Contemporary Mathematics
Volume **00**, 0000

# Hyperelliptic Curves and Harmonic Analysis

*(Why harmonic analysis on reductive p-adic groups is not elementary)*

THOMAS C. HALES

Abstract. This paper constructs several families of hyperelliptic curves over finite fields and shows how basic objects of $p$-adic harmonic analysis are described by the number of points on these curves. This leads to proofs that there are no general elementary formulas for characters and other basic objects of harmonic analysis on reductive $p$-adic groups. Basic objects covered by this theory include characters, Shalika germs, Fourier transforms of invariant measures, and the orbital integrals of the unit element of the Hecke algebra. Various examples are given for unitary, orthogonal, and symplectic groups.

## 1. Characters and Curves

*What is the form of a character of an admissible representation of a reductive p-adic group, and more generally what is the form of the basic objects of invariant harmonic analysis on these groups?* Kazhdan, Lusztig, and Bernstein were the first to realize that the answer to this question is not elementary, and will have, when the full story is eventually told, a gratifying answer. This is the implication of a 1988 paper of Kazhdan and Lusztig [**KLB**]. The stated purpose of their paper is to study fixed-point varieties on complex affine flag manifolds, but the final section and an appendix by Kazhdan and Bernstein turn to the rank-three symplectic group over the local field $F = \mathbb{F}_q((t))$ of sufficiently large characteristic. They construct a cuspidal representation of the group $Sp(6, F)$ and a collection of regular elliptic elements $\{u_\lambda\}$ parameterized by elements $\lambda$ in

1991 *Mathematics Subject Classification.* 22E50; Secondary 22E35, 14H52, 11G20.
Research supported by an NSF postdoctoral fellowship
This paper is in final form, and no version of it will be submitted for publication elsewhere.

the finite field $\mathbb{F}_q$. The character $\chi_w$ of the representation evaluated at $u_\lambda$ has the form $\chi_w(u_\lambda) = A(q) + B(q)\#E_\lambda(\mathbb{F}_q)$, where $A$ and $B$ are nonzero polynomials in $q$, and $E_\lambda$ is an elliptic curve over the finite field $\mathbb{F}_q$ with $j$-invariant $\lambda$. Based on the form of this character, they conclude the paper with the claim, "In particular, we see that there is no 'elementary' formula for $\chi_w(u)$."

One of the most compelling problems in nonarchimedean harmonic analysis is to understand the implications of this claim for arbitrary reductive groups. In this paper, we adopt the same notion of elementariness: an object is not *elementary* if its description depends essentially on the number of points on a family of nonrational varieties over a finite field. In our examples, these varieties will be elliptic or hyperelliptic curves. (A *hyperelliptic curve* is a complete nonsingular curve of genus $g \geq 2$ that admits a finite morphism of degree two to the projective line $\mathbb{P}^1$.) We will also say, with the same meaning, that the given object or group is *nonrational*. This paper makes significant progress on (without completing) the task of delineating which reductive groups are not elementary. Examples support the expectation that the harmonic analysis on most reductive groups will not be elementary. Perhaps only $GL(n)$ and its relatives (possibly including unramified unitary groups) will possess an elementary theory.

The Kazhdan-Lusztig-Bernstein example for $Sp(6)$ stands in sharp contrast to the experience with $GL(n)$. Substantial evidence suggests a rational theory, especially calculations of characters, Fourier transforms of invariant measures supported on nilpotent orbits, and Shalika germs. The work of Corwin and Howe [**CH**] gives characters on tamely ramified division algebras, which, by the abstract matching theorem [**BDKV**], gives the characters of the discrete series of $GL(n)$ on the elliptic set. Corwin and Sally have made this even more concrete [**CS**]. Harish-Chandra established a local expansion of characters as linear combinations of Fourier transforms of nilpotent orbits, and formulas for these Fourier transforms on $GL(n)$ appear in [**Ho**]. Waldspurger gives an algorithm for computing the Shalika germs on the group $GL(n)$ [**W1**]. In none of this work on the general linear group is there any indication of nonrational behavior.

