Harmonic analysis and Hecke operators

Hee Oh*

Mathematics department, Princeton University, Princeton, NJ 08544, USA
e-mail:heeoh@math.princeton.edu

Abstract. We first construct new uniform pointwise bounds for the matrix coefficients of infinite dimensional unitary representations of a reductive algebraic group over a local field k with semisimple k-rank at least 2 [21]. We explain how this information on local harmonic analysis yields norm estimates for (global) Hecke operators on $L^2(\Gamma\backslash G)$ for a connected almost simple simply connected $\mathbb{Q}$-group G and its congruence subgroup Γ [5]. With the tool of Hecke operators, we settle a question of Linnik raised in the early sixties on the distribution of integer points of Diophantine type varieties when the varieties are homogeneous spaces of a reductive algebraic group over $\mathbb{Q}$ [10]. Lastly we discuss how to obtain evenly distributed sequences on the spheres S^n $(n \geq 4)$ [22], generalizing the work of Lubotzky, Phillips and Sarnak on S^2 and S^3 ([18], [19]).

1 Uniform pointwise bounds $\xi_{\mathcal{S}}$ for matrix coefficients

The aim of this section is to explain the construction of new uniform pointwise bounds for the matrix coefficients of infinite dimensional unitary representations of a reductive algebraic group over a local field [21]. Let k be a local field (char $k \neq 2$), that is, $k = \mathbb{R}$, $\mathbb{C}$, a finite extension of $\mathbb{Q}_p$, or a finite extension of $\mathbb{F}_q((t))$ $(q \neq 2)$. Let G be the group of k-rational points of a connected reductive algebraic group over k. Two main ingredients in the construction of the uniform pointwise bounds $\xi_{\mathcal{S}}$ are the Harish-Chandra function $\Xi_{PGL_2(k)}$ of $PGL_2(k)$ and the strongly orthogonal systems $\mathcal{S}$ of the root system of G. Roughly, there exists a (canonical for the split case) way of attaching to each root a closed subgroup of G locally isomorphic to $PGL_2(k)$. We will then define for each strongly orthogonal system $\mathcal{S}$ a spherical function $\xi_{\mathcal{S}}$ on G, which is essentially the product of the Harish-Chandra functions $\Xi_{PGL_2(k)}$ over all roots belonging to $\mathcal{S}$. Our notation $\xi_{\mathcal{S}}$ is (hopefully) meant to stand for its origin in Ξ (the little Ξ being ξ) over various strongly orthogonal systems $\mathcal{S}$.

Recall the Cartan decomposition of G: $G = KA^+\Omega K$ where K is a good maximal compact subgroup of G, A^+ a closed positive Weyl chamber contained in a maximal k-split torus A of G and Ω a finite subset of the centralizer of A. That is, for each $g \in G$, there exist unique elements $a \in A^+$ and $d \in \Omega$ such that $g \in KadK$. We remark that if k is archimedean or if G is k-split, $\Omega = \{e\}$. A virtue of the Cartan decomposition which will be used

* Partially sponsored by NSF grant DMS 0070544

here is that any bi-K-invariant function on G is completely determined by its restriction to $A^+\Omega$.

Definition of $\Xi_{PGL_2(k)}$ [11]: Let B be the subgroup of $PGL_2(k)$ consisting of the upper triangular matrices. It is well known that the unitarily induced representation $\mathrm{Ind}_B^G(1)$ from the trivial representation 1 on B to $PGL_2(k)$ is irreducible and has a unique (up to scalar) K-invariant unit vector, say v. The Harish-Chandra function $\Xi_{PGL_2(k)}$ is defined by

$$\Xi_{PGL_2(k)}(g) = \langle \mathrm{Ind}_B^G(1)(g)v, v\rangle \quad \text{for any } g \in PGL_2(k).$$

Denote by Φ the set of non-multipliable roots of A in G, and by Φ^+ the set of positive roots in Φ.

Definition: Strongly orthogonal system A subset $\mathcal{S}$ of Φ^+ is called a *strongly orthogonal system* of Φ if neither of $\alpha \pm \beta$ is a root for any two distinct elements α and β of $\mathcal{S}$.

Each root α will be understood as a function on G by setting

$$\alpha(g) := \alpha(a) \quad \text{for } g = k_1 a d k_2 \in KA^+\Omega K.$$

Definition of $\xi_{\mathcal{S}}$: For each strongly orthogonal system $\mathcal{S} \subset \Phi^+$, we set

$$\xi_{\mathcal{S}}(g) = \prod_{\alpha\in\mathcal{S}} \Xi_{PGL_2(k)} \begin{pmatrix} \alpha(g) & 0 \\ 0 & 1 \end{pmatrix} \text{ for each } g \in G. \tag{1}$$

Let G^+ denote the subgroup of G generated by all unipotent k-split subgroups of G and Z denote the center of G. We now state the main theorem:

Theorem 1.1. *Let $k \neq \mathbb{C}$ and k-s.s.rank $(G) \geq 2$ and G/Z almost k-simple. Let $\mathcal{S}$ be a strongly orthogonal system of Φ. Then for any unitary representation ρ of G without a non-zero G^+-invariant vector and its K-finite unit vectors v and w,*

$$|\langle \rho(g)v, w\rangle| \leq \left([K : K\cap dKd^{-1}]\cdot \dim\langle Kv\rangle \dim\langle Kw\rangle\right)^{1/2} \xi_{\mathcal{S}}(g)$$

for any $g = k_1 a d k_2 \in KA^+\Omega K = G$.

Remark:

- The same inequality holds for $k = \mathbb{C}$, provided that in the case when $G/Z(G) \approx Sp_{2n}(\mathbb{C})$, we replace $\Xi_{PGL_2(k)}$ by ${\Xi_{PGL_2(k)}}^{1/2}$ in the definition of $\xi_{\mathcal{S}}$ whenever α is a long root.
- We note that any irreducible unitary representation ρ of G has a non-zero G^+-invariant vector if and only if ρ is of finite dimension. Hence the above theorem works for any infinite dimensional irreducible unitary representations without an assumption on not possessing G^+-invariant vectors.

