Some Computations in Support of Maeda's Conjecture

Seth Kleinerman

February 23, 2004

1 Introduction

$S_k(1)$ is the space of cusp forms of level 1 and weight k. For k odd, this space has dimension zero, since a form in it would have to satisfy $f(\tau) = (-1)^k f(\tau)$, by applying the definition of modular form, using the matrix $-I \in \mathrm{SL}_2(\mathbb{Z})$. For k even, the dimension of $S_k(1)$ grows roughly as $k/12$ (for an exact formula, see Stein's lecture notes for Math 252 [6]). Here we will consider only those k for which the dimension of the space of cusp forms is positive.

The Hecke algebra is a subring of the endomorphism ring of $S_k(1)$, generated by the Hecke operators T_n. Since a Hecke operator acts on the finite-dimensional vector space $S_k(1)$, given a basis of the space we can write down the matrix corresponding to T_n, and a natural thing to do then is to consider the characteristic polynomial of that matrix, since it characterizes the operator without regard to the basis we'd chosen. Yoshitaka Maeda considered these characteristic polynomials and conjectured that where p is a prime, the characteristic polynomial of T_p acting on $S_k(1)$ is irreducible. (It is not generally irreducible on $M_k(1)$, the full modular subspace.) We will confirm his conjecture for the operators T_2 and $k \leq 3000$.

2 Algorithms Testing Polynomial Irreducibility

A standard algorithm used to test for irreducibility of polynomials comes from a factorization algorithm due to Berlekamp (1967): the following treatment is given in complete detail in Knuth [5].

We are given a polynomial $f(x)$ of degree n. First it is standard to reduce to the case of squarefree polynomials (if $f(x)$ isn't squarefree, which we test by computing $\gcd(f(x), f'(x))$, we already know it isn't irreducible). Now choose a prime p. All computations from here on out are in $\mathbb{F}_p$.

Assume that f splits into a product of prime factors $q_1 \dots q_r$. Let's say we have a corresponding set of integers $s_1, \dots, s_r \in \mathbb{F}_p$. By the Chinese remainder theorem, there is a unique polynomial $v(x)$ of degree less than n that reduces to s_i modulo q_i for all i. This polynomial has an interesting property: modulo f, $v(x)^p \equiv v(x)$, because, modulo each of the q_i, we have $v(x)^p \equiv s_i^p = s_i \equiv v(x)$, with the middle equality by Fermat's Little Theorem.

The key observation is that (modulo p) the polynomial identity

$$v(x)^p - v(x) = (v(x) - 0)(v(x) - 1) \dots (v(x) - (p-1))$$

holds for any choice of v. (This is an algebraic identity that arises from considering the factorization of $x^p - x$ in $\mathbb{F}_p$.) In particular, if we have chosen v as above, the left side is divisible by f and so each of the prime factors of f divides one of the elements in the product on the right. If we knew that q_i divided $(v - k)$, we would then know that s_i, from above, equalled k. Then every r-tuple $s_1, \dots, s_r \in \mathbb{F}_p$ is in one-to-one correspondence with a polynomial v for which $v(x)^p \equiv v(x)$ modulo f, and therefore there are obviously p^r such polynomials.

Now construct the matrix

$$Q = \begin{pmatrix} a_{0,0} & a_{0,1} & \cdots & a_{0,n-1} \\ \vdots & \vdots & & \vdots \\ a_{n-1,0} & a_{n-1,1} & \cdots & a_{n-1,n-1} \end{pmatrix}$$

where the entries $a_{m,i}$ are defined by

$$(x^p)^m \equiv \sum_{i=0}^{n-1} a_{m,i} x^i \mod f.$$

A polynomial $v(x) = \sum_{i=0}^{n-1} v_i x^i$ satisfies $v(x)^p \equiv v(x) \mod f$ iff $(v_0, v_1, \ldots, v_{n-1})Q = (v_0, v_1, \ldots, v_{n-1})$, as follows:

$$v(x) = \sum_i v_i x^i = \sum_i \sum_j v_j a_{j,i} x^i,$$

but we can simplify this sum as

$$\sum_j v_j (x^p)^j = v(x^p) = v(x)^p$$

by the equivalence that defines the elements $a_{j,i}$.

