LINEAR DEPENDENCE AMONG HECKE EIGENVALUES

Abstract. We prove an explicit upper bound on the absolute value of the coefficients of a non-trivial integral linear relation among Hecke eigenvalues of a given cuspidal eigenform. Our motivation lies in its algorithmic application. For any fixed positive integer n, the bound established here yields an algorithm that computes cuspidal Hecke eigenforms whose Hecke eigenvalues generate a number field of degree n. By working with linear combinations of Hecke operators, the resulting algorithm avoids multiplication of large matrices.

1. Introduction

Hecke showed that, if

$$f(q) = \sum_{m=1}^{\infty} a_m q^m, \ a_m \in \mathbb{C}$$

is the Fourier expansion of a primitive normalized cuspidal modular form of weight $k \geq 2$, then its coefficients satisfy

$$a_m = O(m^{\frac{k}{2}})$$

where the implied constant only depends on the form. Deligne, using his deep work confirming the Weil conjecture, lowered the exponent by one half. Furthermore, the implied constant was made absolute. More precisely, he showed that the inequality

$$|a_m| \leq d(m) m^{\frac{k-1}{2}}$$

holds true for any $m \geq 1$, where $d(m)$ denotes the number of positive divisors of m.

On the other hand, the Hecke field of $f(q)$, the subfield of $\mathbb{C}$ generated by all a_m's is of finite degree, say n, over $\mathbb{Q}$. Then, Deligne's bound allows one to bound the coefficients of the minimal polynomial of a_m in terms of k, m, and n. This cuts out a finite collection of polynomials that can be potentially satisfied by some a_m.

Our aim in this article is to construct a collection of linear relations among multiple a_m's. More precisely, for a given choice $(m_1, m_2, \cdots, m_{n+1})$ of $n+1$ distinct indices, we want to produce positive integers $b_1, b_2, \cdots, b_{n+1}$ which shall guarantee a non-trivial relation

$$\sum_{i=1}^{n+1} \lambda_i a_{m_i} = 0, \quad \lambda_i \in \mathbb{Z}$$

such that $|\lambda_i| \leq b_i$ for all i.

To state our main results, we need some notation. For integers $k \geq 1$ and $m \geq 1$, let

$$\rho_{m,k} = d(m) m^{\frac{k-1}{2}}$$

Date: October 2018.

be the Deligne bound. For an integer $n \geq 1$, define

$$\rho'_{m,k} = \begin{cases} \rho_{m,k} & \text{if } m = 1 \text{ or } k = 1 \\ \left(\rho_{m,k}^2 - \frac{4}{n}\right)^{\frac{1}{2}} & \text{if } m \geq 2 \text{ and } k \geq 2. \end{cases}$$

Clearly, $\rho_{m,k} \geq \rho'_{m,k}$, and the inequality is strict unless $m = 1$ or $k = 1$. We also need two real-valued quantities $\eta(n)$ and $\theta(n)$. We require that $\eta(n)$ is a lower bound for the root discriminant of a totally real number field. Explicit values of $\eta(n)$ have been obtained by Odlyzko [8]. For $\theta(n)$, we require that any lattice of dimension n inside $\mathbb{R}^n$ admits a basis whose orthogonality defect is at most $\theta(n)$. Various forms of $\theta(n)$ are available [6, 9]. Asymptotically, $\eta(n) = 60^n - o(n^{-2/3})$ due to [8], and $\theta(n) = 2^{O(n \log n)}$ due to [6]. In any case, we define

$$\rho(n) = \frac{\theta(n)}{\eta(n)^{n/2}}$$

to be the ratio.

Theorem 1.1. *Let $f(q) = \sum_{n \geq 1} a_n q^n$ be a normalized cuspidal Hecke eigenform of level N, character χ, and weight $k \geq 1$. Let n be the degree of the maximal totally real subfield of the Hecke field of $f(q)$. Choose $m_1, \cdots, m_{n+1}$ such that $\chi(m_i) = 1$ for all i. For each $1 \leq i \leq n+1$, define $b_{i,n,k}$ to be*

$$b_{i,n,k} = n^{n/2} \rho(n) \sum_{j \neq i} \rho'_{m_j,k}$$

where the sum is taken over the range $1 \leq j \leq n+1$ and $j \neq i$. Then, there is a non-trivial linear relation $\sum \lambda_i a_i = 0$ with $\lambda_i \in \mathbb{Z}$ and $|\lambda_i| \leq b_{i,n,k}$, or one of the two following degenerate cases occur.