The following properties of $\xi_{\mathcal{S}}$ can be directly deduced from those of $\Xi_{PGL_2(k)}$:

Properties of $\xi_{\mathcal{S}}$:

- $0 < \xi_{\mathcal{S}}(g) \leq 1$ for any $g \in G$.
- For any $\epsilon > 0$, there are constants $d_1 > 0$ and $d_2(\epsilon) > 0$ such that

$$d_1 \left(\prod_{\alpha \in \mathcal{S}} |\alpha(g)| \right)^{-1/2} \leq \xi_{\mathcal{S}}(g) \leq d_2(\epsilon) \left(\prod_{\alpha \in \mathcal{S}} |\alpha(g)| \right)^{-1/2+\epsilon} \quad \text{for any } g \in G$$

  where $|\cdot|$ denotes the standard norm on k in the sense of ([27], Ch 1).
- For $g \in G$, $\xi_{\mathcal{S}}(g) = 1$ if and only if $\alpha(g) = 1$ for all $\alpha \in \mathcal{S}$.

The second inequality implies that $\xi_{\mathcal{S}}$ decays fastest when $\mathcal{S}$ is maximal in the following sense:

Definition: A strongly orthogonal system $\mathcal{S}$ is called *maximal* if the coefficient of each simple root in the formal sum $\sum_{\alpha \in \mathcal{S}} \log \alpha$ is not less than the one in $\sum_{\alpha \in \mathcal{O}} \log \alpha$ for any strongly orthogonal system $\mathcal{O}$ of Φ.

A maximal strongly orthogonal system has been explicitly given for each reduced irreducible root system in [20].

In general there exist more than one maximal strongly orthogonal systems in Φ. However the following product is independent of the choice of $\mathcal{Q}$, in fact, an invariant of the root system Φ:

$$\eta_G := \prod_{\alpha \in \mathcal{Q}} \alpha$$

for a maximal strongly orthogonal system $\mathcal{Q}$ in Φ.

The following is then immediate from Theorem 1.1:

Corollary 1.1. *Under the same assumption as in Theorem 1.1, for any $\epsilon > 0$, there exists a constant C (depending only on ϵ and G) such that*

$$|\langle \rho(g)v, w \rangle| \leq C \cdot (\dim\langle Kv \rangle \dim\langle Kw \rangle)^{1/2} \, |\eta_G(g)|^{-1/2+\epsilon}$$

for any $g \in G$, ρ, v and w as in Theorem 1.1.

Example 1.1. Let $G = SL_n(k)$. For $a = \mathrm{diag}(a_1, \cdots, a_n) \in A^+$ (here a_i's are in decreasing order with respect to the norm on k), let $\gamma_i(a) = \frac{a_i}{a_{n+1-i}}$ for each $1 \leq i \leq \llcorner \frac{n}{2} \lrcorner$. Then $\mathcal{Q} = \{\gamma_i \mid 1 \leq i \leq \llcorner \frac{n}{2} \lrcorner\}$ is a maximal strongly orthogonal system.

Hence

$$|\eta_G(a)| = \prod_{i=1}^{\llcorner n/2 \lrcorner} \left(\frac{|a_i|}{|a_{n+1-i}|} \right)^{-1/2}.$$

A key notion in the proof of Theorem 1.1 is the following:

Definition: Let L be the group of the k-rational points of a connected reductive linear algebraic group over k with a good maximal compact subgroup M. A unitary representation ρ of L is said to be *tempered* if for any M-finite unit vectors v and w,

$$|\langle \rho(g)v, w\rangle| \leq (\dim\langle Mv\rangle \dim\langle Mw\rangle)^{1/2}\, \Xi_L(g) \text{ for any } g \in L$$

where Ξ_L denotes the Harish-Chandra function of L.

A unitary representation ρ being tempered is equivalent to the condition that ρ is weakly contained in the regular representation of L

The scheme of the proof of Theorem 1.1 is then roughly as follows: to each root $\alpha \in \mathcal{S}$, we attach the group H_α, locally isomorphic to the algebraic subgroup generated by the one-dimensional root subgroups $U_{\pm\alpha}$. The first step is to show that the restriction of ρ to H_α is *tempered* for any root $\alpha \in \Phi$. This is proved based on Mackey's theorem on the unitary representation of the semi-direct products and the theory of oscillator representations.

Since $\mathcal{S}$ is a strongly orthogonal system, H_α and H_β commute with each other for any $\alpha, \beta \in \mathcal{S}$. In the spirit of Howe's strategy, we then show that the restriction $\rho|_{H_{\mathcal{S}}}$ is tempered where $H_{\mathcal{S}}$ is the subgroup generated by H_α, $\alpha \in \mathcal{S}$. Denote by $L_{\mathcal{S}}$ the subgroup generated by $H_{\mathcal{S}}$ and the maximal k-split torus A. Then $H_{\mathcal{S}}$ has a finite index in $L_{\mathcal{S}}$, up to modulo their centers. We then show that the temperedness of $\rho|_{H_{\mathcal{S}}}$ transfers to the temperedness of $\rho|_{L_{\mathcal{S}}}$ using the work of Cowling-Haggerup-Howe [6]. Up to a constant term, this implies Theorem 1.1.

A weaker bound in Theorem 1.1 in a form of $\Xi_G^{1/m}$ (here Ξ_G denotes the Harish-Chandra function of G) for some positive integer m can be deduced from the work of Cowling [7], Howe [12], and Cowling-Haggerup-Howe [6]. An optimal bound for m has not been obtained in general (cf. [14], [15], [20], [21]). Even in the case when the optimal bound m is known, for instance, $G = SL_n(\mathbb{R})$, the new bound presented in Theorem 1.1 is much sharper in every regular direction.

Moreover when $\mathcal{Q}$ is maximal, the uniform pointwise bound $\xi_{\mathcal{Q}}$ turns out to be optimal in two important class of groups: $SL_n(k)\,(n \geq 3)$ and $Sp_{2n}(k)\,(n \geq 2)$. In the following theorem, the group $Sp_{2n}(k)$ is defined by the bi-linear form $\begin{pmatrix} 0 & \bar{I}_n \\ -\bar{I}_n & 0 \end{pmatrix}$ where $\bar{I}_n$ denotes the skew diagonal $n \times n$-identity matrix.

