline{\rho}_{g,\lambda'}$.

Example: $n_f = 38$ and $n_g = 58$

$\ell = 5$

$k_f = k_g = 2$

$n_f = 38 = 2 \cdot 19 \qquad n_g = 58 = 2 \cdot 29$

$\epsilon_f = \epsilon_g = \mathrm{Ind}(\mathbf{1})$

p	2	3	5	7	11	13	17	19	23	29	31	37	41	43
$f(T_p)$	1	4	1	3	2	4	3	4	4	0	2	3	2	4
$g(T_p)$	1	4	1	3	2	4	3	0	4	4	2	3	2	4

Example: $n_f = 38$ and $n_g = 58$

$\ell = 5$

$n_f = 38 = 2 \cdot 19 \qquad n_g = 58 = 2 \cdot 29$

$\epsilon_f = \epsilon_g = \mathrm{Ind}(\mathbf{1})$

p	2	3	5	7	11	13	17	19	23	29	31	37	41	43
$f(T_p)$	1	4	1	3	2	4	3	4	4	0	2	3	2	4
$g(T_p)$	1	4	1	3	2	4	3	0	4	4	2	3	2	4

It seems that $\rho_f \cong \rho_g$ since for lots of primes p we have $\mathrm{Tr}(\rho_f(\mathrm{Frob}_p)) = f(T_p) = Tr(\rho_g(\mathrm{Frob}_p)) = g(T_p)$ and $\det(\rho_f(\mathrm{Frob}_p)) = \epsilon_f(p) = \det(\rho_g(\mathrm{Frob}_p)) = \epsilon_g(p)$.

How can we prove this?

Computing ρ_f is "difficult", but theoretically it **can be done in polynomial time** in $n, k, \#\mathbb{F}$:

Edixhoven, Couveignes, de Jong, Merkl, Bruin, Bosman ($\#\mathbb{F} \leq 32$):

Example: for $n = 1$, $k = 22$ and $\ell = 23$, the number field corresponding to $\mathbb{P}\rho_f$ (Galois group isomorphic to $\mathrm{PGL}_2(\mathbb{F}_{23})$) is given by:

$$
\begin{aligned}
x^{24} &- 2x^{23} + 115x^{22} + 23x^{21} + 1909x^{20} + 22218x^{19} + 9223x^{18} + 121141x^{17} \\
&+ 1837654x^{16} - 800032x^{15} + 9856374x^{14} + 52362168x^{13} - 32040725x^{12} \\
&+ 279370098x^{11} + 1464085056x^{10} + 1129229689x^{9} + 3299556862x^{8} \\
&+ 14586202192x^{7} + 29414918270x^{6} + 45332850431x^{5} - 6437110763x^{4} \\
&- 111429920358x^{3} - 12449542097x^{2} + 93960798341x - 31890957224
\end{aligned}
$$

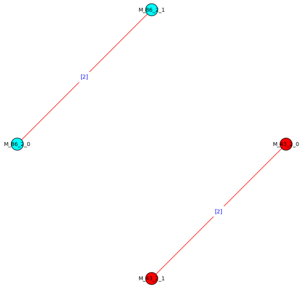
Mascot, Zeng, Tian ($\#\mathbb{F} \leq 53$).

Isomorphism Graphs

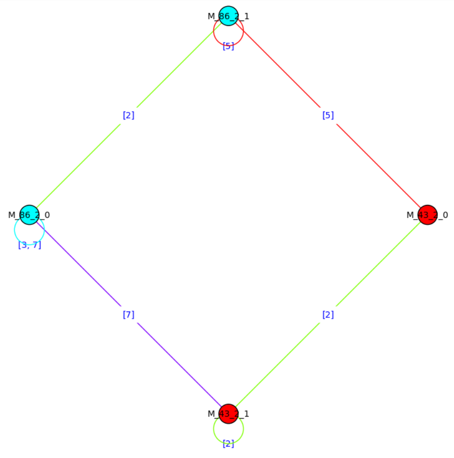
- $\boxed{\textbf{Nodes}}$ correspond to Hecke orbits of newforms of level and weight in a given set (for $f \in S_k(n)^{\mathrm{new}}$ a Hecke orbit is the set of forms $\tau(f)$ for $\tau : \mathbb{Q}_f \to \overline{\mathbb{Q}}$).
- We draw an $\boxed{\textbf{edge}}$ between two nodes if for two forms f and g in the respective orbits there is a prime ℓ, and there exist primes $\lambda, \lambda' \mid \ell$ such that

$$\overline{\rho}_{f,\lambda} \cong \overline{\rho}_{g,\lambda'}$$

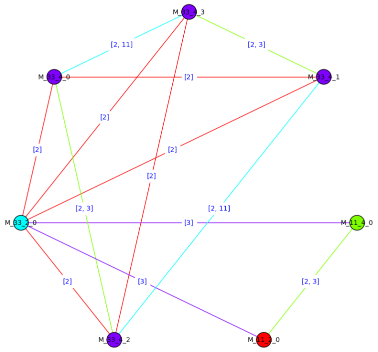
Let S be the set of **divisors of a positive integer** and let W be a **finite set of weights**, $\boxed{\mathcal{G}^{\rho}_{S,W}}$ denotes the associated graph.



