Bethe Forum "Constructive methods in number theory", Bonn

"Galois representations attached to modular forms and Belyi maps"

2015/03/05, Bonn. Bas Edixhoven. 45 minutes.

Thm (Couveignes, E., R. de Jong, Merkl, Bruin, Javan Peykar)
There is an algorithm that on input an eigenform f of level n and weight $k \geq 2$ with coefficients in a finite field $\mathbb{F}$, computes the Galois representation $\rho_f : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F})$ in time polynomial in n, k and $\#\mathbb{F}$. Once ρ_f has been computed, for $p \nmid n \cdot \mathrm{char}(\mathbb{F})$ one can compute $\mathrm{tr}(\rho_f(\mathrm{Frob}_p)) = a_p(f)$ in time polynomial in k, n, ~~log p~~. $\#\mathbb{F}$ and $\log p$.

There is an algorithm that on input a modular form f of level n, weight k and coeff. in a number field K, and m in factored form, computes $a_m(f)$ in time polynomial in n, k and $\log m$, under GRH.

The idea is very simple: $\rho_f^{\otimes \chi_\ell}$ is realised by $V \subset J_1(n')(\overline{\mathbb{Q}})[\ell]$, with V 2-dim. over $\mathbb{F}' = \mathbb{T}(n',2)/m$.

Take $\alpha : J_1(n') \dashrightarrow \mathbb{A}^1_{\mathbb{Q}}$ a suitable rational function, $F := \prod_{x \in V - \{0\}} (X - \alpha(x)) \in \mathbb{Q}[X]$.

1. Bound $h(F)$ polyn. in $n, k, \#\mathbb{F}$ (E + de Jong + Merkl) (Bruin)
2. Approximate F numerically with required precision in time pol. in $n, k, \#\mathbb{F}$. (Couveignes) (Bruin)

Nice from theoretical perspective: we have a theorem.
But: it is not at all practical.

Before going on: $V \subset J_1(n')(\overline{\mathbb{Q}})[\ell] = H^1(X_1(n')_{\overline{\mathbb{Q}},et}, \mu_\ell) = \{$ isom. classes of unr. $\mu_\ell(\overline{\mathbb{Q}})$-covers $C \to X_1(n')_{\overline{\mathbb{Q}}}$ $\}$.

$$\begin{tikzcd} C \arrow[r] \arrow[dr, "\text{Belyi map}"'] & X_1(n')_{\overline{\mathbb{Q}}} \arrow[d, "j"] \\ & \mathbb{P}^1_{\overline{\mathbb{Q}}} \end{tikzcd}$$

Practical computations

Bosman, 2004 – 2008, $\rho^{\mathrm{proj}}_{\Delta_k, \ell}$ for $k \in \{12, 16, 18, 20, 22\}$, $\ell \leq 23$

$\mathbb{Q}[x]/(f^{\mathrm{proj}}_{k,\ell})$, $\deg(f^{\mathrm{proj}}_{k,\ell}) = \ell + 1$, Gal. grp. of splitting field $\subset \mathrm{PGL}_2(\mathbb{F}_\ell)$.

For example: $f^{\mathrm{proj}}_{22,23} = x^{24} - 2x^{23} + 115x^{22} \cdots\cdots - 318909 57224$. (6 lines of text). (2k€/polynomial)

And: $\tau(10^{1000} + 1357) \equiv \pm 4 \ (19)$.

Method: Complex numerical computations, ~~power series around cusps of $X_1(\ell)$~~ homotopy method.

Correctness ~~Verified~~ proof of result, application of Khare-Wintenberger, Zeng alone

~~Zeng~~ Zeng Jinxiang + Derickx + van Hoeij, (2012 – 2013) (Lectures in Beijing by me and Couveignes).

$f^{\mathrm{proj}}_{12,31} = x^{32} - 4 \cdot x^{31} - 155x^{28} + \cdots - 1261963$ (6 lines text).

$f_{12,19} = x^{19^2-1} + \cdots$, $\tau(10^{1000} + 1357) \equiv -4 \ (19)$.

Zeng 2012

The three together: quite a few new $f^{\mathrm{proj}}_{k\ell}$, e.g. $f^{\mathrm{proj}}_{26,41}$ (15 lines...)

Method: $J_1(\ell)(\mathbb{F}_{p^r})$ p small auxiliary prime., algorithms by Hess (following Couveignes).

Innovation: work with a $\mathrm{jac}(X_1(\ell)/H)$ $H \subset \mathbb{F}_\ell^\times$, or smallest sub.ab. var. of $J_1(\ell)$ containing ~~the 2-dim rep~~ $\rho_{k,\ell}$, good plane models of $X_1(\ell)/H$. use Dokchitser resolvents for $\rho_f(\mathrm{Frob}_p)$.