(1) $a_{m_j}^2 \in \mathbb{Z}$ for some j.

(2) The $\mathbb{Z}$-module spanned by all a_{m_j}'s has rank strictly smaller than n.

The quantity $\rho(n)$ is independent of k. We list some of its values in Table 1.

TABLE 1. Some values of $\rho(n)$

n	2	3	4	5	6	7	8
$\rho(n)$	0.5165	0.3866	0.3855	0.4645	0.7890	1.4139	4.2889

The choice $m_1, m_2, \cdots, m_{n+1}$ that minimizes $\sum \rho'_{m_j,k}$ depends on k, because the ordering of positive integers by there associated Deligne bounds $\rho_{m,k}$ is not the same as the natural one. Roughly speaking, primes appear early in the ordering if k is small. We present Table 2 for readers' convenience.

Corollary 1.2. *Suppose that χ is trivial and $k = 2$. For each $2 \leq n \leq 8$, Table 3 shows the values of $b_{i,n,k}$, where m_i's are chosen to be the first $n+1$ elements in the second row of Table 2*

Corollary 1.3. *Suppose that χ is trivial and $n = 3$, $k = 2$. Then $|\lambda_1| \leq 7$, $|\lambda_2| \leq 6$, $|\lambda_3| \leq 6$, and $|\lambda_5| \leq 4$.*

TABLE 2. Ordering positive integers by Deligne bounds

$k=1$	1	2	3	5	7	11	13	17	19	23	29	31	37	41
$k=2$	1	2	3	5	7	4	11	13	17	19	9	23	6	29
$k=3$	1	2	3	5	4	7	11	6	13	9	8	17	19	10
$k=4$	1	2	3	5	4	7	6	11	9	8	13	10	17	19
$k=5$	1	2	3	4	5	7	6	11	9	8	13	10	17	19
$k=6$	1	2	3	4	5	7	6	8	9	11	13	10	17	14

TABLE 3. Values of $b_{i,n,2}$ with $2 \leq n \leq 8$

i	1	2	3	4	5	6	7	8	9
m_i	1	2	3	5	7	4	11	13	17
$n=2$	5	4	3						
$n=3$	10	9	8	7					
$n=4$	18	16	15	14	13				
$n=5$	31	29	28	26	25	24			
$n=6$	71	67	65	63	61	59	57		
$n=7$	112	106	104	101	98	96	94	92	
$n=8$	520	499	492	479	470	461	454	447	434

As an application of Theorem 1.1, we propose an algorithm to enumerate cuspidal Hecke eigenforms whose Hecke fields have bounded degrees. The input is a basis for a rational vector space V of cuspidal modular forms of level N and character χ, together with Hecke operators $T_{m_1}, \cdots, T_{m_{n+1}}$ such that $\chi(m_j) = 1$ for all j. We assume that V is semisimple as a module over the Hecke algebra. The output is the list of n-dimensional irreducible Hecke submodules inside V. This would solve the enumeration problem since such a Hecke submodule is necessarily generated by Galois conjugates of a desired eigenform. If $W \subset V$ is such a submodule to be found, then it can be characterized as its annihilators; elements in the Hecke algebra which act as multiplication by zero on W. Theorem 1.1 allows one to find a non-trivial annihilator of W as follows. If $f(q) \in W \otimes_{\mathbb{Q}} \mathbb{C}$ is a desired eigenform which is non-degenerate in the sense of Theorem 1.1, then it must be killed by some $T_\lambda := \sum_i \lambda_i T_{m_i}$ whose coefficients satisfy $|\lambda_i| \leq b_{i,n,k}$. Therefore, finding kernels of T_λ and decomposing them into irreducible Hecke submodules will yield a complete list of such forms. Degenerate forms need to be found separately.