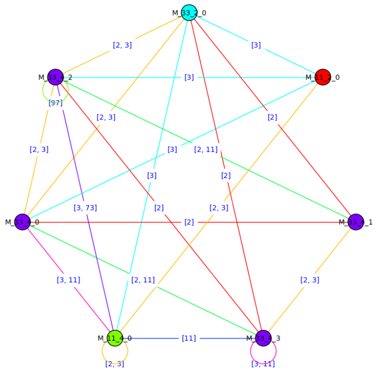
$\mathcal{G}_{[1,2,43,86],[2]}$



$\mathcal{G}^{\rho}_{[1,2,43,86],[2]}$



$\mathcal{G}_{[1,3,11,33],[2,4]}$



$\mathcal{G}^{\rho}_{[1,3,11,33],[2,4]}$

Checking isomorphisms

joint with Peter Bruin (Leiden University)

Degeneracy maps

Degeneracy maps

Let ℓ be a prime and let $n, k \in \mathbb{Z}_{\geq 1}$ be such that $\ell \nmid n$.
Suppose $n = mp^r$ with $r \geq 1$ and where p is a prime not dividing m.
We have two degeneracy maps B_p and B_1 on $X_1(n)_{\overline{\mathbb{F}}_\ell}$:

$$\begin{tikzcd}
& X_1(m, p^r)_{\overline{\mathbb{F}}_\ell} \arrow[dl, "B_1"'] \arrow[dr, "B_p"] & \\
X_1(m, p^{r-1})_{\overline{\mathbb{F}}_\ell} & & X_1(m, p^{r-1})_{\overline{\mathbb{F}}_\ell}
\end{tikzcd}$$

Degeneracy maps : B_1

Let ℓ be a prime and let $n, k \in \mathbb{Z}_{\geq 1}$ be such that $\ell \nmid n$.
Suppose $n = mp^r$ with $r \geq 1$ and where p is a prime not dividing m.
We have two degeneracy maps $\boxed{B_1}$ and B_p on $X_1(n)_{\overline{\mathbb{F}}_\ell}$:

$$\begin{tikzcd} X_1(m, p^r)_{\overline{\mathbb{F}}_\ell} \arrow[d, "B_1"] \\ X_1(m, p^{r-1})_{\overline{\mathbb{F}}_\ell} \end{tikzcd} \qquad \begin{tikzcd} (E, P, Q) \arrow[d, "B_1"] \\ (E, P, pQ) \end{tikzcd}$$

Moduli interpretation for $X_1(n)_{\overline{\mathbb{F}}_\ell}$: E/S elliptic curve over an $\overline{\mathbb{F}}_\ell$-scheme S, with P and Q points of order m and p^r.

Degeneracy maps: B_p

Let ℓ be a prime and let $n, k \in \mathbb{Z}_{\geq 1}$ be such that $\ell \nmid n$.
Suppose $n = mp^r$ with $r \geq 1$ and where p is a prime not dividing m.
We have two degeneracy maps B_1 and $\boxed{B_p}$ on $X_1(n)_{\overline{\mathbb{F}}_\ell}$:

$$\begin{array}{ccc} X_1(m, p^r)_{\overline{\mathbb{F}}_\ell} & & (E, P, Q) \\ \Big\downarrow{\scriptstyle B_p} & & \Big\downarrow{\scriptstyle B_p} \\ X_1(m, p^{r-1})_{\overline{\mathbb{F}}_\ell} & & (E/\langle p^{r-1}Q\rangle, \beta(P), \beta(Q)) \end{array}$$

Moduli interpretation for $X_1(n)_{\overline{\mathbb{F}}_\ell}$: E/S elliptic curve over an $\overline{\mathbb{F}}_\ell$-scheme S, with P and Q points of order m and p^r, where β is an isogeny such that

$$\langle p^{r-1}Q\rangle \rightarrowtail E \xrightarrow{\beta} E/\langle p^{r-1}Q\rangle.$$

Degeneracy maps

Let $m, n, d, k \in \mathbb{Z}_{\geq 1}$ with $m \mid n$ and $d \mid \frac{n}{m}$ the degeneracy map

$$B^*_{d,m,n} \colon M(\Gamma_1(m), k)_{\overline{\mathbb{F}}_\ell} \to M(\Gamma_1(n), k)_{\overline{\mathbb{F}}_\ell}$$

is the map induced in cohomology by the map B_d.
In terms of the q-expansion this map is the substitution $q \mapsto q^d$:

$$f = \sum_{n \geq 0} a_n(f) q^n \longmapsto B^*_d(f) = \sum_{n \geq 0} a_n(f) q^{dn}$$