Theorem 1.2. *Let G be either $SL_n(k)\,(n \geq 3)$ or $Sp_{2n}(k)$ $(n \geq 2,\, k \neq \mathbb{C})$. Let P be the maximal parabolic subgroup of G which stabilizes ke_1 and v a (unique) K-invariant unit vector in $\mathrm{Ind}_P^G(1)$. Then for any $\epsilon > 0$, there exist positive constants C_1 and $C_2 = C_2(\epsilon)$ such that*

$$C_1 \cdot |\eta_G(g)|^{-1/2} \leq \langle \mathrm{Ind}_P^G(1)(g)v, v\rangle \leq C_2 \cdot |\eta_G(g)|^{-1/2+\epsilon}$$

for any $g \in G$.

For $Sp_{2n}(\mathbb{C})$, the optimalness of ξ_Q is achieved by considering the even component of the oscillator representation of $Sp_{2n}(\mathbb{C})$ [21].

2 Equidistribution of Hecke points

The notion of the Hecke operator is classical and has proven to be very useful in the theory of automorphic forms as well as in counting the integer points of some Diophantine type varieties. In this section, we explain how one uses the uniform bounds on the spherical unitary dual of $\mathcal{G}(\mathbb{Q}_p)$'s for a semisimple algebraic $\mathbb{Q}$-group $\mathcal{G}$ explained in section 1 to obtain norm estimates on Hecke operators on $L^2(\Gamma\backslash\mathcal{G}(\mathbb{R}))$ for a congruence subgroup Γ. This is joint work with L. Clozel and E. Ullmo [5].

Let $\mathcal{G}$ be a connected almost simple simply connected algebraic group over $\mathbb{Q}$ and $\Gamma \subset \mathcal{G}(\mathbb{Q})$ a congruence subgroup. Set $G = \mathcal{G}(\mathbb{R})$. We denote by μ_G the normalized Haar measure on $\Gamma\backslash G$. For simplicity, we assume that $\mathrm{rank}_{\mathbb{Q}}(G) \geq 1$, referring to [5] for a more general situation.

Definition: Hecke operator T_a Let $a \in G(\mathbb{Q})$. We denote by $\deg(a)$ the cardinality of $\Gamma\backslash\Gamma a\Gamma$, or equivalently $[\Gamma : \Gamma \cap a^{-1}\Gamma a]$. The Hecke operator T_a is defined as follows: for any $f \in L^2(\Gamma\backslash G)$ and $g \in \Gamma\backslash G$,

$$T_a(f)(g) = \frac{1}{\deg(a)} \sum_{x \in \Gamma\backslash\Gamma a\Gamma} f(xg).$$

To state our theorem, we first set up some notation. For each prime p, let A_p be a maximal $\mathbb{Q}_p$-split torus of $\mathcal{G}$ and Φ_p the set of non-multipliable roots of the root system $\Phi(\mathcal{G}, A_p)$. Set

$$R_1 = \{p \mid \mathrm{rank}_{\mathbb{Q}_p}\mathcal{G} = 1\};$$

$$R_2 = \{p \mid \mathrm{rank}_{\mathbb{Q}_p}\mathcal{G} \geq 2\}.$$

We denote by $T_a^0 : L_0^2(\Gamma\backslash G) \to L_0^2(\Gamma\backslash G)$ the restriction of T_a to $L_0^2(\Gamma\backslash G)$ where

$$L_0^2(\Gamma\backslash G) = \{f \in L^2(\Gamma\backslash G) \mid \int_{\Gamma\backslash G} f d\mu_G = 0\}.$$

The notation $\|T_a^0\|$ denotes the usual operator norm.

Recalling the definition of $\xi_{\mathcal{S}_p}$ from section 1, we now state the following norm estimates for T_a^0:

Theorem 2.1. *There exists a constant* C *(depending only on* $\mathcal{G}$ *and* Γ*) such that for any* $a \in \mathcal{G}(\mathbb{Q})$

$$\|T_a^0\| \leq C \left(\prod_{p \in R_1} \xi_{\mathcal{S}_p}^{1/2}(a)\right)\left(\prod_{p \in R_2} \xi_{\mathcal{S}_p}(a)\right)$$

where $\mathcal{S}_p$ is a (maximal) strongly orthogonal system of Φ_p for each p.

In order to explain the proof of Theorem 2.1, let $\mathcal{G}(\mathbb{A})$ denote the adele group associated to $\mathcal{G}$ and $\mathcal{G}(\mathbb{A}_f)$ the group of finite adeles. Let $U_f = \prod_{p:prime} U_p$ be an open compact subgroup of $\mathcal{G}(\mathbb{A}_f)$ such that $\Gamma = G(\mathbb{Q}) \cap U_f$.

By the strong approximation, we have $\mathcal{G}(\mathbb{Q})\, GU_f = \mathcal{G}(\mathbb{A})$; hence

$$\Gamma\backslash G = \mathcal{G}(\mathbb{Q})\backslash\mathcal{G}(\mathbb{A})/U_f.$$

Moreover there exists a natural isometry between

$$L^2(\mathcal{G}(\mathbb{Q})\backslash\mathcal{G}(\mathbb{A})/U_f)\,(\simeq L^2(\mathcal{G}(\mathbb{Q})\backslash\mathcal{G}(\mathbb{A}))^{U_f})$$

and $L^2(\Gamma\backslash G)$. Via this isometry, the Hecke operator T_a corresponds to the product, over all primes p, of the local Hecke operators $T_{a(p)}$, which is precisely (after the normalization) the convolution operator by the characteristic function on $U_p a U_p$: for $f \in L^2(\mathcal{G}(\mathbb{Q})\backslash\mathcal{G}(\mathbb{A})/U_f)$ and $g \in \mathcal{G}(\mathbb{Q})\backslash\mathcal{G}(\mathbb{A})/U_f$

$$T_{a(p)}(f)(g) = \frac{1}{|U_p\backslash U_p a U_p|} \sum_{y \in U_p\backslash U_p a U_p} f(gy^{-1})$$

and

$$T_a = \prod_p T_{a(p)}.$$

Now if v and w are U_p-invariant vectors of an irreducible $\mathcal{G}(\mathbb{Q}_p)$-component, say, ρ_p, of a representation weakly contained in $L^2_0(\mathcal{G}(\mathbb{Q})\backslash\mathcal{G}(\mathbb{A}))$, then

$$\langle T_{a(p)} v, w\rangle = \langle \rho_p(a) v, w\rangle.$$

Furthermore, the Langlands spectral decomposition of $L^2_0(\mathcal{G}(\mathbb{Q})\backslash\mathcal{G}(\mathbb{A}))$ says that each ρ_p can be assumed non-trivial (cf. [1]). Since $\mathcal{G}(\mathbb{Q}_p)$ is non-compact, almost simple and simply connected, any non-trivial irreducible representation is indeed infinite-dimensional.