Mascot (2013, 2014) $f_{k,\ell}$ for $k < \ell \leq 31$. (also f's with coeff. $\notin \mathbb{Q}$).

$\tau(10^{1000} + 453) \equiv 19 \ (31)$, $\equiv 21 \ (29)$. $\deg(f_{k,\ell}) = \ell^2 - 1$, does not list them.

Method: complex approximations, Khuri-Makdisi alg's for $J_1(\ell)(\mathbb{C})$ (idea of Couveignes)

(no homotopy method when convergence becomes ~~difficult~~ harder.

Innovations ① a much better rat'l function on $J_1(\ell)$. ~~(Eucl. divisors of degree g)~~.

$(x \mapsto [E_x - g \cdot 0]$, $H^0(X, \mathcal{O}(F - E_x)) = \mathbb{C} \cdot t_x$, $\mapsto t_x(a)/t_x(b)$.)

deg 29, fixed

② Use $(V_f - \{0\})/S$

where $S \subset \mathbb{F}_\ell^\times$ prime to 2 part. (Derickx)

Use ~~this~~ also to reduce the polynomial $\prod_{x \in (V_f - \{0\})/S} (X - \alpha(x))$ to $f^S_{k,\ell}$. subgrp. of $\mathbb{F}_\ell^\times$

Tian Peng ~~Peng Tian~~ (2014) $f^{\mathrm{proj}}_{k,\ell}$ $(k,\ell) \in \{(12,31), (16,27), (20,31), (22,31)\}$: $\mathrm{jac}(X_1(\ell)/H)$

Method: Johan Bosman's code, adapted.

Arakelov theory & Belyi maps.

Let $\pi : X \longrightarrow \mathbb{P}^1_{\overline{\mathbb{Q}}}$ be a Belyi map, $g := \text{genus}(X)$

$(10\cdot g + 12)\deg\pi$

<u>Thm</u> (Javanpeykar, 2013) $h_{Falt}(X) \leqslant 13\cdot 10^6 \cdot g \cdot (\deg \pi)^5$

(and similar bounds for discriminant of X, self int. dualising sheaf & δ-inv.).

<u>Thm</u> (Bilu-Strambi; 2008) bounds for $[K:\mathbb{Q}]$, $\text{discr}(K/\mathbb{Q})$, $h(f) \leqslant (2\cdot(g+1)(\deg\pi)^{2})$

What does this mean? Let $\mathbb{Q} \subseteq K \subset \overline{\mathbb{Q}}$ finite s.t. X_{O_K} stable model.

$$X_{O_K} \xrightarrow{p} \operatorname{Spec}(O_K)$$

Then $h_{Falt}(X) = \frac{1}{[K:\mathbb{Q}]} \cdot \widehat{\deg}_{O_K}\left(\Lambda^g p_* \omega\right)$

$$= \frac{1}{[K:\mathbb{Q}]} \cdot \widehat{\deg}_{O_K}\Big(\overbrace{\Lambda^g\, 0^* \Omega^1_{J/O_K}}^{\omega_{J/O_K}}\Big) \qquad J := \operatorname{Pic}^0_{X_{O_K}/O_K}.$$

To get degree of line bundle, need a rational section: a Siegel mod. form.

Let $f \in H^0(\mathcal{A}_{g,1}, \omega^{\otimes k})$ s.t. $f(J/O_K) \neq 0$.

Let $\underset{\neq 0}{\alpha} \in \omega_{J/O_K}$, then $f(J/O_K) = \beta \cdot \alpha^{\otimes k}$ for a unique $\beta \in K$.

Then: $$\log \#\left(\omega^{\otimes k}_{J/O_K} / O_K \cdot f(J/O_K)\right) - \sum_{\sigma : K \to \mathbb{C}} \tfrac{1}{2} \cdot \log\left(|\sigma(\beta)|^2 \cdot \left(\int_{(\sigma J)(\mathbb{C})} \left(\tfrac{i}{2}\right)^g \cdot (-1)^{\binom{g}{2}} \cdot \alpha\overline{\alpha}\right)^k\right)$$

$$\leqslant k \cdot [K:\mathbb{Q}] \cdot 13 \cdot 10^6 \cdot g \cdot (\deg\pi)^5.$$

For example, for $g=1$, and $f = \Delta$:

$$h_{Falt}(E) = \frac{1}{12\cdot[K:\mathbb{Q}]} \cdot \left(\log N_{K/\mathbb{Q}}(\text{discr}(E/O_K)) - \sum_{\sigma: K \to \mathbb{C}} \log\left(|\Delta(\tau_\sigma)| \cdot (\operatorname{Im}\tau_\sigma)^6\right)\right)$$

$$\left(\Delta(\tau) = \frac{1}{(2\pi)^{12}} \cdot q \prod_{n \geqslant 1}(1-q^n)^{24}, \quad q = e^{2\pi i \tau}.\right)$$

for $g=2$: ---