For every prime number p, using the degeneracy maps, we define the following $\overline{\mathbb{F}}_\ell$-linear map:

$$\eta_p \colon M(\Gamma_1(n), k)_{\overline{\mathbb{F}}_\ell} \to \begin{cases} M(\Gamma_1(np), k)_{\overline{\mathbb{F}}_\ell} & \text{if } p \mid n \\ M(\Gamma_1(np^2), k)_{\overline{\mathbb{F}}_\ell} & \text{if } p \nmid n \end{cases}$$

by

$$\eta_p = \begin{cases} B^*_{1,n,np} - B^*_{p,n,np} T_p & \text{if } p \mid n; \\ B^*_{1,n,np^2} - B^*_{p,n,np^2} T_p + p^{k-1} B^*_{p^2,n,np^2} \langle p \rangle & \text{if } p \nmid n. \end{cases}$$

Compatibility Hecke operators and degeneracy maps: $\eta_p(T_p) = 0$.

How do we check isomorphisms of Galois representations?

Let $n_f, n_g, k \in \mathbb{Z}_{\geq 1}$ and let ℓ be a prime number $\ell \nmid n_f n_g$, denote:

$$\begin{aligned} N &:= \operatorname{lcm}(n_f, n_g) \prod_{p \mid n_f n_g \text{ prime}} p, \\ B_{\text{naive}}(n_f, n_g, k, \ell) &:= \frac{k+\ell+1}{12}[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(N)]. \end{aligned}$$

Lemma

Let $f : \mathbb{T}(n_f, k) \to \overline{\mathbb{F}}_\ell$ and $g : \mathbb{T}(n_g, k) \to \overline{\mathbb{F}}_\ell$ be ring homomorphisms. If $\epsilon_f = \epsilon_g$ and $f(T_p) = g(T_p)$ **for all primes** *$p \nmid N$* **and** *$p \leq B_{\textbf{naive}}(n_f, n_g, k, \ell)$, then $\rho_f \cong \rho_g$.*

The previous lemma is not “efficient”: using degeneracy maps, we move the problem of comparing forms of different level and weight to the problem of comparing forms of the same level, but this level is very BIG. It is an improvement on the results of Takai of 2011.

This approach avoids the study of the primes dividing the level, that are the primes where the associated representation can ramify.

Example: $n_f = 38$ and $n_g = 58$

$\ell = 5$
$n_f = 38 = 2 \cdot 19$ $n_g = 58 = 2 \cdot 29$
$\epsilon_f = \epsilon_g = \mathrm{Ind}(\mathbf{1})$

$$B_{\text{naive}}(n_f, n_g, k, \ell) = 1322400$$

To prove that $\rho_f \cong \rho_g$ we have to show

$$\mathrm{Tr}(\rho_f(\mathrm{Frob}_p)) = f(T_p) = Tr(\rho_g(\mathrm{Frob}_p)) = g(T_p)$$

for all prime $p \leq 1322400$.

Serre's Conjecture

Theorem (Khare, Wintenberger, Dieulefait, Kisin), Serre's Conjecture

Let ℓ be a prime number and let $\rho\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$ be an odd, absolutely irreducible, continuous representation. Then ρ is **modular** of level n_ρ, weight k_ρ and character $\epsilon(\rho)$.

- n_ρ (the level) is the Artin conductor away from ℓ.
- k_ρ (the weight) is given by a recipe in terms of $\rho|_{I_\ell}$.
- $\epsilon(\rho)\colon (\mathbb{Z}/n_\rho\mathbb{Z})^* \to \overline{\mathbb{F}}_\ell^*$ is given by:

$$\det \rho = \epsilon(\rho)\chi_\ell^{k_\rho - 1},$$

where χ_ℓ is the cyclotomic character mod ℓ.

Local representation at primes dividing the level and at ℓ

Theorem (Gross, Vignéras, Fontaine, Serre: Conjecture 3.2.6?)

Let $\rho : G_{\mathbb{Q}} \to \mathrm{GL}(V)$ be a continuous, odd, irreducible representation, with V a 2-dimensional $\overline{\mathbb{F}}_\ell$-vector space. Let $f : \mathbb{T}(n_\rho, k_\rho) \to \overline{\mathbb{F}}_\ell$ be a ring homomorphism such that $\rho_f \cong \rho$. Let p be a prime divisor of ℓn.

(1) *If $f(T_p) \neq 0$, then there exists a stable line $D \subset V$ for the action of G_p, such that I_p acts trivially on V/D. Moreover, the eigenvalue of Frob_p acting on V/D is equal to $f(T_p)$.*

(2) *If $f(T_p) = 0$, then there exists no stable line $D \subset V$ as in (1).*

(1) $\Rightarrow \rho_f|_{G_p}$ is reducible;

(2) $\Rightarrow \rho_f|_{G_p}$ is irreducible.