Hence for the prime p such that $\mathbb{Q}_p$-rank of $\mathcal{G}(\mathbb{Q}_p)$ is at least 2, we can use the uniform pointwise bound $\xi_{\mathcal{S}_p}$ for the matrix coefficients of irreducible infinite dimensional unitary representations of $\mathcal{G}(\mathbb{Q}_p)$'s presented in section 1 to obtain norm estimates of $T_{a(p)}$. As for the prime p such that the $\mathbb{Q}_p$-rank of $\mathcal{G}(\mathbb{Q}_p)$ is 1, such a uniform pointwise bound does not exist because $\mathcal{G}(\mathbb{Q}_p)$ does not have Kazhdan property (T). However the method developed by Burger and Sarnak in [2] (see [4] for its p-adic version) enables us to lift the Gelbart-Jacquet bound [9] toward the Ramanujan conjecture for SL_2 to $\mathcal{G}$, in order to obtain the bound $\xi^{1/2}_{\mathcal{S}_p}$ on the part of the unitary dual of $\mathcal{G}(\mathbb{Q}_p)$ coming from $L^2_0(\mathcal{G}(\mathbb{Q})\backslash\mathcal{G}(\mathbb{A})/U_f)$.

Remark:

- If the Ramanujan conjecture for SL_2 is assumed, then we can replace $\xi^{1/2}_{\mathcal{S}_p}$ by $\xi_{\mathcal{S}_p}$ in Theorem 2.1

- The Hecke operator norm bounds obtained in the above theorem are optimal for $SL_n\,(n \geq 3)$ and $Sp_{2n}\,(n \geq 2)$ when maximal strongly orthogonal systems $\mathcal{S}_p$ are used. In view of Theorem 1.2, this follows from the observation that in those two cases, there is contribution on the boundary of the spherical unitary dual of each $\mathcal{G}(\mathbb{Q}_p)$ from the spectrum of $L^2(G(\mathbb{Z})\backslash G)$.

Example 2.1. Let $G = SL_n(\mathbb{R})$ for $n \geq 3$ and $\Gamma = SL_n(\mathbb{Z})$. Let

$$a = \mathrm{diag}(a_1, \cdots, a_n) \in G(\mathbb{Q})$$

with $a_i \geq a_{i+1} > 0$ for each $1 \leq i \leq n-1$. Using the maximal strongly orthogonal system $\mathcal{Q}$ in Example 1 at each prime p, we obtain from Theorem 2.1 for any $\epsilon > 0$, there exists a constant C (depending only on ϵ) such that

$$\|T_a^0\| \leq C \prod_{i=1}^{\llcorner n/2 \lrcorner} \left(\frac{a_i}{a_{n+1-i}} \right)^{-1/2+\epsilon}.$$

We can easily deduce the following from Theorem 2.1. For $x \in \Gamma\backslash G$, set $T_a x = \{[\Gamma a \Gamma x] \in \Gamma\backslash G\}$.

Corollary 2.1. *Let $\{a_n \in \mathcal{G}(\mathbb{Q}) \mid n \in \mathbb{N}\}$ be a sequence with $deg(a_n)$ tending to infinity. Then for any $x \in \Gamma\backslash G$, the sets $T_{a_n}x$ are equidistributed with respect to $d\mu_G$, in the sense that*

$$\lim_{n\to\infty} T_{a_n} f(x) = \int_{\Gamma\backslash G} f(g)\, d\mu_G(g)$$

for any continuous function f on $\Gamma\backslash G$ with compact support.

It is observed in [2] that when a_n tends to an element which is not a commensurator of Γ, one can also deduce the above corollary from Ratner's theorem on orbit closures of unipotent flows. However the rate of convergence as in Theorem 2.1 would not be obtained.

A Sobolev type argument then enables us to transfer the L^2-convergence rate obtained in Theorem 2.1 to a pointwise convergence rate under suitable differentiability assumption on f. For instance, we have the following:

Theorem 2.2. *For any smooth function f on $\Gamma\backslash G$ with a compact support, there exists a constant C_f depending on f such that for any $x \in \Gamma\backslash G$ and for any $a \in \mathcal{G}(\mathbb{Q})$,*

$$\left| T_a f(x) - \int_{\Gamma\backslash G} f(g)\, d\mu_G(g) \right| \leq C_f \left(\prod_{p\in R_1} \xi_{\mathcal{S}_p}^{1/2}(a) \right) \left(\prod_{p \in R_2} \xi_{\mathcal{S}_p}(a) \right)$$

where $\mathcal{S}_p$ is a (maximal) strongly orthogonal system of Φ_p for each $p \in R_1 \cup R_2$.

A special case of Theorem 2.1 for $G = SL_n$ was first announced by Sarnak in his address in the 1991 international congress of mathematics in Kyoto [23]. Chiu afterwards obtained some analogues of Theorem 2.1 for SL_2 and SL_3 in [3] for special types of Hecke operators. Clozel and Ullmo, in their joint work [4], have also obtained some special cases of the above results for GL_n and GSp_{2n}.

3 Equidistribution of Integer points on a family of homogeneous varieties

Let f be a homogeneous polynomial of degree d in n variables with integer coefficients. For any integer m, consider the affine subvariety of $\mathbb{R}^n$ defined by

$$V_m = \{x \in \mathbb{R}^n : f(x) = m\}.$$

This variety is defined over $\mathbb{Z}$. It is a classical problem in number theory to understand the distribution of the set $V_m(\mathbb{Z})$ of integer points in V_m.

Here is a problem raised by Linnik in the early sixties [16]:

Let $\pi : V_m \to V_1$ be the radial projection. What is the distribution of $\pi(V_m(\mathbb{Z}))$ on V_1 as $m \to \infty$? In particular are these points equidistributed?