For a general reductive group very little explicit work has been done along these lines. But there is mounting evidence to show that the harmonic analysis on a general reductive group behaves more like the $Sp(6)$ example than $GL(n)$. Specifically, examples show that the following objects of local harmonic analysis admit no elementary description. In the following theorem, let $F$ be a $p$-adic field of characteristic zero, and assume that its residual characteristic is odd. We say that there is no *general elementary formula* for an object, if there exists a reductive $p$-adic group $G$ over $F$, and a given object on the group $G$ whose description is not elementary (in the sense given above).

Theorem 1.1.

(1) *There is no general elementary formula for characters.*

(2) *There is no general elementary formula for the Fourier transform of invariant measures supported on nilpotent orbits.*
(3) *There is no general elementary formula for Shalika germs.*
(4) *There is no general elementary formula for the orbital integrals of the unit element of Hecke algebras.*
(5) *The Langlands principle of functoriality is not generally elementary.*

Statement 5 has the following interpretation. Kottwitz and Shelstad have developed a theory of twisted endoscopy ([**KS1**],[**KS2**]). In it, they make precise conjectures about the relationship between orbital integrals on two different groups. In special cases, we express orbital integrals in terms of points on varieties over finite fields. The conjectures of Kottwitz and Shelstad may then be viewed as conjectural relationships (e.g., correspondences) between the underlying varieties. Statement 5 asserts that examples may be produced in which the underlying varieties on the two groups are not rational and, moreover, are not birationally equivalent to each other. What we actually show is more precise: the varieties in our example are elliptic curves, and the matching or transfer is expressed as an isogeny between the two curves.

It seems likely that Murnaghan's work on Kirillov-type formulas for local character expansions will also imply that there is no general elementary formula for the coefficients $c_{\mathcal{O}}(\pi)$ arising in Harish-Chandra's local character expansion, but I have not checked this (see [**M2**]).

We would also like to delineate which groups exhibit nonrational behavior (say (1), (2), (3), or (4) of Theorem 1.1). The following groups display at least one of these four types of nonrational behavior. In the next theorem, suppose that $F$ is a $p$-adic field of characteristic zero, with sufficiently large residual characteristic.

THEOREM 1.2. *The invariant harmonic analysis on the following groups is not elementary:*

(1) *the group ${}^2A_n$, for $n \geq 2$ (quasi-split or an inner form), assuming that the group splits over a ramified quadratic extension,*
(2) *the group $B_n$, for $n \geq 2$ (split or an inner form),*
(3) *the split group $C_n$, for $n = 2, 3$,*
(4) *the split group $D_4$.*

To prove the theorem, we show that the Shalika germs associated with certain subregular unipotent classes, when evaluated at particular elliptic semisimple elements, are expressed by the number of points on families of elliptic or hyperelliptic curves over finite fields. In the list of Theorem 1.2, the center of the group is irrelevant, and one can build further examples by taking products, isogenies, and so forth. The groups $U(3)$ and $GSp(4)$ come as pleasant surprises because of the already considerable literature on these groups.

Assuming the principle of functoriality, we can add more groups to this list. Again, we assume that $F$ is a $p$-adic field of characteristic zero and odd residual characteristic.

THEOREM 1.3. *Assume the conjectures of Kottwitz and Shelstad on the stabilization of twisted orbital integrals. Then the invariant harmonic analysis on the following additional groups is not elementary:*

(1) *the split group $C_n$, for $n \geq 2$,*
(2) *the group $D_n$, for $n \geq 5$ (any quasi-split form).*

In all of our examples, we produce nonrational behavior on the elliptic set. Trivial extensions of these theorems could be obtained by including the full set of regular semisimple elements.

I have not determined whether the exceptional groups $(G_2, F_4, E_6, E_7, E_8)$ display nonrational behavior on the elliptic set. I suspect that none of the exceptional groups will be elementary. Also, the status of unramified unitary groups remains unresolved. The Shalika germs that I have considered here are elementary, and it would not be overly surprising for the entire theory to be rational in this case.

Other results along these lines arise in the twisted harmonic analysis on reductive groups with an automorphism (see [**KS1**],[**KS2**]). For instance, consider the group $GL(2n+1)$ and the outer automorphism of the group fixing a splitting. Then for $n \geq 2$, its twisted theory is not elementary. Assuming the conjectures of Kottwitz and Shelstad, one can add several other twisted cases to the list, including $GL(2n)$ twisted by the outer automorphism that fixes a splitting, for $n \geq 2$.

