Manual of the MAGMA package WEAKCONG

Gabor Wiese

6th December 2016

Abstract

The purpose of this MAGMA package is to compute whether Hecke eigenforms over $\overline{\mathbb{Q}}_p$ belong to given $\mathbb{Z}_p$-orbits of Hecke eigenforms modulo powers of p.

1 Definitions

Cusp forms and Hecke algebra

Let $S(\mathbb{C})$ be a space of modular forms, e.g. $S_k(N, \epsilon; \mathbb{C})$, the space of cusp forms of weight k, level N and character ϵ. Most of the time ϵ is trivial and we only write $S_k(N; R)$. Moreover, most of the time, the space will be an orbit ($\mathbb{Q}$, $\mathbb{Z}_p$ or $\mathbb{Q}_p$, see below). We are always in situations when it has a basis of coefficients in $\mathbb{Z}$ or $\mathbb{Z}_p$.
We denote by $S(R)$ the corresponding space with coefficients in the ring R. Here the notion $S(R)$ is the naive one via the standard q-expansion: $S(R)$ is the set of R-linear combinations of the image of the $\mathbb{Z}$-basis in $R[[q]]$ via the standard q-expansion.
The space $S(R)$ can also be characterised as follows. The Hecke operators T_n for $n \in \mathbb{N}$ acting on $S(\mathbb{C})$ generate a ring (a $\mathbb{Z}$-algebra), denoted $\mathbb{T}$, and we have the isomorphism

$$S(R) \cong \mathrm{Hom}_{\mathbb{Z}}(\mathbb{T}, R).$$

Concretely, if $\varphi \in \mathrm{Hom}_{\mathbb{Z}}(\mathbb{T}, R)$, then $\sum_{n\geq 1} \varphi(T_n)q^n$ is a cusp form. Thus a $\mathbb{Z}$-basis of $\mathbb{T}$ gives rise to a 'dual basis' of $S(R)$. We also speak of an 'echelonised basis'. See below.

$\mathbb{Q}$-orbits

By basic commutative algebra, we have decompositions

$$\mathbb{T}_{\mathbb{Q}} := \mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{T} \cong \prod_{[f]} \mathbb{T}_{[f]} \text{ and } S(\mathbb{Q}) \cong \bigoplus_{[f]} S_{[f]}(\mathbb{Q}),$$

where the product and the sum run over $G_{\mathbb{Q}}$-orbits of Hecke eigenforms. If the space $S(\mathbb{C})$ is a new space, then $S_{[f]}$ is the set of forms with coefficients in $\mathbb{Q}$ in the $\mathbb{C}$-span of all the $G_{\mathbb{Q}}$-conjugates of f. We understand by a $\mathbb{Q}$-orbit $S_{[f]}(\mathbb{Z})$. Concretely, this is the $\mathbb{Z}$-dual of the $\mathbb{Z}$-algebra generated by the Hecke operators T_n in $\mathbb{T}_{[f]}$. All Hecke operators acting on $S_{[f]}(\mathbb{Z})$ are represented as matrices with $\mathbb{Z}$-entries.

$\mathbb{Z}_p$-orbits

We consider $S(\mathbb{Z}_p)$ and $\mathbb{T}_{\mathbb{Z}_p} = \mathbb{Z}_p \otimes_{\mathbb{Z}} \mathbb{T}$. Then we have that $S(\mathbb{Z}_p) = \mathrm{Hom}_{\mathbb{Z}_p}(\mathbb{T}_{\mathbb{Z}_p}, \mathbb{Z}_p)$. Importantly, we have the decompositions

$$\mathbb{T}_{\mathbb{Z}_p} \cong \prod_{[\overline{f}]} \mathbb{T}_{[\overline{f}]} \text{ and } S(\mathbb{Z}_p) \cong \bigoplus_{[\overline{f}]} S_{[\overline{f}]}(\mathbb{Z}_p),$$

where the sum and the product run over the $G_{\mathbb{F}_p}$-orbits of Hecke eigenforms in $S(\overline{\mathbb{F}}_p)$. These correspond to the maximal ideals of $\mathbb{T}_{\mathbb{Z}_p}$. We refer to the $S_{[\overline{f}]}(\mathbb{Z}_p)$ as $\mathbb{Z}_p$-orbits, but the name $\mathbb{F}_p$-orbits would also be appropriate.
In the main application, $S(\mathbb{Z})$ will be one of the $\mathbb{Q}$-orbits $S_{[f]}(\mathbb{Z})$, i.e., we are taking $\mathbb{Z}_p$-orbits inside a $\mathbb{Q}$-orbit.

$\mathbb{Q}_p$-orbits

We are only interested in $\mathbb{Q}_p$-orbits of eigenforms inside a $\mathbb{Z}_p$-orbit. Note that $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} S(\mathbb{Z}_p) = S(\mathbb{Q}_p)$ breaks as a direct sum

$$S(\mathbb{Q}_p) \cong \bigoplus_{[\tilde{f}]} S_{[\tilde{f}]}(\mathbb{Q}_p),$$

where the sum runs over the $\overline{\mathbb{Q}}_p$-valued eigenforms up to $G_{\mathbb{Q}_p}$-conjugation. We will only compute one representative per $G_{\mathbb{Q}_p}$-orbit. The fact that these $G_{\mathbb{Q}_p}$-orbits lie in a single $\mathbb{Z}_p$-orbit simply means that they are all congruent modulo a uniformiser.