In joint work with W. T. Gan [10], we settle the above Linnik's question when the varieties V_m are homogeneous varieties of a linear semisimple algebraic group.

Let $\mathcal{G}$ be a linear reductive $\mathbb{Q}$-split algebraic group with absolutely almost simple derived group and connected one dimensional center. Set $G = \mathcal{G}(\mathbb{R})^0$ and $G_0 = [G, G]^0$. Suppose that G acts (from the right) on $\mathbb{R}^n$ by a representation ρ defined over $\mathbb{Z}$ with a non-trivial central character and that the polynomial f is a semi-invariant of G. Then G_0 acts on each V_m. Let $v_0 \in V_1(\mathbb{Z})$ and assume that the identity component of the stabilizer of v_0 in G_0 does not possess any non-trivial $\mathbb{Q}$-rational character.

The following generalizes the equidistribution statement obtained by Linnik and Skubenko ([16], [17]) for the case when $f = det$ and $G = GL_n$.

Theorem 3.1. *Fix a compact subset $\Omega \subset v_0 G_0$ and for any small $\epsilon > 0$, consider the standard division of $\mathbb{R}^n$ into ϵ-cubes. Then there exists a constant $m_{\Omega,\epsilon}$ such that for any positive integer $m > m_{\Omega,\epsilon}$, any ϵ-cube intersecting the interior of Ω contains at least one point in the radial projection of $V_{m^r}(\mathbb{Z})$ into V_1. Here r is an explicit positive integer which depends only on G and ρ.*

Remark

- We remark that there are fundamental obstructions to having Theorem 3.1 for any sequence m tending to infinity; the restriction to a subsequence of an r-th power of m as in Theorem 3.1 is necessary. In fact it follows from the work of Shintani [26] that when f is the discriminant of a binary cubic form and $\mathcal{G} = GL_2$, one can find a compact subset Ω with non-empty interior in v_0G_0 and a sequence $m_i \to \infty$ such that the cardinalities of the sets consisting of the points in $V_{m_i}(\mathbb{Z})$ which are radially projected into Ω are uniformly bounded over all m_i's (cf. [10], Example 3).

- If V_1 is the union of finitely many G_0-orbits each of which possessing an integer point, then one can replace v_0G_0 by the whole variety V_1 in Theorem 3.1. For example, in the case of a regular prehomogeneous vector space with a unique semi-invariant, each V_m $(m \neq 0)$ is the union of finitely many G_0-orbits. Therefore the classification of $\mathbb{Q}$-split irreducible regular prehomogeneous vector spaces given by Sato and Kimura in [24] provides explicit examples to which Theorem 3.1 applies, with v_0G_0 replaced by V_1, as long as each G_0-orbit contains an integer point.
- In [10], we discuss Linnik's question in a slightly more general situation where the varieties in question are of type

$$V_{m_1,\cdots,m_k} = \{x \in \mathbb{R}^n \mid f_i(x) = m_i \text{ for each } 1 \leq i \leq k\}$$

for a system of semi-invariants $f_1, \cdots f_k$.

Corollary 3.1. *Given any open set $U \subset v_0G_0$, there exists a constant m_U such that U contains a point in the radial projection of $V_{m^r}(\mathbb{Z})$ for any positive integer $m > m_U$.*

In particular, the radial projections of $V_m(\mathbb{Z})$ onto V_1 becomes dense as $m \to \infty$.

We set $\Gamma = G(\mathbb{Z})$. Let Z denote the connected component of the center of G and let H be the stabilizer of v_0 in G. By the assumption, $H \subset G_0$ and $H \cap \Gamma$ is a lattice in H. We let μ_G and μ_H the normalized Haar measures on $Z\Gamma\backslash G$ and $(H \cap \Gamma)\backslash H$ respectively. Then the measures μ_G and μ_H induce a unique G-invariant measure on $ZH\backslash G \simeq H\backslash G_0$, which we will denote by μ. For a measurable set $\Omega \subset ZH\backslash G$, we will write $\mathrm{vol}(\Omega)$ for $\mu(\Omega)$.

The main idea in the proof of Theorem 3.1 is based in the crucial observation made by Sarnak [23] on the relation of Hecke operators with this type of equidistribution question.

For a simply connected group $\mathcal{G}$, we obtained norm estimates of the Hecke operator T_a defined in section 2 by reducing the global problem to local harmonic analysis on $\mathcal{G}(\mathbb{Q}_p)$'s. When $\mathcal{G}$ is not simply connected, we give a slightly modified definition of a Hecke operator below, designed so that the passage between local and global Hecke operators continues to hold.

Let U_f be an open compact subgroup of $\mathcal{G}(\mathbb{A}_f)$ such that $\Gamma = G(\mathbb{Q}) \cap U_f$. For each $a \in G(\mathbb{Q})$, we consider the double Γ-invariant subset

$$G[a] = \{g \in G(\mathbb{Q}) : g \in U_f a U_f\}.$$

If G is simply connected, then $G[a]$ is simply equal to $\Gamma a \Gamma$.

We now set $\deg(a) = |\Gamma\backslash G[a]|$. A modified definition of a Hecke operator T_a is given as follows: T_a acts on on the space of functions on $Z\Gamma\backslash G$ by

$$T_a(f)(g) = \frac{1}{\deg(a)} \sum_{\gamma\in\Gamma\backslash G[a]} f(\gamma g).$$

For a compact subset $\Omega \subset ZH\backslash G$, define a function on $Z\Gamma\backslash G$ by

$$F_\Omega(g) = \sum_{\gamma\in(\Gamma\cap H)\backslash H} \chi_\Omega(\gamma g)$$

where χ_Ω is a characteristic function of Ω.

Observe that

$$T_a(F_\Omega)(1) = \frac{1}{|\Gamma\backslash G[a]|} \sum_{\gamma\in\Gamma\backslash G[a]} |\Omega \cap v_0\Gamma\gamma|$$

and $\|F_\Omega\|_1 = \mathrm{vol}(\Omega)$.