Sections 4 through 7 will give complete proofs of Theorems 1.1, 1.2, and 1.3 except for the proofs of the nonrationality of $C_3$ and $D_4$. Although we do not give the proof that $C_3$ and $D_4$ are not elementary, this is at least made plausible by Examples 2.3 and 2.6 of Section 2. These examples show how elliptic curves are associated with $Sp(6)$ and $SO(8)$ (without relating these examples back to the harmonic analysis of the group). Section 2 gives short arguments establishing the existence of elliptic or hyperelliptic curves in several reductive groups.

In Section 3 we give a brief account of a general framework that ties harmonic analysis to varieties over finite fields. This section contains no proofs (and no theorems). Section 4 gives a series of concrete examples that establish that certain Shalika germs are not elementary for many reductive groups. The stable orbital integrals of the unit element of the spherical Hecke algebra of $SO(2n+1)$ are treated in Section 5. Section 6 gives a couple of examples of the Fourier transforms of nilpotent orbits in low rank. Section 7 shows how the examples of Sections 4, 5, and 6 establish Theorems 1.1, 1.2, and 1.3 (with the exception, noted above, of the nonrationality of $C_3$ and $D_4$). The proof that the harmonic analysis of $D_n$ is not elementary relies on the result for $D_4$.

At a 1992 conference at Luminy, J.-L. Waldspurger announced results concerning the homogeneity of certain invariant distributions ([**W2**],[**W3**]). By giving general explicit estimates on the domain of validity of Harish-Chandra's local character expansion, Waldspurger's work related the Kazhdan-Lusztig-Bernstein example on $Sp(6)$ to the Fourier transforms of nilpotent orbits in positive characteristic. This gave reason to believe that the Fourier transforms of nilpotent orbits would not be elementary in characteristic zero. At the same conference, G. Laumon suggested to me that it was hardly possible for the fundamental lemma to be elementary, in light of the Kazhdan-Lusztig-Bernstein example. Their comments provided the impetus behind nonrationality results described in this paper, for it was not until then that I clearly understood that nonrationality cannot make any entrance into harmonic analysis without being all-pervasive.

I dedicate this paper to the memory of L. Corwin, whose work with Howe on characters of tamely ramified division algebras gave some of the first general insights into the characters of reductive $p$-adic groups.

## 2. The Construction of Hyperelliptic Curves

The argument that certain Shalika germs are described by hyperelliptic curves is a long one. The first step is made in [**H3**]. This section presents a quick overview of the argument. We show how hyperelliptic curves are associated with some of the classical groups. In Section 3, we give a brief indication of the connection between the curves constructed in this section and the $p$-adic harmonic analysis on reductive groups.

We begin with a split reductive group $G$ defined over a field $k$ whose characteristic is not two, and with a short simple root $\alpha$ of $G$. In practice, $\alpha$ will usually be taken to be adjacent to a long root. From this data we will construct a variety that turns out to be an elliptic or hyperelliptic curve in a number of interesting situations.

We let $\mathfrak{B}$ denote the variety of Borel subalgebras of the Lie algebra of $G$. Let $W$ denote the Weyl group of $G$, which we identify with the $G$-orbits on $(\mathfrak{B} \times \mathfrak{B})$. For $w \in W$, we write $(\mathfrak{B} \times \mathfrak{B})_w$ for the orbit corresponding to $w$. For every Borel subalgebra $B$ and Cartan subgroup $T$ whose Lie algebra lies in $B$, the Weyl group $W(T)$ of $T$ is identified with $W$ by associating $(B, {}^wB)$, for $w \in W(T)$, with the corresponding $G$-orbit $(\mathfrak{B} \times \mathfrak{B})_w$, for $w \in W$. The simple reflections correspond to the orbits of dimension one more than the dimension of $\mathfrak{B}$.

Let $\mathfrak{g}$ denote the Lie algebra of $G$, and let $\tilde{\mathfrak{g}}$ denote the Springer-Grothendieck variety. It consists of the subvariety of $\mathfrak{g} \times \mathfrak{B}$ formed by pairs $(X, B)$, where $X$ belongs to the subalgebra $B$. We let $\mathfrak{h}$ denote the Cartan subalgebra of $\mathfrak{g}$. By definition, $\mathfrak{h}$ is the Lie algebra $B/[B, B]$, where $B$ is a Borel subalgebra, and $[B, B]$ is the commutator ideal. A different choice of Borel subalgebra in the definition of $\mathfrak{h}$ leads to a canonically isomorphic Lie algebra. We have a canonical morphism $\tilde{\mathfrak{g}} \to \mathfrak{h}$ that sends a pair $(X, B)$ in $\mathfrak{g}$ to the image of $X \in B$ in $\mathfrak{h} = B/[B, B]$.