The problem to enumerate degenerate forms has different flavors depending on n. For example, the first degenerate case cannot occur if n is odd. Also, the second non-degenerate case is equivalent to some of a_{m_i} being rational if $n = 2$. We do not make an attempt to handle these degenerate cases, although they must be worked out in order to make the above algorithm practically useful.

Leaving aside the issue of degenerate forms, our algorithm has an additional advantage. Recall that Brandt matrices reproduce the spectra of Hecke operators. Moreover, Brandt matrices are by construction sparse. Empirical evidence suggests that linear relations among multiple Hecke operators tend to have lower density than polynomial relation of a single Hecke operator.

In the case when $n = 1$, $k = 2$, and χ is trivial, our method reduces to that of Cremona which he employed, among many other things, in order to generate his database [4, 5]. In this sense, our theorem can be seen as a modest attempt to extend his strategy to all modular forms.

The organization of the paper is as follows. We first prove a lemma about linear relation among algebraic integers. We review Odlyzko's discriminant bounds and Minkowski-van der Waerden bounds for orthogonality defects, both of which we employ to bound $\rho(n)$. We will explain how Kronecker's theorem can break the barrier of Deligne's bound. Combining these results, we will obtain the main theorem.

Acknowledgements. The author is grateful for helpful comments by J. Cremona, D. Sutherland, and J. Voight. This work is partially supported by Simons Foundation grant 550033.

2. Linear relations among algebraic integers in a given number field

Suppose that F is a number field of degree n with its ring of integers O_F. Its rank as a $\mathbb{Z}$-module is n, so any collection of $n+1$ elements $\alpha_1, \cdots, \alpha_{n+1} \in O_F$ is linearly dependent over $\mathbb{Z}$. We are interested in a quantitative relation between α_i's and their relations.

In this section, we will assume that the $\mathbb{Z}$-submodule of O_F generated by $\alpha_1, \cdots, \alpha_{n+1}$ has rank n. This implies that the subset $\Lambda \subset \mathbb{Z}^{n+1}$ consisting of all $(n+1)$-tuples $\mathbf{r} = (r_1, \cdots, r_{n+1}) \in \mathbb{Z}^{n+1}$ such that $\sum r_i \alpha_i$ is free of rank one as a $\mathbb{Z}$-module. Let

$$\lambda(\alpha_1, \cdots, \alpha_{n+1}) = (\lambda_1, \cdots, \lambda_{n+1}) \in \Lambda$$

be a generator of Λ. It is well-defined up to sign. In particular, for each i, $|\lambda_i|$ is well-defined.

We introduce a characterization of $\Lambda \subset \mathbb{Z}^{n+1}$. Let $\tau\colon F \to \mathbb{Q}$ be the trace map. Consider an auxiliary set of elements

$$\beta_1, \cdots, \beta_{n+1} \in O_F$$

that span O_F. Consider an $(n+1) \times (n+1)$ matrix $B = (b_{ij})_{1 \le i,j \le n+1}$ with its entries $b_{ij} = \tau(\beta_i \alpha_j)$.

Lemma 2.1. *Let $\mathbf{r} \in \mathbb{Z}^{n+1}$. Then, $B\mathbf{r} = 0$ if and only if $\mathbf{r} \in \Lambda$.*

Proof. Assume $\mathbf{r} \in \Lambda$. By definition, $\sum_i r_i \alpha_i = 0$, the sum taken over $i \in \{1, 2, \cdots, n+1\}$. In particular, $\beta_j \sum_i r_i \alpha_i = 0$ for all j. Applying τ, one obtains $\sum_i r_i \tau(\beta_i \alpha_j) = 0$. This means $B\mathbf{r} = 0$.