In the following theorem, we keep the notation A_p, Φ_p and $\xi_{\mathcal{S}_p}(g)$ for a maximal strongly orthogonal system $\mathcal{S}_p$ of Φ_p from section 1. Define the real-valued function ξ on $G(\mathbb{Q})$ by

$$\xi(g) = \prod_{p\in R_1} \xi_{\mathcal{S}_p}(g)^{\frac{1}{2}} \cdot \prod_{p\in R_2} \xi_{\mathcal{S}_p}(g)$$

where

$$R_1 = \{\text{primes } p : \mathbb{Q}_p\text{-rank of } \mathcal{Z}\backslash\mathcal{G} = 1\};$$
$$R_2 = \{\text{primes } p : \mathbb{Q}_p\text{-rank of } \mathcal{Z}\backslash\mathcal{G} \geq 2\}.$$

Fixing a right invariant metric on G, we denote by U_ϵ the ϵ-neighborhood of the identity in G for any $\epsilon > 0$.

Definition: A compact subset $\Omega \subset ZH\backslash G$ is *nice* if for all sufficiently small $\epsilon > 0$ (depending on Ω),

$$\mathrm{vol}(\partial\Omega \cdot U_\epsilon) < C_\Omega \cdot \epsilon$$

for some positive constant C_Ω depending on Ω. Here $\partial\Omega$ denotes the boundary of Ω.

The following can be interpreted as an equidistribution statement of (the projections of) the Hecke orbits $G[a]$ in the homogeneous variety $ZH\backslash G$ as $\deg(a) \to \infty$:

Theorem 3.2. *Let Ω be a nice compact subset of $ZH\backslash G$. There exists a constant C_Ω (depending only on Ω) such that for any $a \in G(\mathbb{Q})$, we have*

$$|T_a F_\Omega(1) - \mathrm{vol}(\Omega)| \leq C_\Omega \cdot \xi(a^{-1})^{\frac{\delta}{d+2}},$$

where $0 < \delta \leq 1$ is the explicitly computable exponent and $d = dim(Z\backslash G)$.

Theorem 3.2 does not follow directly from the results in section 2, since we do not know whether F_Ω has compact support or even belong to $L^2(Z\Gamma\backslash G)$ in general.

To relate Theorem 3.2 to Theorem 3.1, we introduce for each positive integer m a subset $G[m]$ of $G(\mathbb{Q})$:

$$G[m] = \{g \in G(\mathbb{Q}) : \rho(g) \in M_{n\times n}(\mathbb{Z}) \text{ and } \chi_0(g) = m\},$$

where χ_0 denotes the basis element of the character group of G with a positive pairing with the central character of ρ.

For some integer m, $G[m]$ might be empty; when it is not empty, it is a finite union of the Hecke orbit $G[a]$'s for $a \in G(\mathbb{Q})$ with $\chi_0(a) = m$. We make an explicit choice of the exponent r_0 (depending only on G and ρ) to guarantee that $G[m^{r_0}]$ is non-empty for any positive integer m. If the action of G on f is given by $f(vg) = \chi_0(g)^{r_1} f(v)$, then r in the Theorem 3.1 is equal to $r_0 \cdot r_1$ and hence $v_0 G[m^{r_0}] \subset V_{m^r}(\mathbb{Z})$. Hence the subsets $G[m^{r_0}]$ allow us to produce many integer points in V_{m^r} starting from $v_0 \in V_1(\mathbb{Z})$. In fact, the following counting statement implies that as $m \to \infty$, the subsets $v_0 G[m^{r_0}]$ are equidistributed on the orbit $v_0 G_0 \subset V_1$ when radially projected.

Theorem 3.3. *Fix a nice compact subset Ω of $v_0 G_0$ and $0 < \epsilon \ll 1$. Then there exists a constant $C_{\Omega,\epsilon}$ such that for any positive integer m,*

$$\left| \frac{\sum_{y \in \Gamma\backslash G[m^{r_0}]} |\mathbb{R}_+ \Omega \cap v_0 \Gamma y|}{|\Gamma\backslash G[m^{r_0}]|} - \mathrm{vol}(\Omega) \right| \le C_{\Omega,\epsilon} \cdot m^{-r_0\kappa + \epsilon}$$

where $\mathbb{R}_+\Omega = \{x \in \mathbb{R}^n : tx \in \Omega \text{ for some } t > 0\}$. Here r_0 is an explicit positive integer depending only on G and ρ and the exponent $\kappa > 0$ is independent of Ω and is explicitly computable.

Since every point in $v_0 G_0$ has a basis of neighborhoods which are nice compact subsets, the above theorem implies Theorem 3.1. Note that it is essential to have estimates for the rate of convergence in Theorem 3.3 in order to deduce Theorem 3.1.

In order to deduce Theorem 3.3 from Theorem 3.2, we need to estimate the number of disjoint Hecke orbits $G[a]$ in $G[m]$ as well as the number of single Γ-orbits in each $G[a]$.

We conclude this section by discussing the classical example treated by Linnik and Skubenko in [17] and revisited by Sarnak in [23].

Example 3.1. Consider the action of GL_n $(n \ge 3)$ on the space M_n of $n \times n$ matrices by right multiplication. The determinant map is a homogeneous polynomial on M_n of degree n. Then

$$V_m(\mathbb{Z}) = \{A \in M_n(\mathbb{Z}) : det(A) = m\} = G[m].$$

Set $\|A\| = (\sum_{i,j} A_{ij}^2)^{\frac{1}{2}}$. Then, taking v_0 to be the identity matrix I_n, Theorem 3.3 implies that for any given positive numbers R and $0 < \epsilon \ll 1$,

$$|\{A \in M_n(\mathbb{Z}) : det(A) = m, \ \|A\| \le m^{\frac{1}{n}} R\}| = c_{n,R} b_{m,n} (1 + O(m^{-\frac{1}{2n^2+2}+\epsilon}))$$

as $m \to \infty$. Here $c_{n,R}$ is the volume of the set $\{A \in SL_n(\mathbb{R}) : \|A\| \le R\}$ with respect to the Haar measure of $SL_n(\mathbb{R})$ giving $SL_n(\mathbb{Z})\backslash SL_n(\mathbb{R})$ volume 1 and if $m = \prod_i p_i^{k_i}$ where p_i's are primes, then

$$b_{m,n} = \prod_i \frac{(p_i^{k_i+1} - 1) \cdots (p_i^{k_i+n-1} - 1)}{(p_i - 1) \cdots (p_i^{n-1} - 1)}.$$

In fact, if $g_m = diag(m, 1, ..., 1)$, then

$$b_{m,n} = [SL_n(\mathbb{Z}) : SL_n(\mathbb{Z}) \cap g_m SL_n(\mathbb{Z}) g_m^{-1}]$$

for each positive integer m. For $n = 2$, the same asymptotic holds except that the error term should be replaced by $m^{-\frac{1}{20}+\epsilon}$.