We let $\tilde{\mathfrak{g}}^{rs}$ denote the elements $(X, B)$ of $\tilde{\mathfrak{g}}$ whose first coordinate $X$ is a regular semisimple element of $\mathfrak{g}$. There is an action of the Weyl group on $\tilde{\mathfrak{g}}^{rs}$. The element $w$ sends a pair $(X, B)$ to a pair $(X, B')$, where $B'$ is the unique Borel subalgebra containing $X$ such that $(B', B)$ belongs to the orbit $(\mathfrak{B} \times \mathfrak{B})_w$. To distinguish this action from various other actions to be defined below we let $\phi_w(X, B)$ denote the resulting pair. The group $W$ acts naturally on $\mathfrak{h}$, and the morphism $\tilde{\mathfrak{g}}^{rs} \to \mathfrak{h}^{rs}$ is equivariant. We also denote the action on $\mathfrak{h}$ by $\phi_w$.

We introduce a formal parameter $t$ in the Cartan subalgebra as follows. Let $k_1 = k(\mathfrak{h})$ denote the field of rational functions on $\mathfrak{h}$. The field contains the linear dual $\mathfrak{h}^*$ of $\mathfrak{h}$. The Weyl group $W$ acts on $\mathfrak{h}^*$ by $\langle \sigma_w \cdot X^*, \phi_w \cdot X\rangle = \langle X^*, X\rangle$, where $X^* \in \mathfrak{h}^*$, $X \in \mathfrak{h}$, and $\langle \cdot, \cdot \rangle$ is the canonical pairing. This action extends to field automorphisms $\sigma_w$ on $k_1$. The desired formal parameter $t$ is then the canonical element of $\mathfrak{h} \otimes_k \mathfrak{h}^* \subseteq \mathfrak{h} \otimes_k k_1 = \mathfrak{h}(k_1)$ (the algebra of $k_1$ points of $\mathfrak{h}$). It equals the element $\sum e_i \otimes e_i^*$, where $\{e_i\}$ is a basis of $\mathfrak{h}$ and $\{e_i^*\}$ is the dual basis of $\mathfrak{h}^*$. Equivalently, it is the $k_1$-point in $\mathfrak{h}(k_1) = \mathrm{Hom}_{k-\mathrm{alg}}(k[\mathfrak{h}], k(\mathfrak{h}))$, obtained by the canonical inclusion of the algebra $k[\mathfrak{h}]$ of regular functions on $\mathfrak{h}$ into its quotient field of rational functions $k(\mathfrak{h})$. The canonical element $t$ is invariant under the automorphism $\phi_w \sigma_w$ of $\mathfrak{h}(k_1)$.

The construction of the curve depends on a choice of a particular nilpotent element $N$. It is well known that if $N$ is a nilpotent element of the Lie algebra, then $r = (\dim C_G(N) - \mathrm{rank}(G))/2$ is a nonnegative integer, and we say that $N$ is $r$-regular if this number equals $r$. When $r = 0$, we also say that $N$ is *regular*, and when $r = 1$, the nilpotent element is also called *subregular*. Over the algebraic closure $\bar{k}$ of $k$, there is exactly one conjugacy class of regular nilpotent elements. Over $\bar{k}$, there is exactly one conjugacy class of subregular nilpotent elements for each connected component of the Dynkin diagram of the group. We fixed, at the beginning of this section, a particular simple root $\alpha$, which lies in a particular component of the Dynkin diagram. Hence the given simple root $\alpha$ determines a subregular nilpotent element $N$ up to stable conjugacy. We fix such an element $N$. It is a $k$-point of the Lie algebra $\mathfrak{g}$.