Therefore we are looking for left-multiplication eigenvectors of Q with eigenvalue 1, and so the thing to do is examine the matrix $Q - I$. Its kernel contains exactly the polynomials we need; the dimension of the kernel is the number of irreducible factors of f. To see this, remember that the number of such polynomials is p^r as explained above, where r is the number of irreducible factors of f, and thus the dimension of the kernel is r.

So that represents a test of irreducibility: construct Q as above. If $\dim(\ker(Q - I)) = 1$, then the polynomial f is irreducible; if not, then it splits into $\dim(\ker(Q - I))$ factors.

MAGMA has been using a recent algorithm by van Hoeij (2002) [4], which he calls “knapsack factoring.” It relies on Berlekamp’s method but is supposed to be more practical in some ranges.

3 Computations

Previous computations (by Kevin Buzzard and by William Stein using MECCAH and NERON) have produced the characteristic polynomials of T_2 acting on $S_k(\mathrm{SL}_2(\mathbb{Z}))$ for $k \leq 3000$. Since the conjecture has been confirmed for these polynomials with $k \leq 2048$ (see Farmer and James [2] for the result up to 2000, and Buzzard for the check up to 2048) it remained to check the irreducibility of these polynomials for $2048 < k \leq 3000$.

To do the check, first we wrote the strings “is” and “close,” which when girding the polynomials makes them MAGMA-executable files:

```
echo "R<x> := PolynomialRing(Integers()); time IsIrreducible(" > is
echo ");" > close
```

Next, we wrote a script to test the polynomials of weight k in a certain range, which we called test.sh:

```
#!/bin/sh
for x in ‘seq $1 2 $2‘; do cat is $x close | magma > $x.out; done &
```

Finally, we ran twelve occurences of this script, one on each processor of the MECCAH cluster, with ranges breaking up 2050-3000 given here by [start] and [end]:

```
nohup ./test.sh [start] [end]
```

MECCAH is working on these and should be finished in a few days. Each computation takes somewhere between 1 and 8 hours on its processors, which are Athlon 2800 MPs. We use the following command to output the number of polynomials confirmed to be irreducible, and the number of failures:

```
grep "^true" *.out | awk -F: ’{ print $1; }’ | wc -l;
grep "^false" *.out | awk -F: ’{ print $1; }’ | wc -l
```

To date, MECCAH has confirmed the irreducibility of 130 of the 476 polynomials, and produced no counterexamples to Maeda’s conjecture.

4 Applications

Hida [3] mentions in a lecture that if one assumes Maeda's conjecture and a conjecture about the prevalence of "ordinarity" for Hecke eigenforms, all Hecke eigenforms of level 1 are liftable. However, his notes on the subject are only schematic.

References

[1] K. Buzzard. *On the Eigenvalues of the Hecke Operator* T_2. Journal of Number Theory, vol. 57, no. 1, pp. 130-132.

[2] D.W. Farmer and K. James. *The Irreducibility of Some Level 1 Hecke Polynomials.* Mathematics of Computation, vol. 71, no. 239, pp. 1263-1270.

[3] H. Hida. *Modularity Problems of* $\mathbb{Q}$*-motives and Base-Change.* Notes for lecture series at Strasbourg, France, 31 Jan.-4 Feb 2000.

[4] M. van Hoeij. *Factoring Polynomials and the Knapsack Problem.* Journal of Number Theory, vol. 95, no. 2, pp. 167-189.

[5] D.E. Knuth. *The Art of Computer Programming*, vol. 2. Addison Wesley, Reading, Massachusetts, 3rd edition, 1997, pp. 439-461.

[6] W. Stein. Lecture notes for Math 252.