The above example is deceptively simple and exceptional because of the following two reasons. Firstly, $r_0 = r = 1$ and every point in $V_m(\mathbb{Z})$ is a Hecke point obtained from v_0, i.e. $V_m(\mathbb{Z}) = v_0 G[m]$. In the general case, there is of course no reason to expect that every point in $V_{m^r}(\mathbb{Z})$ is a Hecke point; in fact there will be primitive or new points in $V_{m^r}(\mathbb{Z})$ which do not arise from any lower stratum in this way.

Secondly, the stabilizer of v_0 in GL_n is trivial. This ensures that the sets $v_0 SL_n(\mathbb{Z}) y$ appearing in Theorem 3.3 are disjoint as y ranges over $SL_n(\mathbb{Z})\backslash G[m]$. When the stabilizer of v_0 is non-trivial, this will not be the case and Theorem 3.3 should be interpreted as an equidistribution theorem for Hecke points counted *with multiplicities*.

4 Distributing points on the spheres S^n $(n \ge 4)$

Lastly we discuss how one uses the information on local harmonic anaylsis described in section 1 to obtain uniformly distributed sequences on the spheres S^n $(n \ge 4)$ [22], generalizing the work of Lubotzky, Phillips and Sarnak ([18], [19]) on S^2 and S^3.

Definition: For a finite subset S of $SO(n + 1)$, we define a Hecke operator T_S on $L^2(S^n)$ by

$$T_S f(x) = \frac{1}{|S|} \sum_{\gamma \in S} f(\gamma^{-1} x), \quad \text{for any } f \in L^2(S^n).$$

Denote by λ_S the operator norm of the restriction $T_S : L_0^2(S^n) \to L_0^2(S^n)$ where $L_0^2(S^n)$ denotes the orthogonal complement in $L^2(S^n)$ to the space of constant functions.

Theorem 4.1. *Let $n \geq 4$. For any prime $p \neq 3$ satisfying*

$$\begin{cases} p \neq 2 & \text{if } n \neq 1 \pmod 4 \\ p = 1 \pmod 4 & \text{if } n = 1 \pmod 4 \end{cases} \tag{4.1}$$

we construct a subset $S_p \subset SO(n+1)$ such that

$$|S_p| = \begin{cases} (\sum_{i=0}^{n-1} p^i) & \text{for } n \text{ even} \\ (\sum_{i=0}^{(n-1)/2} p^i)(1+p^{(n-1)/2}) & \text{for } n \text{ odd} \end{cases}$$

and

$$\lambda_{S_p} \leq C \cdot \left(\frac{2\sqrt{p}}{p+1} \right).$$

Here C is a positive constant independent of p.

The above theorem implies that the finite subsets S_p are becoming equidistributed on S^n as $p \to \infty$. We refer to [18] for more implications of a statement like Theorem 4.1.

We remark that whereas the results in [18] rely on a deep theorem on automorphic forms, Deligne's theorem on the Ramanujan conjecture for holomorphic cusp forms [8], which in fact yields the optimal equidistribution rates for S^2 and S^3, our rates in Theorem 4.1 is based on a uniform pointwise bound on matrix coefficients of the spherical unitary dual of a special orthogonal group discussed in section 1.

Our construction of S_p follows what was referred to as "the lattice method" in [19]. To construct subsets S_p, we start with a quadratic form Q of $n+1$ variables defined over $\mathbb{Q}$ such that $SO(Q)_{\mathbb{R}} \simeq SO(n+1)$ and for each prime p listed in (4.1), $SO(Q)_{\mathbb{Q}_p} \simeq SO(\bar{I}_{n+1})_{\mathbb{Q}_p}$ where $\bar{I}_{n+1}$ is the skew-identity $n+1$ by $n+1$ matrix. Existence of such Q can be verified using the theory of quadratic forms [25]. Set $G_\infty = SO(Q)_{\mathbb{R}}$ and $G_p = SO(Q)_{\mathbb{Q}_p}$. By a suitable embedding $SO(Q)$ into SL_{n+1}, we may assume that $K_p = SO(Q) \cap SL_{n+1}(\mathbb{Z}_p)$ is a hyperspecial compact subgroup of G_p for each p in (4.1).

Let Γ be the image of the congruence subgroup

$$\{g \in G(\mathbb{Z}[\frac{1}{p}]) \mid g \equiv I_{n+1} \pmod{3\mathbb{Z}[\frac{1}{p}]}\}$$

under the diagonal embedding into $G_\infty \times G_p$ and let Γ_p be the image of Γ under the canonical projection into G_p. Then Γ_p is a torsion-free uniform lattice in G_p, and hence there exists a finite subset Δ_p such that for any $g \in G_p$, there exist unique elements $\gamma \in \Gamma_p$ and $\delta \in \Delta_p$ such that $g \in \gamma\delta K_p$.

Via the isomorphism $G_p \simeq SO(\bar{I}_{n+1})_{\mathbb{Q}_p}$, let a_p be the element in G_p corresponding to $\mathrm{diag}(p, I_{n-1}, p^{-1}) \in SO(\bar{I}_{n+1})_{\mathbb{Q}_p}$ We set $\deg(a_p) = |K_p a_p K_p / K_p|$. Write $K_p a_p K_p$ as $\amalg_{j=1}^{\deg(a_p)} \gamma_j \delta_j K_p$ where $\gamma_j \in \Gamma_p$ and $\delta_j \in \Delta_p$, and set

$$S_p = \{\gamma_j \in \Gamma_p \mid j = 1, \cdots, \deg(a_p)\}.$$

Since $\Gamma = \{(\gamma, \gamma) \in G_\infty \times G_p \mid \gamma \in \Gamma_p\}$, S_p acts on G_∞ by left translations and hence on S^n. In fact, it suffices to prove Theorem 4.1 considering T_{S_p} as an operator on $L^2(G_\infty)$.