Conversely, assume $B\mathbf{r} = 0$. Let $\gamma = \sum_i r_i \alpha_i$. Then, $\tau(\beta_j \gamma) = 0$ for all j. Since the trace form in non-degenerate and β_j's span F, it implies that $\gamma = 0$, or equivalently that $\mathbf{r}$ belongs to Λ. □

We return to our goal of the section: to bound $|\lambda_i|$ from above in terms of β_i's. Define a map

$$\mathcal{M}\colon F \to \mathbb{R}$$

so that $\mathcal{M}(\alpha)$ is the average of $|\sigma(\alpha)|^2$ taken over the archimedean places σ of F. In fact, $\mathcal{M}(\alpha)$ is absolute in that it does not depend on the choice of a number field that contains

α. For example, $\mathcal{M}(1+\sqrt{2}) = \frac{1}{2}(3+2\sqrt{2}) + \frac{1}{2}(3-2\sqrt{2}) = 3$ and $\mathcal{M}(1+\sqrt{-3}) = 4$. We also define

$$\mu(\alpha) = (\mathcal{M}(\alpha))^{1/2}.$$

Lemma 2.2. *For each $i = 1, 2, \cdots, n+1$, we have*

$$|\lambda_i| \leq \frac{n^n}{|D_F|} \prod_j \mu(\beta_j) \sum_k \mu(\alpha_k)$$

where j and k run over $\{1, 2, \cdots, i-1, i+1, \cdots, n+1\}$.

Proof. By symmetry, in suffices to prove the assertion when $i = n+1$. We may further assume that $\lambda_{n+1} \neq 0$, otherwise the desired inequality is vacuously true. This further assumption is equivalent to the collection $\alpha_1, \cdots, \alpha_n$ being linearly independent over $\mathbb{Z}$.

The proof consists of two steps. First, we will construct $\lambda^* = (\lambda_1^*, \cdots, \lambda_{n+1}^*) \in \Lambda \setminus \{0\}$ and prove

$$|\lambda_{n+1}^*| \leq n^n \prod_{i=1}^{n} \mu(\beta_i) \sum_{j=1}^{n} \mu(\alpha_j). \tag{2.3}$$

Second, we will show that $\lambda^* \in D_F\Lambda$. Combining these two assertions, one would deduce the desired inequality by noting that $\frac{1}{D_F}\lambda^* = c\lambda$ for some $c \in \mathbb{Z} \setminus \{0\}$.

Let us construct λ^*. By Lemma 2.1, it suffices to construct λ^* with $B\lambda^* = 0$. We employ the Laplace expansion. Let $B(i,j)$ be the $n \times n$ minor of B obtained by removing the i-th row and the j-th column. Define $\lambda_i^* = (-1)^{i+1+n} \det B(n+1, i)$. The Laplace expansion for $\det B$, which is zero, implies that $B\lambda^* = 0$.

Let us verify $\lambda^* \neq 0$. It suffices to show $\lambda_{n+1}^* \neq 0$ or equivalently $\det B(n+1, n+1) \neq 0$. Indeed, by the assumption that $\alpha_1, \cdots, \alpha_n$ are linearly independent, one deduces $\det B(n+1, n+1) \neq 0$.

To obtain (2.3), we need to bound $\det B(n+1, n+1)$. Recall that the magnitude of the determinant of a matrix is at most the product of the Euclidean lengths of its columns. On the other hand, $|\tau(\alpha\beta)| \leq n\mu(\alpha)\mu(\beta)$ by the Cauchy-Schwartz inequality. Applying these two, one obtains

$$\begin{aligned} |B(n+1, n+1)| &\leq \prod_{i=1}^{n} \left(\sum_{j=1}^{n} \tau(\beta_i \alpha_j)^2 \right)^{1/2} \\ &\leq \prod_{i=1}^{n} \sum_{j=1}^{n} |\tau(\beta_i \alpha_j)| \\ &\leq \prod_{i=1}^{n} \sum_{j=1}^{n} n\mu(\beta_i)\mu(\alpha_j) = n^n \prod_{i=1}^{n} \mu(\beta_i) \sum_{j=1}^{n} \mu(\alpha_j). \end{aligned}$$