Descendant and ancestors

Let $n, k \in \mathbb{Z}_{\geq 1}$ such that $n \geq 1$, $\ell \nmid n$ and $2 \leq k \leq \max\{4, \ell+1\}$.

Let $f\colon \mathbb{T}(\Gamma_1(n), k) \to \overline{\mathbb{F}}_\ell$ and $p \neq \ell$ a prime. Let

$$R_p(f) = \begin{cases} \text{roots of } x^2 - f(T_p)x + f(\langle p \rangle)p^{k-1} & \text{if } p \nmid n, \\ \text{roots of } x^2 - f(T_p)x & \text{if } p \mid n. \end{cases}$$

Definition

*A p-**descendant** of (n, k, f) is a triple of the form (np, k, g), where $g\colon \mathbb{T}(\Gamma_1(np), k) \to \overline{\mathbb{F}}_\ell$ is a ring homomorphism satisfying*

- $g(T_q) = f(T_q)$ *for all primes* $q \neq p$,
- $g(T_p) \in R_p(n, k, f)$,
- $\epsilon_g(d) = g(\langle d \rangle) = f(\langle d \bmod n \rangle)$ *for all* $d \in (\mathbb{Z}/np\mathbb{Z})^\times$.

Lemma

Let $f\colon \mathbb{T}(\Gamma_1(n),k) \to \overline{\mathbb{F}}_\ell$ *be a ring homomorphism, and let* $p \neq \ell$ *be a prime number. Then*

$$\{g(T_p) \mid g \text{ is a } p\text{-descendant of } (n,k,f)\} = R_p(f).$$

Let $n \in \mathbb{Z}_{\geq 1}$ be such that $\ell \nmid n$.

Definition (companion)

Let $f\colon \mathbb{T}(\Gamma_1(n), \ell) \to \overline{\mathbb{F}}_\ell$ be a ring homomorphism. A **companion** *of f is a ring homomorphism $g\colon \mathbb{T}(\Gamma_1(n), \ell) \to \overline{\mathbb{F}}_\ell$ such that $\epsilon_f = \epsilon_g$, $f(T_p) = g(T_p)$ for all primes $p \neq \ell$, $f(T_\ell) \neq g(T_\ell)$ and $f(T_\ell)g(T_\ell) = f(\langle \ell \rangle)$.*

Let $n \in \mathbb{Z}_{\geq 1}$ be such that $\ell \nmid n$.

Definition (companion)

Let $f \colon \mathbb{T}(\Gamma_1(n), \ell) \to \overline{\mathbb{F}}_\ell$ be a ring homomorphism. A **companion** *of f is a ring homomorphism $g \colon \mathbb{T}(\Gamma_1(n), \ell) \to \overline{\mathbb{F}}_\ell$ such that:*

- $\epsilon_f = \epsilon_g$;
- $f(T_p) = g(T_p)$ *for all primes* $p \neq \ell$;
- $f(T_\ell) \neq g(T_\ell)$ *and* $f(T_\ell)g(T_\ell) = f(\langle \ell \rangle)$.

Remarque

This means that $f(T_\ell) \in \overline{\mathbb{F}_\ell}^\times$ and $g(T_\ell)$ is a root of the quadratic polynomial $x^2 - \left(f(T_\ell) + \frac{f(\langle \ell \rangle)}{f(T_\ell)}\right)x + f(\langle \ell \rangle)$, different from $f(T_\ell)$.

For all integers $n \geq 1$ and $k \geq 2$, **multiplication by the Hasse invariant** defines an injective $\overline{\mathbb{F}}_\ell$-linear map

$$\iota_{n,k,\ell} \colon M(\Gamma_1(n), k)_{\overline{\mathbb{F}}_\ell} \rightarrowtail M(\Gamma_1(n), k+\ell-1)_{\overline{\mathbb{F}}_\ell}.$$

This map is compatible with the Hecke and diamond operators so there is a canonical surjective ring homomorphism

$$\pi_{n,k,\ell} \colon \mathbb{T}(\Gamma_1(n), k+\ell-1)_{\overline{\mathbb{F}}_\ell} \twoheadrightarrow \mathbb{T}(\Gamma_1(n), k)_{\overline{\mathbb{F}}_\ell}$$

such that for each element $T \in \mathbb{T}(\Gamma_1(n), k+\ell-1)_{\overline{\mathbb{F}}_\ell}$, we have $\iota_{n,k,\ell} \circ (\pi_{n,k,\ell}(T)) = T \circ \iota_{n,k,\ell}$.

Let $n_h, k_h \in \mathbb{Z}_{\geq 1}$ be such that $\ell \nmid n_h$ and $2 \leq k_h \leq \max\{4, \ell+1\}$.
Let $h\colon \mathbb{T}(\Gamma_1(n_h), k_h) \to \overline{\mathbb{F}}_\ell$ be a ring homomorphism.

