Mod $\ell$ representations associated to newforms

**Theorem (Deligne).** For a newform $f = \sum a_n q^n \in S_k(\Gamma_1(N))$ with character $\chi$, a prime number $\ell$ and a prime $\ell$ | $\ell$ of the coefficient ring of $f$, there exists a two-dimensional representation $\rho_{f,\ell} : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \text{GL}_2(\mathbb{F}_\ell)$ that is unramified outside $N\ell$ and satisfies
\[
\text{charpol}(\rho_{f,\ell}((\text{Frob}_p))) = x^2 - a_p x + \varepsilon(p)p^{k-1}
\]
for all primes $p \nmid N\ell$.
Assume $k \leq \ell + 1$ and that $\rho_{f,\ell}$ is absolutely irreducible. Then one can find $\overline{\rho}_{f,\ell}$ as the action of $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on a subspace of $J_1(N')(\mathbb{C})[\ell]$ with $N' = N = k = 2$ and $N' = N\ell$ otherwise.

**MAGMA computations**

Open MAGMA and attach the source with intricins:

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

Choose your favourite cusp form, e.g.

\[
\Delta = \sum (1 - q^n)^24 = \sum \tau(n)q^n \in S_1(\text{SL}_2(\mathbb{Z})).
\]

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

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

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

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

\[
\overline{\rho}_{\Delta L} : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \text{Gal}(K_\ell/\mathbb{Q}) \hookrightarrow \text{GL}_2(\mathbb{F}_\ell).
\]

A polynomial with splitting field $K_\ell$ can be computed as follows:

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

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

**Smaller polynomials**

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

\[
\tilde{\rho} : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \text{Gal}(K'_\ell/\mathbb{Q}) \hookrightarrow \text{PGL}_2(\mathbb{F}_\ell).
\]

We can compute a polynomial $P$ with splitting field $K'_\ell$:

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

This polynomial has degree $\ell + 1$; the action of $\text{Gal}(K'_\ell/\mathbb{Q})$ on its roots is compatible with the action of $\text{im}\tilde{\rho} \subset \text{PGL}_2(\mathbb{F}_\ell)$ on $\mathbb{P}^2(\mathbb{F}_\ell)$. The intrinsic $\text{ComputeBigPGLPolynomial}$ does a reduction of coefficients as its final step.

```magma
> 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;
```

**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:

```magma
> 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 $P$:

```magma
> 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 $\rho = \overline{\rho}(2)$ so the field $K = \mathbb{Q}^{\varepsilon(\rho)}$ has Galois group $\text{SL}_2(\mathbb{F}_{16})$.

```magma
> 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 );
```

**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 $\ell$-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 $\text{ComputeBigPGLPolynomial}$. For newforms $f$ of level one, polynomials attached to $\tilde{\rho}_f$ have been computed for $\ell \leq 23$, see [B]. Several Galois groups have been explicitly realised, the most complicated ones are $\text{SL}_2(\mathbb{F}_{32})$ and $\text{PSL}_2(\mathbb{F}_{29})$.

**Reference**