2 Mathematical background and algorithms

Echelonised basis

Let $n_1, \ldots, n_r$ be indices such that $T_{n_1}, \ldots, T_{n_r}$ form a basis of the Hecke algebra $\mathbb{T}$. We speak of *basis indices*. So, for any n, we have $T_n = \sum_{i=1}^{r} a_{n,i} T_{n_i}$; in particular, $a_{n_j,i} = \delta_{i,j}$. For each $i \in \{1, \ldots, r\}$, we define a cusp form f_i by specifying its coefficients as follows:

$$a_n(f_i) := a_{n,i}.$$

Then $f_1, \ldots, f_r$ form an R-basis of $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{T}, R)$. We call this basis echelonised because it is at the coefficients $n_1, \ldots, n_r$. It is also the dual basis of $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{T}, R)$ with respect to the basis $T_{n_1}, \ldots, T_{n_r}$ of $\mathbb{T}$.

Computing $\mathbb{Q}$-orbits

This is standard commutative algebra. We use the implementation in the MAGMA package ARTINALGEBRAS.

Computing $\mathbb{Z}_p$-orbits

We compute $\mathbb{Z}_p$-orbits using Hensel lifting of idempotents, as implemented in the MAGMA package PADICALGEBRAS.
A basis of modular forms in $S_{[\overline{f}]}(\mathbb{Z}_p)$ is computed as the dual basis in echelonised form (see above) for indices of Hecke operators $n_1, \dots, n_r$; the latter are computed via Nakayama's lemma, i.e. by reducing the matrices to $\mathbb{F}_p$.

Computing $\mathbb{Q}_p$-eigenforms

This is standard linear algebra over local fields, using both the new MAGMA command LocalField and the older implementation. If we find that a system of linear equations which mathematically must have a solution does not seem to have any, then we lower the precision until the desired solution exists. Thus, in this procedure generally some precision is lost.

Weak congruences

Let $g = \sum_{n \geq 1} b_n q^n \in S(\overline{\mathbb{Q}}_p)$ be an eigenform in some level and weight. Let $\mathcal{O}$ be the valuation ring of some finite extension of $\mathbb{Q}_p$ that contains all coefficients b_n of g, and let π be a uniformiser of $\mathcal{O}$. The main purpose of this package is to compute the maximum integer m such that g lies in a given $\mathbb{Z}_p$-orbit (some level and some weight) modulo π^m.
Let $f_1, \dots, f_r$ be a $\mathbb{Z}_p$-basis of the $\mathbb{Z}_p$-orbit with respect to given basis indices $n_1, \dots, n_r$ as above. Put $h := g - \sum_{i=1}^r b_{n_i} f_i$. We then have:

$$h \equiv 0 \mod \pi^m \Leftrightarrow \exists\, s_1, \dots, s_r \in \mathcal{O} : g \equiv \sum_{i=1}^{r} s_i f_i \mod \pi^m.$$

This equivalence is clear as the basis is echelonised, whence automatically $s_i = b_{n_i}$ for all $i = 1, \dots, r$.
The desired highest exponent m can thus be computed as the minimum of the valuations of the coefficients of h up to the Sturm bound.

Acknowledgements

I thank Panos Tsaknias for having programmed the code for the database, for which this package has mainly been developed, having set it up and for many very useful discussions.

3 Usage and Example

We first need to attach the package.

```
folder := "~/Dropbox/wtlow_ell-adic/";
Attach(folder*"weak_cong/WeakCong.m");
```

The most basic command is this one:

```
WeakCong (L1,L2 : bound := 100, prime_to := 1);
```

Here L1 is for instance the list of Hecke operators in first $\mathbb{Z}_2$-orbit in the only $\mathbb{Q}$-orbit of modular forms of level 1, weight 30, in the sense that L1[n] is T_n. For L2 one can for instance take the list of Hecke operators in first $\mathbb{Z}_2$-orbit in the only $\mathbb{Q}$-orbit of modular forms of level 1, weight 46, also in the sense that L2[n] is T_n. For each such $\overline{\mathbb{Q}}_2$-eigenform f described by the matrices in L2, compute the highest exponent n such that f lies in the first $\mathbb{Z}_2$-orbit described by L1. The answer is:

```
[ <6, 1>, <12, 2> ]
```

This means that there are two $\overline{\mathbb{Q}}_2$-eigenforms (up to $G_{\mathbb{Q}_2}$-conjugacy) in the high weight. The first one is congruent to a form in the low weight modulo 2^6 and the coefficient field is unramified. The second one is congruent to a form in the low weight modulo π^{12}, where π is a uniformiser of an extension of $\mathbb{Q}_2$ of ramification index 2; i.e. also the second congruence is modulo 2^6.