Definition (descendants, $\mathrm{Old}(h)$)

The set of **descendants** *of* (n_h, k_h, h)*, denoted by* $\mathrm{Old}(h)$*, is the minimal set of triples* (n, k, f) *consisting of positive integers* n*,* k *and a ring homomorphism* $f : \mathbb{T}(\Gamma_1(n), k) \to \overline{\mathbb{F}}_\ell$ *such that the following hold:*

- *the triple* (n_h, k_h, h) *is in* $\mathrm{Old}(h)$*;*
- *if* $(n, k, f) \in \mathrm{Old}(h)$ *then for every prime* $p \neq \ell$ *every* p*-descendant* g *of* (n, k, f) *satifies* $(np, k, g) \in \mathrm{Old}(h)$*;*

Definition (descendants, $\mathrm{Old}(h)$)

- *("multiplication by the Hasse invariant") if* $(n,k,f) \in \mathrm{Old}(h)$ *with* $k+\ell-1 \leq \max\{4, \ell{+}1\}$, *then* $(n, k+\ell-1, f \circ \pi_{n,k,\ell}) \in \mathrm{Old}(h)$;
- *("division by the Hasse invariant") if* $k+\ell-1 \leq \max\{4, \ell{+}1\}$ *and* $(n, k+\ell-1, f \circ \pi_{n,k,\ell}) \in \mathrm{Old}(h)$ *then triple* $(n,k,f) \in \mathrm{Old}(h)$;
- *if* $(n,\ell,f) \in \mathrm{Old}(h)$ *and* f *admits a companion* g *then* $(n,\ell,g) \in \mathrm{Old}(h)$.

Definition (ancestor)

Given positive integers n, k and a ring homomorphism $f : \mathbb{T}(\Gamma_1(n), k) \to \overline{\mathbb{F}}_\ell$, an **ancestor** *of f is any triple (n_h, k_h, h) as above such that (n, k, f) is a descendant of (n_h, k_h, h).*

$$\mathrm{Old}(h, n) = \{(k, f) : (n, k, f) \in \mathrm{Old}(h)\}$$

$$\mathrm{Old}(h, n, k) = \{f : (n, k, f) \in \mathrm{Old}(h)\}.$$

All triples $(n, k, f) \in \mathrm{Old}(h)$ satisfy the following properties:

- $\ell \nmid n$;
- $n_h \mid n$;
- $2 \leq k \leq \max\{4, \ell+1\}$;
- $k \equiv k_h \bmod \ell-1$;
- $f(T_p) = h(T_p)$ for all $p \nmid n\ell$;
- $f(\langle d \rangle) = h(\langle d \rangle)$ for all $d \in (\mathbb{Z}/n\mathbb{Z})^*$.

Goal

We would like to give computational criteria for deciding whether a given form is in $\mathrm{Old}(h)$.

We define a finite subset $C_\ell(h) \subset \overline{\mathbb{F}}_\ell$ by

$$C_\ell(h) = \begin{cases} \left\{ h(T_\ell), \dfrac{h(\langle \ell \rangle)}{h(T_\ell)} \right\} & \text{if } k_h \equiv \ell \bmod \ell{-}1 \text{ and } h(T_\ell) \neq 0; \\ \{h(T_\ell)\} & \text{if } k_h \not\equiv \ell \bmod \ell{-}1 \text{ or } h(T_\ell) = 0. \end{cases}$$

Let n be a multiple of n_h with $\ell \nmid n$, and let p be a prime divisor of n. We define a finite subset $C_p(h,n) \subset \overline{\mathbb{F}}_\ell$ by

$$C_p(h,n) = \begin{cases} \{h(T_p)\} & \text{if } p \nmid n/n_h; \\ R_p(h) & \text{if } p \parallel n/n_h; \\ \{0\} \cup R_p(h) & \text{if } p^2 \mid n/n_h. \end{cases}$$

Lemma

We have

$$\{f(T_\ell) : (n,k,f) \in \mathrm{Old}(h)\} \subseteq C_\ell(h).$$

Lemma

Let n be a multiple of n_h with $\ell \nmid n$, and let p be a prime number different from ℓ. Then we have

$$\{f(T_p) : (k,f) \in \mathrm{Old}(h,n)\} = C_p(h,n).$$

Proposition

Let (n_h, k_h, h) *be as above, and let* (n, k, f) *be a descendant of* (n_h, k_h, h)*. Then*

$$\rho_f \cong \rho_h.$$

Proposition

Let $\rho\colon G_{\mathbb{Q}} \to \mathrm{Aut}_{\overline{\mathbb{F}}_\ell} V$ *be a semi-simple modular two-dimensional representation. Then there exist an integer* k_h *with* $2 \leq k_h \leq \max\{4, \ell{+}1\}$ *and* $k_h \equiv k_\rho \bmod \ell{-}1$ *and a ring homomorphism*

$$h\colon \mathbb{T}(\Gamma_1(n_\rho), k_h) \to \overline{\mathbb{F}}_\ell$$

satisfying $\rho_h \cong \rho$ *(up twisting by the cyclotomic character) and such that every triple* (n_f, k_f, f) *satisfying* $\rho_f \cong \rho$ *lies in* $\mathrm{Old}(h)$*.*

Sketch of the proof.

