Polynomials for mod ℓ representations in MAGMA

Johan Bosman, Universiteit Leiden, The Netherlands

Mod ℓ representations associated to newforms

Theorem (Deligne). *For a newform $f = \sum a_n q^n \in S_k(\Gamma_1(N))$ with character ε, a prime number ℓ and a prime $\lambda \mid \ell$ of the coefficient ring of f, there exists a two-dimensional representation*

$$\overline{\rho}_{f,\lambda} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_\lambda)$$

that is unramified outside $N\ell$ and satisfies

$$\mathrm{charpol}(\overline{\rho}_{f,\lambda}(\mathrm{Frob}_p)) \equiv x^2 - a_p x + \varepsilon(p)p^{k-1}$$

for all primes $p \nmid N\ell$.

Assume $k \leq \ell+1$ and that $\overline{\rho}_{f,\lambda}$ is absolutely irreducible. Then one can find $\overline{\rho}_{f,\lambda}$ as the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on a subspace of $J_1(N')(\overline{\mathbb{Q}})[\ell]$ with $N' = N$ for $k=2$ and $N' = N\ell$ otherwise.

MAGMA computations

Open MAGMA and attach the source with intrinsics:

```
> Attach( "modrep.m" );
```

Choose your favourite cusp form, e.g.

$$\Delta = q\prod(1-q^n)^{24} = \sum \tau(n)q^n \in S_{12}(\mathrm{SL}_2(\mathbb{Z})).$$

```
> S12 := CuspForms( Gamma0(1), 12 );
> Delta := Newform( S12, 1 );
```

Choose a prime ℓ for the mod ℓ representation, and enter it as an ideal of the coefficient ring of Δ, e.g. $\ell = 13$.

```
> L := ideal< Integers() | 13 >;
```

Note that $\rho = \overline{\rho}_{\Delta,\ell} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_\ell)$ factors through the number field $K_\ell = \overline{\mathbb{Q}}^{\ker(\rho)}$:

$$\overline{\rho}_{\Delta,\ell} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \twoheadrightarrow \mathrm{Gal}(K_\ell/\mathbb{Q}) \hookrightarrow \mathrm{GL}_2(\mathbb{F}_\ell).$$

A polynomial with splitting field K_ℓ can be computed as follows:

```
> pol := ComputeBigGLPolynomial( Delta, L );
```

This polynomial has degree ℓ^2-1; the action of $\mathrm{Gal}(K_\ell/\mathbb{Q})$ on its roots is compatible with the action of $\mathrm{im}\,\rho \subset \mathrm{GL}_2(\mathbb{F}_\ell)$ on $\mathbb{F}_\ell^2 - \{0\}$. The computation makes use of numerical approximations of ℓ-torsion points in $J_1(\ell)$ over $\mathbb{C}$.

Smaller polynomials

Instead of ρ, we can consider the *projectivised* representation $\tilde{\rho}$ that is obtained by composing ρ with $\mathrm{GL}_2(\mathbb{F}_\ell) \twoheadrightarrow \mathrm{PGL}_2(\mathbb{F}_\ell)$. The representation $\tilde{\rho}$ factors through a number field K'_ℓ:

$$\tilde{\rho} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \twoheadrightarrow \mathrm{Gal}(K'_\ell/\mathbb{Q}) \hookrightarrow \mathrm{PGL}_2(\mathbb{F}_\ell).$$

We can compute a polynomial P with splitting field K'_ℓ:

```
> pol := ComputePGLPolynomial( Delta, L );
```

This polynomial has degree $\ell+1$; the action of $\mathrm{Gal}(K'_\ell/\mathbb{Q})$ on its roots is compatible with the action of $\mathrm{im}\,\tilde{\rho} \subset \mathrm{PGL}_2(\mathbb{F}_\ell)$ on $\mathbb{P}^1(\mathbb{F}_\ell)$. The intrinsic `ComputePGLPolynomial` does a reduction of coefficients as its final step.

```
> pol;
X^14 + 7*X^13 + 26*X^12 + 78*X^11 + 169*X^10 +
    52*X^9 - 702*X^8 - 1248*X^7 + 494*X^6 +
    2561*X^5 + 312*X^4 - 2223*X^3 + 169*X^2 +
    506*X - 215
```

In more complicated cases, we may wish to skip this automatic reduction and do it by hand afterwards:

```
> bigpol := ComputeBigPGLPolynomial( Delta, L );
```

Verification

The computations do not give a *proven* output. We can use built-in procedures of MAGMA for several verifications, for instance the Galois group:

```
> G, R, S := GaloisGroup( pol );
> GaloisProof( pol, S );
true
> IsIsomorphic( G, PGL(2,13) );
true
```

Also, we can compute the discriminant of the number field defined by P:

```
> OM := MaximalOrder( pol );
> Factorisation( Discriminant(OM) );
[ <13, 23> ]
```

Thanks to the fact that *Serre's conjecture* has been proven, one can now use these verifications to show that P really belongs to a representation isomorphic to $\tilde{\rho}$, see [B].

Another example

The computations can also be used to produce polynomials that have certain prescribed Galois group. In $S_2(\Gamma_0(137))$ there is a newform f for which $[K_f : \mathbb{Q}] = 4$ and 2 is inert in K_f. By computing several coefficients at prime indices of f modulo 2 one can see that all elements of $\mathbb{F}_{16}$ occur as trace of $\rho = \overline{\rho}_{f,(2)}$ so the field $K = \overline{\mathbb{Q}}^{\ker(\rho)}$ has Galois group $\mathrm{SL}_2(\mathbb{F}_{16})$.

```
> S := CuspForms( Gamma0(137), 2 );
> f := Newform( S, 1 );
> Kf := BaseRing( Parent(f) );
> OKf := MaximalOrder( Kf );
> two := Decomposition( OKf, 2 )[1][1];
> pol := ComputePGLPolynomial( f, two ); pol;
X^17 - 5*X^16 + 12*X^15 - 28*X^14 + 72*X^13 -
 132*X^12 + 116*X^11 - 74*X^9 + 90*X^8 - 28*X^7 -
 12*X^6 + 24*X^5 - 12*X^4 - 4*X^3 - 3*X - 1
> G, R, S := GaloisGroup( pol );
> GaloisProof( pol, S );
true
> IsIsomorphic( G, SL(2,16) );
true
```

An explicit example of a polynomial with Galois group $\mathrm{SL}_2(\mathbb{F}_{16})$ was previously unknown.

Current limitations of the code

Currently we can compute polynomials for newforms in $S_k(\Gamma_1(N))$ for $N=1$ and $k \leq \ell+1$ arbitrary or $k=2$ and N prime. The code may sometimes fail in cases where the representation is easy to compute by hand, e.g. when it can be found inside the ℓ-torsion of an elliptic curve. In very complicated cases one may wish to break up the computation in parts. For this, please have a look in the source code of `ComputeBigPGLPolynomial`. For newforms f of level one, polynomials attached to $\tilde{\rho}_{f,\ell}$ have been computed for $\ell \leq 23$, see [B]. Several Galois groups have been explicitly realised, the most complicated ones are $\mathrm{SL}_2(\mathbb{F}_{32})$ and $\mathrm{PSL}_2(\mathbb{F}_{49})$.

Reference

[B] J. G. Bosman, *On the computation of Galois representations associated to level one modular forms*, preprint, arXiv reference 0710.1237.