The variety $\mathfrak{B}_N$ of Borel subalgebras containing a subregular nilpotent element $N$ is a union of projective lines. Each projective line is associated with a simple root. There is precisely one line in $\mathfrak{B}_N$ associated with the short root $\alpha$. Thus, $\alpha$ and $N$ determine a projective line in $\mathfrak{B}$, which we denote $\mathbb{P}(\alpha, N)$. We let $S$ be the surface $\mathbb{P}(\alpha, N) \times \mathbb{P}(\alpha, N)$ in $\mathfrak{B} \times \mathfrak{B}$.

For certain groups $G$ and simple roots $\alpha$, we will construct a rational function on (a twisted form of) the surface $S$. An irreducible component of the zero set of the rational function will be the hyperelliptic curve. The rational function is (more or less) of the form $\sigma(y) - y$, for some involution $\sigma$ of the surface. If we pick a local coordinate on $\mathbb{P}(\alpha, N)$, then a point on $S$ is described by a pair

$(x_1, x_2)$, and the coordinate $y$ of the construction is $x_2 - x_1$. The key is to show that the involution arises naturally.

We pause to clarify the notation. The elements $s_\beta$ represent the simple reflections of the Weyl group, and $w$ denotes a general element of $W$. The corresponding automorphisms of the field $k_1$ associated with $W$ are denoted $\sigma_\beta$ and $\sigma_w$. The automorphisms of the regular semisimple part $\tilde{\mathfrak{g}}^{rs}$ of the Springer-Grothendieck variety are denoted $\phi_{s_\beta}$ and $\phi_w$. The same notation is used for the action of $W$ on $\mathfrak{h}$. The automorphisms $\phi_w$ are defined over $k$, so $\sigma_w$ and $\phi_w$ commute on the $k_1$-points of $\tilde{\mathfrak{g}}^{rs}$. Finally, $\sigma_\beta^*$ and $\sigma_w^*$, to be constructed in Lemma 2.2 below, denote the birational action (composed with field automorphisms) of $W$ on the surface $S$.

Let $Z_\alpha$ denote the variety of regular triples:

$$Z_\alpha = \{(Y, B_1, B_2) \in \mathfrak{g}^{rs} \times \mathfrak{B} \times \mathfrak{B} : Y \in B_1 \cap B_2,\ \phi_{s_\alpha}(Y, B_1) = (Y, B_2)\}.$$

Let $(B_1, B_2)$ be an element of $S(k_1)$ with $B_1 \neq B_2$. We select a deformation $(N(\lambda), B_1(\lambda), B_2(\lambda))$, for $\lambda \in k^\times$, of $(N, B_1, B_2)$ satisfying the following properties:

(1) $(N(\lambda), B_1(\lambda), B_2(\lambda))$, for $\lambda \neq 0$, belongs to $Z_\alpha(k_1)$.
(2) The center $(N(0), B_1(0), B_2(0))$ of the deformation is $(N, B_1, B_2)$.
(3) The image of $(N(\lambda), B_1(\lambda))$ in $\mathfrak{h}(k_1)$, under the canonical map $\tilde{\mathfrak{g}}^{rs} \to \mathfrak{h}$ is $\lambda t$, where $t$ is the canonical element of $\mathfrak{h}(k_1)$.

Such deformations exist.

Now fix an element $w$ in the Weyl group. Define $B_1'(\lambda)$ and $B_2'(\lambda)$ by the conditions $\phi_w(N(\lambda), B_1(\lambda)) = (N(\lambda), B_1'(\lambda))$ and $\phi_{s_\alpha}(N(\lambda), B_1'(\lambda)) = (N(\lambda), B_2'(\lambda))$. Let $(N, B_1', B_2')$ denote the center $(N(0), B_1'(0), B_2'(0))$ of the resulting deformation $(N(\lambda), B_1'(\lambda), B_2'(\lambda))$.

Lemma 2.1. *On a Zariski open set of $S$, the pair $(B_1', B_2')$ is independent of the choice of deformation.*

Notation. We define $\sigma_w^*(B_1, B_2) = (\sigma_w B_1', \sigma_w B_2')$, for $(B_1, B_2)$ in a Zariski open set of $S/k_1$.

Lemma 2.2. *$(B_1, B_2) \mapsto \sigma_w^*(B_1, B_2)$ defines an action of the Weyl group (by birational maps composed with field automorphisms of $k_1$).*

Proof (Lemmas 2.1 and 2.2). The definitions show directly that $\sigma_1^*(B_1, B_2)$ does not depend on the choice of deformation and that $\sigma_1^*(B_1, B_2) = (B_1, B_2)$.