First suppose that ρ is irreducible. By assumption, ρ is modular. By the Khare–Wintenberger theorem (Serre's conjecture), there exists a ring homomorphism $h\colon \mathbb{T}(\Gamma_1(n_\rho), k_\rho) \to \overline{\mathbb{F}}_\ell$ such that ρ and ρ_h are isomorphic.

Now let (n_f, k_f, f) be a triple satisfying $\rho_f \cong \rho$. Using the results of Gross, Vignéras and Fontaine for the restriction of the representation at primes dividing the level and ℓ, we can show that (n_f, k_f, f) is a descendant of (n_ρ, k_h, h).

Sketch continuation.

Next suppose that ρ is reducible. Then there are characters $\epsilon_1, \epsilon_2 \colon G_{\mathbb{Q}} \to \overline{\mathbb{F}}_\ell^*$ of conductors n_1, n_2, say, satisfying $n_1 n_2 \mid n_\rho$, such that ρ is of the form

$$\rho \cong \epsilon_1 \oplus \epsilon_2 \chi_\ell^{k_\rho - 1}.$$

To ρ we associate an appropriate Eisenstein series E of level n_ρ and weight $k_h \equiv k_\rho \bmod \ell - 1$. Let $h \colon \mathbb{T}(\Gamma_1(n_\rho), k_h) \to \overline{\mathbb{F}}_\ell$ be a ring homomorphism obtained by composing $E \colon \mathbb{T}(\Gamma_1(n_\rho), k_h) \to \overline{\mathbb{Z}}$ with the reduction map. We can show that (n_f, k_f, f) is a descendant of (n_ρ, k_h, h). $\square$

S-linked

Definition (S-linked)

*Let $f\colon \mathbb{T}(\Gamma_1(n_f), k_f) \to \overline{\mathbb{F}}_\ell$ and $g\colon \mathbb{T}(\Gamma_1(n_g), k_g) \to \overline{\mathbb{F}}_\ell$ be ring homomorphisms. Let S be any set of primes not dividing $n_f n_g \ell$. We say that f and g are S-**linked** if the following conditions hold:*

- $k_f \equiv k_g \bmod \ell{-}1$;
- *for all primes $p \in S$ we have $f(T_p) = g(T_p) = a_p$;*
- *there exist $n_h, k_h \in \mathbb{Z}_{\geq 1}$ and a ring homomorphism $h\colon \mathbb{T}(\Gamma_1(n_h), k_h) \to \overline{\mathbb{F}}_\ell$ such that*
    - $n_h \mid \gcd(n_f, n_g)$;
    - $2 \leq k_h \leq \max\{4, \ell{+}1\}$ *and* $k_h \equiv k_f \equiv k_g \bmod \ell{-}1$;
    - $\epsilon_f = \mathrm{Ind}(\epsilon_h)$ *and* $\epsilon_g = \mathrm{Ind}(\epsilon_h)$;
    - *for all $p \in S$ we have $h(T_p) = a_p$;*
    - $f(T_\ell) \in C_\ell(h)$, $\forall p \mid n_f n_g$ *we have* $f(T_p) \in C_p(h, n_f)$.
    - $g(T_\ell) \in C_\ell(h)$, $\forall p \mid n_f n_g$ *we have* $g(T_p) \in C_p(h, n_g)$.

For any choice of (n_h, k_h, h) as above, we also say that f and g are *S-linked by* (n_h, k_h, h).

Lemma

Let (n_h, k_h, h) be as above, and let (n_f, k_f, f) and (n_g, k_g, g) be descendants . Then for every set S of primes not dividing $n_f n_g \ell$, the forms f and g are S-linked by (n_h, k_h, h).