We proceed to the second step. We need to show $\lambda^* \in D_F\Lambda$. It is equivalent to showing that $|D_F|$ divides $B(n+1, i)$ for every i. Indeed, it is a general property of discriminants. If K is any number field of degree n containing two sets of algebraic integers $\{\alpha_1', \cdots, \alpha_n'\}$ and $\{\beta_1', \cdots, \beta_n'\}$, then the determinant of the $n \times n$ matrix with entries $\tau(\alpha_i'\beta_j')$ is always divisible by D_K. $\square$

We would like to further bound the upper bound in Lemma 2.2. Without loss of generality, it suffices to consider the case $i = n+1$. We split the upper bound into three parts;

$$\frac{n^{n/2}}{|D_F|^{1/2}} \times \frac{n^{n/2}}{|D_F|^{1/2}} \prod_{j=1}^{n} \mu(\beta_j) \times \sum_{k=1}^{n} \mu(\alpha_k).$$

In subsequent sections, we will discuss upper bounds for these factors.

3. Discriminants and Odlyzko Bound

We review the work of Odlyzko on lower bounds for discriminants of number fields. Let F be a number field of degree n. Let D_F be the discriminant of F, and $\delta_F := |D_F|^{1/n}$ be its root discriminant. Our main concern is to bound δ_F when F is totally real.

By a root discriminant bound, we shall mean an inequality of the form

$$\delta_F \geq \eta(n)$$

where $\eta(n)$ is a function of n and r_2. Table 4 contains some of the root discriminant bounds obtained by Odlyzko, where $\eta(n)$ denotes an unconditional bound while $\eta^*(n)$ is conditional on a generalized Riemann hypothesis.

Table 4. Root discriminant bounds, totally real fields

n	2	3	4	5	6	7	8	9
$\eta(n)$	2.223	3.610	5.067	6.523	7.941	9.301	10.596	11.823
$\eta^*(n)$	2.225	3.630	5.124	6.640	8.143	9.611	11.036	12.410

4. Lattice reduction and Orthogonality defect

Let $\Lambda \subset \mathbb{R}^n$ be a lattice of rank n. Let $v(\Lambda)$ be the covolume of Λ. For a basis $\mathbf{x} = (x_1, \cdots, x_n)$ of λ, define the orthogonality defect of it to be

$$od(\mathbf{x}) = \frac{\prod_{i=1}^{n} ||x_i||}{v(\Lambda)},$$

where $|| \cdot ||$ denotes the Euclidean norm. The Hadamard inequality tells us that the orthogonality defect is at least one, and is equal to one if and only if the basis is orthogonal. Thus it provides a way to measure the extent to which a basis fails to be orthogonal. It is natural to consider

$$od(\Lambda) := \inf_{\mathbf{x}} od(\mathbf{x}),$$

where the infimum is taken over all basis of Λ. We will call it as the orthogonality defect of the lattice Λ.

Another important quantity associated to Λ is the length of shortest non-zero vector in it, often denoted by $\lambda_1(\Lambda)$. The Hermite constant γ_n is defined to be

$$\gamma_n = \sup_{\Lambda} \lambda_1(\Lambda),$$

where the supremum is taken over the set of all lattices with unit volume. Clearly, $\gamma_1 = 1$, and other known values of γ_n range over $2 \leq n \leq 8$ and $n = 24$. On the other hand, we have an upper bound

$$\gamma_n \leq \frac{2}{\pi}\Gamma(2+\frac{n}{2})^{2/n}$$

due to Blichfeldt [1]. Better upper bounds for γ_n were established in [2]. and computed for $n \leq 36$, through the relation between lattice packing density and Hermite constants [3, p.20].

TABLE 5. Some known values of powers of Hermite constants

n	2	3	4	5	6	7	8	24
γ_n^n	$\frac{4}{3}$	2	4	8	$\frac{64}{3}$	64	2^8	4^{24}

Various reduction algorithms provide upper bounds for $od(\Lambda)$ in the form

$$od(\Lambda) \leq \theta(n)$$

where $\theta(n)$ only depends on the lattice dimension n. We will recall those arising from the Minkowski reduction and the Korkin-Zolotarev reduction. The Minkowski reduction implies [9]

$$od(\Lambda) \leq \begin{cases} \gamma_n^{n/2} & \text{if } n \leq 4, \\ \gamma_n^{n/2}\left(\frac{5}{4}\right)^{(n-3)(n-4)/4} & \text{if } n > 4. \end{cases}$$

The Korkin-Zolotarev reduction implies [6]

$$od(\Lambda) \leq \gamma_n^{n/2}\prod_{i=1}^{n}\left(\frac{i+3}{4}\right)^{1/2}.$$

Lastly, there is a bound

$$od(\Lambda) \leq \left(\frac{4}{3}\right)^{n(n-1)/4}$$

based on the Hermite reduction [7, p.47].