We will show below that Lemma 2.1 holds when $w$ is a simple reflection. Assuming this result for the moment, we prove Lemma 2.1 by induction on the length $\ell(w)$ of $w$. Assume $\ell(w) \geq 2$. Pick a simple reflection $s_\beta$ such that $w' = s_\beta w$ has length less than $\ell(w)$. Let $(N(\lambda), B_1'(\lambda), B_2'(\lambda))$ be associated as above with a deformation $(N(\lambda), B_1(\lambda), B_2(\lambda))$ and the Weyl group element $w$. Let $(N(\lambda), B_1''(\lambda), B_2''(\lambda))$ be associated with the same deformation and the Weyl group element $w'$. Set $(B_1'', B_2'') = \sigma_{w'}^*(B_1, B_2)$. By our induction hypothesis, it is independent of the choice of deformation, and is defined on a Zariski open set. We show that the center of $(N(\lambda), B_1'(\lambda), B_2'(\lambda))$ is $\sigma_w^{-1}(\sigma_\beta^*(B_1'', B_2''))$, which, by the induction hypothesis, is indeed independent of the choice of deformation. To calculate $\sigma_\beta^*(B_1'', B_2'')$ we use the deformation

$$(\sigma_{w'} N(\lambda), \sigma_{w'} B_1''(\lambda), \sigma_{w'} B_2''(\lambda)).$$

This satisfies Conditions 1, 2, and 3 given above. Then

$$\phi_{s_\beta}(\sigma_{w'} N(\lambda), \sigma_{w'} B_1''(\lambda)) = \sigma_{w'} B_1'(\lambda),$$
$$\phi_{s_\alpha}(\sigma_{w'} N(\lambda), \sigma_{w'} B_1'(\lambda)) = \sigma_{w'} B_2'(\lambda).$$

So $\sigma_\beta^*(\sigma_{w'}^*(B_1, B_2))$ is the center of $\sigma_\beta \sigma_{w'}(N(\lambda), B_1'(\lambda), B_2'(\lambda))$ as desired.

It is now a formality that we have a group action. Take $w'$ and $w$. Write $\sigma_{w'}^*(B_1, B_2) = (B_1'', B_2'')$, obtained by a deformation $(N(\lambda), B_1(\lambda), B_2(\lambda))$. Use the same deformation to compute $\sigma_{ww'}^*(B_1, B_2)$, and use the deformation

$$(\sigma_{w'} N(\lambda), \sigma_{w'} B_1''(\lambda), \sigma_{w'} B_2''(\lambda))$$

to compute $\sigma_w^*(B_1'', B_2'')$, where

$$\phi_{w'}(N(\lambda), B_1(\lambda)) = (N(\lambda), B_1''(\lambda)) \text{ and } \phi_{s_\alpha}(N(\lambda), B_1''(\lambda)) = (N(\lambda), B_2''(\lambda)).$$

With these choices, composition holds.

We have thus reduced to Lemma 2.1 for simple reflections. Suppose that the simple root is $\alpha$. Then from the definitions it follows easily that $\sigma_\alpha^*(B_1, B_2) = (\sigma_\alpha B_2, \sigma_\alpha B_1)$. For the other simple reflections $s_\beta$, the calculation essentially reduces to the rank-two system containing the roots $\alpha$ and $\beta$. For instance, if $s_\beta$ and $s_\alpha$ commute then we find that $\sigma_\beta^*(B_1, B_2) = (\sigma_\beta B_1, \sigma_\beta B_2)$. The explicit rank-two relations are obtained in a slightly different context in [**H3,VI.1.6**]. Particular cases are found in Examples 2.3 and 2.6. Details are left to the reader. □