Let n_f, n_g, k_f and k_g be positive integers satisfying $\ell \nmid n_f n_g$ and $2 \leq k_f, k_g \leq \max\{4, \ell{+}1\}$. We define

$$\tilde{k} = \begin{cases} 6 & \text{if } \ell = 2, \\ \ell + 2 & \text{if } \ell > 2 \text{ and } k_f = k_g = \ell, \\ \ell + 1 & \text{if } \ell > 2 \text{ and } k_f \equiv k_g \equiv 2 \bmod \ell{-}1, \\ k_f \ (= k_g) & \text{otherwise.} \end{cases}$$

Definition (distinguishing set)

A **distinguishing set** *for* $(n_f, n_g, \tilde{k})$ *is a set* S *of primes such that each of the anaemic Hecke algebras* $\mathbb{T}'(\Gamma_0(n_f), \tilde{k})$ *and* $\mathbb{T}'(\Gamma_0(n_g), \tilde{k})$ *is generated as a* $\mathbb{Z}$*-algebra by the subset* $\{T_p \mid p \in S\}$ *of the respective algebra.*

Lemma

Let $f\colon \mathbb{T}(\Gamma_1(n_f), k_f) \to \overline{\mathbb{F}}_\ell$ *and* $g\colon \mathbb{T}(\Gamma_1(n_g), k_g) \to \overline{\mathbb{F}}_\ell$ *be ring homomorphisms, and let* S *be a distinguishing set. If the triples* (n_f, k_f, f) *and* (n_g, k_g, g) *are* S*-linked, then they have a common ancestor.*

Let us define

$$B(n, \tilde{k}) = \frac{\tilde{k}}{12}[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(n)]$$

and

$$B(n_f, n_g, \tilde{k}) = \max\{B(n_f, \tilde{k}), B(n_g, \tilde{k})\}.$$

Furthermore, we define

Definition (S_B)

$$S_B = \{p \text{ prime} \mid p \nmid n_f n_g \ell \text{ and } p \leq B(n_f, n_g, \tilde{k})\}.$$

Lemma

Let $f\colon \mathbb{T}(\Gamma_1(n_f), k_f) \to \overline{\mathbb{F}}_\ell$ *and* $g\colon \mathbb{T}(\Gamma_1(n_g), k_g) \to \overline{\mathbb{F}}_\ell$ *be ring homomorphisms. If* f *and* g *are* S_B*-linked, then* (n_f, k_f, f) *and* (n_g, k_g, g) *have a common ancestor.*

Theorem

Let $f\colon \mathbb{T}(\Gamma_1(n_f), k_f) \to \overline{\mathbb{F}}_\ell$ *and* $g\colon \mathbb{T}(\Gamma_1(n_g), k_g) \to \overline{\mathbb{F}}_\ell$ *be ring homomorphisms. Then for any distinguishing set of primes* S*, the following are equivalent:*

1. f *and* g *are* S*-linked;*
2. f *and* g *are* S_B*-linked;*
3. f *and* g *have a common ancestor;*
4. ρ_f *and* ρ_g *are isomorphic.*

Examples

Example 1: $n_f = 38$ and $n_g = 58$

$\ell = 5$

$k_f = k_g = 2,\ \tilde{k} = 6$

$n_f = 38 = 2 \cdot 19 \qquad n_g = 58 = 2 \cdot 29$

$B(n_f, n_g, \tilde{k}) = 45 < B_{\mathrm{naive}}(n_f, n_g, k, \ell) = 1322400.$

p	2	3	5	7	11	13	17	19	23	29	31	37	41	43
$f(T_p)$	1	4	1	3	2	4	3	4	4	0	2	3	2	4
$g(T_p)$	1	4	1	3	2	4	3	0	4	4	2	3	2	4

p	2	3	5	7	11	13	17	19	23	29	31	37	41	43
$f(T_p)$	1	4	1	3	2	4	3	4	4	0	2	3	2	4
$g(T_p)$	1	4	1	3	2	4	3	0	4	4	2	3	2	4

Let us consider all mod 5 eigenforms of level $d \in \{1, 2\}$ and weight $k \in \{2, 6\}$: we have

(d, k)	(1,6)	(2,2)	(2,6)	(2,6)
	E_6	$E_2^{(2)}$	$E_6^{(1)}$	$E_6^{(2)}$

p	2	3	5	7	11	13	17	19	23	29	31	37	41	43
$f(T_p)$	1	4	1	3	2	4	3	4	4	0	2	3	2	4
$g(T_p)$	1	4	1	3	2	4	3	0	4	4	2	3	2	4
$E_6(T_p)$	3	4	1	3	2	4	3	0	4	0	2	3	2	4
$E_2^{(2)}(T_p)$	1	4	1	3	2	4	3	0	4	0	2	3	2	4
$E_6^{(1)}(T_p)$	2	4	1	3	2	4	3	0	4	0	2	3	2	4
$E_6^{(2)}(T_p)$	1	4	1	3	2	4	3	0	4	0	2	3	2	4

$$n_f = 38 = 2 \cdot 19$$

p	$C_p(E_6, 38)$	$C_p(E_2^{(2)}, 38)$	$C_p(E_6^{(1)}, 38)$	$C_p(E_6^{(2)}, 38)$
2	$\{1,2\}$	$\{1\}$	$\{2\}$	$\{1\}$
19	$\{1,4\}$	$\{1,4\}$	$\{1,4\}$	$\{1,4\}$