Here's the same example again, but presented 'by hand' and thus illustrating other functions. Suppose that L1 and L2 are as above.

```
F1,bi1 := Zp_forms(L1);
F2 := Qpbar_eigenforms(L2);
#F2;
belongs_to_mod_pm (F1,bi1,F2[1]);
belongs_to_mod_pm (F1,bi1,F2[2]);
```

All modular forms are realised as functions with source $\mathbb{N}$. When they are evaluated, some system of linear equations is solved. In some applications one wants to use the same coefficient several times. In order to avoid recomputing the same system of linear equations, it is possible to transform the functions into lists of their values and to work with these data. We illustrate this by presenting the same example in the list/tuple version.

```
F1,bi1 := Zp_forms(L1);
F2 := Qpbar_eigenforms(L2);

M1 := make_tup_of_lists(F1);
M2 := make_tup_of_lists(F2);

belongs_to_mod_pm_lists (M1,bi1,M2[1]);
belongs_to_mod_pm_lists (M1,bi1,M2[2]);
```

Here are the most important signatures with a little explanation.

```
intrinsic Extract_Zp_basis (L : known_dim := 0) -> Any
```

Input: L=list of matrices over a p-adic ring.
Option: known_dim=the dimension of the space spanned by L.
Output: Basis of the space spanned by L.
This function uses Nakayama's lemma and works by computing an $\mathbb{F}_p$-basis of the reductions.

```
intrinsic Zp_forms (L : known_dim := 0) -> Any
```

Input: L=list of Hecke operators over $\mathbb{Z}_p$ such that L[n] is the n-th Hecke operator.
Option: known_dim=dimension of the span of L (if known).
Output: out,bi, where out=list the elements of which form a basis of the space of modular forms described by the dual of the algebra generated by the given Hecke operators. Any modular form is represented as a function $\mathbb{N} \to \mathbb{Z}_p$, sending n to a_n. bi=list the elements of which are indices i such that the L[i] form a $\mathbb{Z}_p$-basis.

```
intrinsic belongs_to_mod_pm ( F :: SeqEnum, bi :: SeqEnum, g :: Any :
                                          bound := 2000, prime_to := 1) -> Any
```

Input: F=list of functions $\mathbb{N} \to \mathbb{Z}_p$ which are an echelonised basis, where the echelon part is given by bi.
g=another function $\mathbb{N} \to \mathcal{O}$, where $\mathcal{O}$ is a valuation ring.
Output: <m,e> with maximum m such that modulo the uniformiser of $\mathcal{O}$ to the m-th power, g belongs to the space spanned by F; e is the ramification index of the coefficient ring of g. Only coefficients will be compared the index of which is prime to prime_to. bound is an upper bound for the number of coefficients to be used.

```
intrinsic belongs_to_mod_pm_lists ( F :: Tup, bi :: SeqEnum, g :: SeqEnum :
                                          bound := 2000, prime_to := 1) -> Any
```

Input: F=list of lists representing functions $\mathbb{N} \to \mathbb{Z}_p$ which are an echelonised basis, where the echelon part is given by bi.
g=list representing a function $\mathbb{N} \to \mathcal{O}$, where $\mathcal{O}$ is a valuation ring.
Output: <m,e> with maximum m such that modulo the uniformiser of $\mathcal{O}$ to the m-th power, the function given by g belongs to the space spanned by by the functions in F; e is the ramification index of the coefficient ring of g. Only coefficients will be compared the index of which is prime to prime_to. bound is an upper bound for the number of coefficients to be used.

```
intrinsic make_list ( F :: Any : bound := 0 ) -> SeqEnum
```

Input: F=function with source $\mathbb{N}$.
Output: a list of the values of F.
Option: If bound has a nonzero value, then only go up to that value. Otherwise go on until the evaluation fails.

```
intrinsic make_tup_of_lists ( F :: Any : bound := 0 ) -> Tup
```

Input: F=list of functions with source $\mathbb{N}$. Output: a tuple the i-th entry of which is a list of the values of F[i]. Option: If bound has a nonzero value, then only go up to that value. Otherwise go on until the evaluation fails.

```
intrinsic Qpbar_eigenforms (L :: SeqEnum) -> Any
```

Input: L=list of Hecke operators over $\mathbb{Z}_p$ such that L[n] is the n-th Hecke operator.
Output: list of common eigenvectors given as functions $\mathbb{N} \to \mathcal{O}$, sending n to the corresponding eigenvalue of L[n].

```
intrinsic WeakCong (L1 :: SeqEnum, L2 :: SeqEnum : prime_to := 1, bound := 2000)
                                                                          -> Any
```

Input: L1,L2=lists of Hecke operators over $\mathbb{Z}_p$ such that Li[n] is the n-th Hecke operator.
Output: List of entries of the form <n,e>, where n means that there is a $\overline{\mathbb{Q}}_p$-eigenform in the $\mathbb{Z}_p$-orbit of g that is congruent modulo π^n to a modular form in the $\mathbb{Z}_p$-orbit f; n is maximal with this property; π is a uniformiser of th p-adic coefficient field of g, which is of absolute ramification index e.
Option: prime_to indicates that in the comparison only Hecke operators with index prime to prime_to are used; bound is an upper bound for the number of coefficients to be compared.