COMPUTING A BASIS OF MODULAR FORMS

DENIS XAVIER CHARLES

1. Introduction

In this article we consider the problem of computing the Fourier coefficients of a basis of modular forms. Let S_k be the space of cusp forms of weight k for the full modular group $SL_2(\mathbb{Z})$. The standard basis for this space for k even consists of the forms $\Delta^i G_{k-i}$ for $1 \le i \le \lfloor \frac{k-4}{12} \rfloor$, and $\Delta^{\frac{k}{12}}$ if $k \equiv 0 \mod 12$, where G_k is the weight k Eisenstein series and Δ is the discriminant function. It is easy to see that the n-th Fourier coefficient of any of these basis forms can be computed in time $O(n^2)$. In this article we show that there is a basis for this space composed of forms for which we can compute the n-th Fourier coefficient in time $O(n^{\frac{1}{2}+\epsilon})$ by a randomized algorithm.

2. Cyclic basis for modular forms

Let V be any finite dimensional vector space and let $T : V \to V$ be a linear map. Suppose that there is a $\mathbf{v} \in V$ such that $T(\mathbf{v}), T(T(\mathbf{v})), \cdots$, form a basis of V, then we say that V has a *cyclic basis* with respect to T (or simply T has a cyclic basis). For example, the finite field $\mathbb{F}_{p^n}$ is a $\mathbb{F}_p$-vector space of dimension n, and it is a fact that $\mathbb{F}_{p^n}$ has a cyclic basis with respect to the Frobenius automorphism $x \mapsto x^p$.

For the space S_k of cusp forms of weight k and level 1, we have a family of operators T_p for each prime p, called the Hecke operators. These operators are easily defined by their action on the Fourier coefficients of the modular forms. Suppose $f = \sum_{1 \le n} a(n) q^n \in S_k$, then

$$T_p f \stackrel{\triangleright}{=} \sum_{1 \le n} \big(a(np) + p^{k-1} a(n/p) \big) q^n.$$

It is natural to ask: for which primes p does S_k have a cyclic basis with respect to T_p. A complete answer to this question is very difficult. For example, for $k = 12$ the operator T_p has a cyclic basis iff $\tau(p) \neq 0$ and so the existence of a cyclic basis for T_p for every prime p is equivalent to Lehmer's conjecture. In what follows we will show that for every even $k \ge 12$ there is a set of primes $\mathcal{P}$ of density 1 such that for every $p \in \mathcal{P}$ the operator T_p has a cyclic basis. We begin with a lemma.

Lemma 2.1. *Let V be a finite dimensional vector space (say $\dim V = d$), and let $T : V \to V$ be a linear map. Suppose that V has a basis of eigenvectors $\mathbf{v}_1, \cdots, \mathbf{v}_d$ with corresponding eigenvalues $\alpha_1, \cdots, \alpha_d$. If $\alpha_i \neq 0$ and $\alpha_i \neq \alpha_j$ for $i \neq j$ then T has a cyclic basis.*

Proof : Consider the vector $\mathbf{w} = \mathbf{v}_1 + \mathbf{v}_2 + \cdots + \mathbf{v}_d$. Now $T(\mathbf{w}), T(T(\mathbf{w})), \cdots, T^d(\mathbf{w})$ are linearly independent iff the determinant of the following matrix does not vanish:

$$\begin{pmatrix} \alpha_1 & \alpha_2 & \cdots & \alpha_d \\ \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_d^2 \\ \vdots & \vdots & & \vdots \\ \alpha_1^d & \alpha_2^d & \cdots & \alpha_d^d \end{pmatrix}.$$

Date: 26 June, 2003.

Since this is a Vandermonde matrix, its determinant is

$$\alpha_1 \cdots \alpha_d \prod_{1 \leq i < j \leq d} (\alpha_i - \alpha_j)$$

and so the lemma follows. □

Now we are ready to prove our main theorem.

Theorem 2.2. *Let S_k be the space of weight k level 1 cusp forms. If $k \geq 12$ is even, then there is a set of primes $\mathcal{P}$ of positive density such that for every prime $p \in \mathcal{P}$ the p-th Hecke operator T_p has a cyclic basis.*

Proof : The space S_k has a basis of forms that are simulataneously eigenforms for all the Hecke operators T_p. Moreover, these forms can be normalized such that the p-th Hecke eigenvalue is their p-th Fourier coefficient. We show that the hypotheses of lemma 2.1 are satisfied by T_p for a density 1 subset of the primes. Let $f_i = \sum_n a_i(n)q^n, 1 \leq i \leq d$ be the Hecke eigenforms which form a basis for S_k. Let P_i denote the set of primes where $a_i(p) \neq 0$, and let P_{ij} denote the set of primes where $a_i(p) \neq a_j(p)$ for $i \neq j$. A theorem of Serre shows that each of the sets P_i is a density 1 subset of the primes ([Ser81] Corollary 2 to Theorem §7.2.15). A *super-strong* multiplicity one theorem due to Rajan [Raj98] shows us that if $f \neq g$ are cuspidal eigenforms of level 1 then there is a density 1 subset of primes on which their coefficients differ. Note that the techniques of Serre yield only that there is a constant proportion of primes where their coefficients differ. Now the set $\mathcal{P} = \cap_i P_i \cap_{i \neq j} P_{ij}$ has density 1 since we are taking the intersection of finitely many subsets each of density 1. Furthermore, for any prime $p \in \mathcal{P}$ the Hecke operator T_p satisfies all the hypotheses of lemma 2.1 and consequently has a cyclic basis. □

3. Description of the algorithm

In this section we give a brief description of the algorithm to compute a basis for the space S_k. For details on some of the steps refer to [Cha03].

The space $M_k = E_k \oplus S_k$, where E_k is the space generated by the Eisenstein series of weight k. The n-th Fourier coefficient of E_k is $\sigma_{k-1}(n)$ for $n > 1$. We can compute this function in $O(\exp(\sqrt{\log n \log\log n}))$ time using randomized subexponential time factoring algorithms. We show that there is a basis for S_k of forms whose n-th Fourier coefficient can be computed in $O(n^{\frac{1}{2}+\epsilon})$ time by a randomized algorithm. By theorem 2.2 there is a density 1 subset of primes p for which the p-th Hecke operator T_p has a cyclic basis. In particular, for each k there exists *a* prime p_k such that T_{p_k} has a cyclic basis. Moreover, lemma 2.1 says that the cyclic vector can be taken to be the form whose coefficients are given by the trace of the Hecke operators. In [Cha03] it is shown that this trace can be computed by a randomized algorithm in $O(n^{\frac{1}{2}+\epsilon})$ time. Now we can compute the n-th Fourier coefficient of each of the basis forms by finding the n-th Fourier coefficient of the form whose coefficients are the Hecke traces and then explicitly computing the action of the operator T_{p_k} on this form.

References

[Cha03] Charles, Denis; *Computing the Ramanujan Tau function*, preprint, 2003.

[Raj98] Rajan, C., S.; *On strong multiplicity one for ℓ-adic representations*, Int. Math. Res. Notices, **3**, 161-172, 1998.

[Ser81] Serre, Jean-Pierre; *Quelques applications du Théorème de Densité de Chebotarev*, Publ. Math. I.H.E.S., **54**, 123-201, 1981.