p	2	3	5	7	11	13	17	19	23	29	31	37	41	43
$f(T_p)$	1	4	1	3	2	4	3	4	4	0	2	3	2	4
$g(T_p)$	1	4	1	3	2	4	3	0	4	4	2	3	2	4
$E_6(T_p)$	3	4	1	3	2	4	3	0	4	0	2	3	2	4
$E_2^{(2)}(T_p)$	1	4	1	3	2	4	3	0	4	0	2	3	2	4
$E_6^{(1)}(T_p)$	2	4	1	3	2	4	3	0	4	0	2	3	2	4
$E_6^{(2)}(T_p)$	1	4	1	3	2	4	3	0	4	0	2	3	2	4

$$n_f = 38 = 2 \cdot 19$$

p	$C_p(E_6, 38)$	$C_p(E_2^{(2)}, 38)$	$C_p(E_6^{(1)}, 38)$	$C_p(E_6^{(2)}, 38)$
2	$\{1,2\}$	$\{1\}$	$\{2\}$	$\{1\}$
19	$\{1,4\}$	$\{1,4\}$	$\{1,4\}$	$\{1,4\}$

So E_6 and $E_2^{(2)}$ are both ancestors of f.

p	2	3	5	7	11	13	17	19	23	29	31	37	41	43
$f(T_p)$	1	4	1	3	2	4	3	4	4	0	2	3	2	4
$g(T_p)$	1	4	1	3	2	4	3	0	4	4	2	3	2	4
$E_6(T_p)$	3	4	1	3	2	4	3	0	4	0	2	3	2	4
$E_2^{(2)}(T_p)$	1	4	1	3	2	4	3	0	4	0	2	3	2	4
$E_6^{(1)}(T_p)$	2	4	1	3	2	4	3	0	4	0	2	3	2	4
$E_6^{(2)}(T_p)$	1	4	1	3	2	4	3	0	4	0	2	3	2	4

$$n_g = 58 = 2 \cdot 29$$

p	$C_p(E_6, 58)$	$C_p(E_2^{(2)}, 58)$	$C_p(E_6^{(1)}, 58)$	$C_p(E_6^{(2)}, 58)$
2	$\{1, 2\}$	$\{1\}$	$\{2\}$	$\{1\}$
29	$\{1, 4\}$	$\{1, 4\}$	$\{1, 4\}$	$\{1, 4\}$

So E_6 and $E_2^{(2)}$ are both ancestors of g. Therefore:

$$\rho_f \cong \rho_g \cong \rho_{E_6} \cong 1 \oplus \chi_5,$$

where χ_5 is the mod5 cyclotomic character.

Example 2: $n_h = 57$ and $n_g = 58$

$\ell = 5$

$k_h = k_g = 2$, $\tilde{k} = 6$

$n_h = 57 = 3 \cdot 19 \qquad n_g = 58 = 2 \cdot 29$

$B(n_h, n_g, \tilde{k}) = 45 < B_{\text{naive}}(n_f, n_g, \tilde{k}, \ell) = 15868800.$

p	2	3	5	7	11	13	17	19	23	29	31	37	41	43
$h(T_p)$	3	1	1	3	2	4	3	4	4	0	2	3	2	4
$g(T_p)$	1	4	1	3	2	4	3	0	4	4	2	3	2	4

p	2	3	5	7	11	13	17	19	23	29	31	37	41	43
$h(T_p)$	3	1	1	3	2	4	3	4	4	0	2	3	2	4
$g(T_p)$	1	4	1	3	2	4	3	0	4	4	2	3	2	4

Let us consider all mod 5 eigenforms of level 1 and weight $k \in \{2, 6\}$: so we have only E_6.

p	2	3	5	7	11	13	17	19	23	29	31	37	41	43
$h(T_p)$	3	1	1	3	2	4	3	4	4	0	2	3	2	4
$g(T_p)$	1	4	1	3	2	4	3	0	4	4	2	3	2	4
$E_6(T_p)$	3	4	1	3	2	4	3	0	4	0	2	3	2	4

E_6 is a common ancestors of h and g. We have that $\tilde{h}$ satisfies:

$$\tilde{h}(q) = E_6(q) - E_6(q^3) - E_6(q^{19}) + 3E_6(q^{57}).$$

Therefore:

$$\rho_h \cong \rho_g \cong \rho_{E_6} \cong 1 \oplus \chi_5.$$

Database

joint with Bruin, Cremona, Roberts, Sutherland

Database

Certified **complete database** of 2-dimensional mod ℓ representations of $G_{\mathbb{Q}}$ which are odd, irreducible, of conductor at most 100, weight at most $\max\{4, \ell+1\}$, for $\ell = 2, 3$ and 5. Moreover, we required the representation to be defined over $\mathbb{F}_\ell$.

This database will be included in the LMFDB.

Isomorphisms of modular Galois representations and graphs

Samuele Anni

Seminair Lithe and Fast Algorithmic Number Theory

3 November 2020 - Bordeaux

Thanks!