The related local Hecke operator is now defined as follows:

Definition: Define the operator $\tilde{T}_{a_p}$ on $L^2(\Gamma\backslash G_\infty \times G_p)^{K_p}$ by

$$\tilde{T}_{a_p}(\psi)(g_\infty, g_p) = \frac{1}{\deg(a_p)} \sum_{x \in K_p a_p K_p / K_p} \psi(g_\infty, g_p x)$$

for $\psi \in L^2(\Gamma\backslash G_\infty \times G_p)^{K_p}$, $g_\infty \in G_\infty$ and $g_p \in G_p$.

Through the G_∞-equivariant maps $G_\infty \hookrightarrow G_\infty \times \Delta_p \simeq \Gamma\backslash(G_\infty \times G_p)/K_p$, the Hecke operator T_{S_p} on $L^2(G_\infty)$ corresponds to $\tilde{T}_{a_p}$ on $L^2(\Gamma\backslash G_\infty \times G_p)^{K_p}$. We obtain:

Proposition 4.1. *Set* $L_0 = L^2(\Gamma\backslash G_\infty \times G_p)^{K_p} \cap L^2_0(\Gamma\backslash G_\infty \times G_p)$. *Then*

$$\lambda_{S_p(m)} \le |\Delta_p| \cdot \|\tilde{T}_{a_p}|_{L_0}\|$$

We then show that $\langle \tilde{T}_{a_p} f_1, f_2 \rangle = \langle a_p f_1, f_2 \rangle$ for any $f_1, f_2 \in L_0$ and no finite dimensional irreducible unitary representation of G_p occurs in L_0. This enables us to apply Theorem 1.1 for G_p (recall that $n \ge 4$) to obtain that

$$\|\tilde{T}_{a_p}|_{L_0}\| \le \Xi_{PGL_2(\mathbb{Q}_p)} \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} = \frac{2\sqrt{p}}{p+1}.$$

Theorem 4.1 now follows by showing that $|\Delta_p|$ is bounded by a constant independent of p [22].

References

1. Arthur, J. (1979) Eisenstein Series and the trace formula. In: Automorphic forms, representations and L-functions by A. Borel and W. Casselman. (Eds.) Proc. Symp. Pure Math. **33**. 253–274:
2. Burger, M., Sarnak, P. (1991) Ramanujan duals II. Invent. math. **106**, 1–11
3. Chiu. P. (1995) Covering with Hecke points. J. Number Theory **53**, 25–44
4. Clozel. L., Ullmo. E. (1999) Equidistribution des points de Hecke. Preprint
5. Clozel. L., Oh. H., Ullmo. E. (2000) Hecke operators and equidistribution of Hecke points. To appear in Invent. math.
6. Cowling. M., Haggerup. U., Howe. R. E (1988) Almost L^2 matrix coefficients, J. Reiner Angew. Math **387** 97–110
7. Cowling. M. (1979) Sur les coefficients des représentations unitaires des groupes de Lie simple, in: P. Eymard, J. Faraut, G. Schiffmann, and R. Takahashi, eds.: Analyse Harmonique sur les Groupes de Lie II (Séminaire Nancy-Strasbourg 1976–78), Lecture Notes in Mathematics **739**, Springer-Verlag, New York 132–178
8. Deligne. P. (1974) La conjecture de Weil I. Publ. Math. I. H. E. S. **43** 273–308

9. Gelbart. S., Jacquet. H. (1978) A relation between automorphic representation of GL_2 and GL_3. Ann. Sci. Ecole Norm. Sup **11**, 471–552
10. Gan. W. T., Oh. H. (2000) Equidisrtibution of integer points on a family of homogeneous varieties: a problem of Linnik. Preprint
11. Harish-Chandra (1973). Harmonic analysis on reductive p-adic groups in: Harmonic analysis on Homogeneous spaces. Proc. Symp. Pure. Math. Providence **26**, 167–192
12. Howe. R. E. (1980) On a notion of rank for unitary representations of the classical groups. Harmonic analysis and group representations: II Circlo, Palazzone della Scuola normale superiore. C. I. M. E 223–331
13. Jacquet. H., Langlands, R. P. (1970) Automorphic Forms on GL_2. Springer Lect. Notes in Math. **114**
14. Li. J-S. (1996) The minimal decay of matrix coefficients for classical groups. Math. Appl (Harmonic analysis in China) **327**. 146–167
15. Li. J-S., Zhu. C-B. (1996) On the decay of matrix coefficients for exceptional groups., Math. Ann. **305**, 249–270
16. Linnik. Y. V. (1962) Additive problems and eigenvalues of the modular operators. Proc. Int. Cong. Math. Stockholm. 270–284.
17. Linnik. Y. V., Skubenko. B. F. (1964) Asymptotic distribution of integral matrices of third order., Vest. Leniner. Univ. Ser. Math. **13**, 25–36
18. A. Lubotzky. A., Phillips. R., Sarnak. P. (1986) Hecke operators and distributing points on S^2. Comm. Pure and Applied Math **39** 149–186
19. A. Lubotzky. A., Phillips. R., Sarnak. P. (1987) Hecke operators and distributing points on S^2 II. Comm. Pure and Applied Math **40** 401–420
20. Oh. H (1998) Tempered subgroups and the representations with minimal decay of matrix coefficients. Bull. Fran. Math. Soc. **126**, 355–380
21. Oh. H (1999) Uniform pointwise bounds for matrix coefficients of unitary representations and applications to Kazhdan constants. Preprint
22. Oh. H (2000) Distributing points on S^n $(n \geq 4)$ d'aprés Lubotzky, Phillips and Sarnak. Preprint
23. Sarnak. P. (1991) Diophantine problems and linear groups. Proc. I. C. M. **1**, 459–471, Springer-Verlag, Tokyo
24. Sato. M., Kimura. T. (1977) A classification of irreducible prehomogeneous vector spaces and their relative invariants. Nagoya Math. Journal **65**, 1–155.
25. Serre. J. P. (1973) A course in Arithmetic. Springer-Verlag
26. Shintani. T. (1972) Dirichlet series and integral binary cubic forms. Jorunal Math. Soc. Japan **24**, 132–188.
27. Weil. A., (1973) Basic Number Theory. Springer- Verlag