For $n = 1, 2$, Minkowski and Hermite agree and they are better than LLS. For $3 \leq n \leq 10$, Minkowski yields the best bound. For $11 \leq n \leq 14$, Hermite yields the best bounds. For $n \geq 15$, LLS yields the best bound. Table 6 summarizes the best among these three methods for $2 \leq n \leq 8$, and $n = 12, 16, 24$.

TABLE 6. Orthogonality Defect bounds

n	2	3	4	5	6	7	8	12	16	24
$\theta(n)$	1.155	1.415	2	3.163	6.455	15.63	48.83	1.4×10^4	1.6×10^7	4.4×10^{13}

5. Kronecker's theorem

Let α be an irrational totally real algebraic integer. Kronecker proved that the conjugates of α are contained in the interval $[-2, 2]$ if and only if α can be written as $\alpha = \zeta + \zeta^{-1}$ where ζ is a root of unity.

Proposition 5.1. *Let α is a totally real algebraic integer of degree n such that α^2 is irrational. Choose a positive real number M with $|\sigma(\alpha)| \leq M$ for any embedding of F into $\mathbb{R}$. Also assume that $M^2 - \frac{4}{n} > 4$. Then*

$$\mu(\alpha) < \left(M^2 - \frac{4}{n}\right)^{1/2}$$

Proof. If α is of the form $\alpha = \zeta + \zeta^{-1}$ for a root of unity ζ, then $\mu(\alpha) \leq 2$ trivially and the claimed inequality follows from the assumption $M^2 - \frac{4}{n} > 4$. Otherwise, Kronecker's theorem forces a conjugate of α^2 to be strictly smaller than $M^2 - 4$. This yields the claimed inequality. □

References

[1] H. F. Blichfeldt. The minimum value of quadratic forms, and the closest packing of spheres. *Math. Ann.*, 101(1):605–608, 1929.

[2] Henry Cohn and Noam Elkies. New upper bounds on sphere packings. I. *Ann. of Math. (2)*, 157(2):689–714, 2003.

[3] J. H. Conway and N. J. A. Sloane. *Sphere packings, lattices and groups*, volume 290 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, New York, third edition, 1999. With additional contributions by E. Bannai, R. E. Borcherds, J. Leech, S. P. Norton, A. M. Odlyzko, R. A. Parker, L. Queen and B. B. Venkov.

[4] J. E. Cremona. *Algorithms for modular elliptic curves*. Cambridge University Press, Cambridge, second edition, 1997.

[5] John Cremona. The elliptic curve database for conductors to 130000. In *Algorithmic number theory*, volume 4076 of *Lecture Notes in Comput. Sci.*, pages 11–29. Springer, Berlin, 2006.

[6] J. C. Lagarias, H. W. Lenstra, Jr., and C.-P. Schnorr. Korkin-Zolotarev bases and successive minima of a lattice and its reciprocal lattice. *Combinatorica*, 10(4):333–348, 1990.

[7] Phong Q. Nguyen and Brigitte Valle. *The LLL Algorithm: Survey and Applications*. Springer Publishing Company, Incorporated, 1st edition, 2009.

[8] A. M. Odlyzko. Bounds for discriminants and related estimates for class numbers, regulators and zeros of zeta functions: a survey of recent results. *Sém. Théor. Nombres Bordeaux (2)*, 2(1):119–141, 1990.

[9] B. L. van der Waerden. Die Reduktionstheorie der positiven quadratischen Formen. *Acta Math.*, 96:265–309, 1956.