**Example 2.3.** Consider the group $G = Sp(6)$. We have three simple roots $\beta_1 = 2t_1$, $\beta_2 = t_2 - t_1$, and $\beta_3 = t_3 - t_2$. We let the fixed simple root $\alpha$ of the construction be $\alpha = \beta_2$. The line $\mathbb{P}(\alpha, N)$ intersects three other projective lines in $\mathfrak{B}_N$, say $\mathbb{P}_1$, $\mathbb{P}_2$, and $\mathbb{P}_3$. We assume that the nilpotent element is *distinguished* in the sense that the lines $\mathbb{P}_1$, $\mathbb{P}_2$, and $\mathbb{P}_3$ are defined over $k$. Assume that the lines $\mathbb{P}_1$, $\mathbb{P}_2$, and $\mathbb{P}_3$ are of types $\beta_1$, $\beta_2$, and $\beta_1$, respectively. Select a coordinate $x$ on $\mathbb{P}(\alpha, N)$ in such a way that the intersections of $\mathbb{P}(\alpha, N)$ with the lines $\mathbb{P}_1$, $\mathbb{P}_2$, and $\mathbb{P}_3$ have coordinates $x = 0, 1$, and $\infty$, respectively. Then on an open set of $S = \mathbb{P}(\alpha, N) \times \mathbb{P}(\alpha, N)$ we may choose the coordinate $x$ for $B_1$ and $x+y$ for $B_2$.

An explicit calculation shows that the birational map $(B_1, B_2) \mapsto \sigma_\beta^{-1}\sigma_\beta^*(B_1, B_2)$ is given for simple roots $\beta$ by

$$
\begin{aligned}
(x,y) &\mapsto \left(x, \frac{(t_1+t_2)yx}{x(t_2-t_1)-t_1 y}\right), \qquad \text{if } \beta=\beta_1,\\
&\mapsto (x+y,-y)\,, \qquad \text{if } \beta=\beta_2,\\
&\mapsto \left(x, \frac{(t_3-t_1)y}{(t_2-t_1)+y(t_3-t_2)/(1-x)}\right), \qquad \text{if } \beta=\beta_3.
\end{aligned}
\tag{2.4}
$$

In this simple case, it can be verified directly from these expressions and the Coxeter relations of the group that $(B_1, B_2) \mapsto \sigma_w^*(B_1, B_2)$ defines a Weyl group action.

Let $w_-$ be the element of longest length in $Sp(6)$. Write $\sigma_-$ and $\sigma_-^*$ for $\sigma_{w_-}$ and $\sigma_{w_-}^*$. The element $\sigma_-$ acts on $t_i$, for $i = 1, 2, 3$, by $\sigma_-(t_i) = -t_i$. Let $k_1^-$ be the field fixed by $\sigma_-$ in $k_1$. We create a twisted form $S^*$ of $S$, defined over $k_1^-$, by using the twisted action $\sigma_-^*$ of the nontrivial element of the Galois group of $\mathrm{Gal}(k_1/k_1^-)$. Since the maps of Lemma 2.2 are only birational, the surface $S^*$ is only defined up to birational equivalence. By writing $w_-$ as a product of simple reflections, Equations 2.4 may be used to find explicit rational functions $X(x, y)$ and $Y(x, y)$ such that

$$\sigma_-(x) = X(x, y), \qquad \sigma_-(y) = Y(x, y)$$

for every rational point $(x, y)$ on the twisted form $S^*(k_1^-)$. In fact, the longest element is $w_- = s_3s_2s_1s_2s_3s_2s_1s_2s_1$, where $s_i = s_{\beta_i}$. The rational functions $X$ and $Y$ are given in the appendix.

Lemma 2.5. *Assume the nondegeneracy condition $t_i^2 \neq t_j^2$, for $i \neq j$. An irreducible component of $Y(x, y) - y = 0$ is an elliptic curve with $j$-invariant*

$$32\left(\sum_{i<j}(\mu_i-\mu_j)^2\right)^3 \Big/ \prod_{i<j}(\mu_i-\mu_j)^2,$$

*where $\mu_i = 1/t_i^2$, $i = 1, 2, 3$. The other irreducible components of $Y(x, y) - y = 0$ define rational curves.*

Bernstein and Kazhdan construct an elliptic curve in $Sp(6)$ with this $j$-invariant by completely different methods. The elliptic curve $y^2 = (1 - xt_1^2)(1 - xt_2^2)(1 - xt_3^2)$ given in $Sp(6)$ in Section 3 also has this $j$-invariant.

Proof (Sketch). The surface $S$ is defined only up to birational equivalence, but the birational class of each irreducible component of the divisor $Y(x, y) - y$ is well-defined. Starting with the explicit formula for the rational function $f(x, y) = Y(x, y) - y$ in the appendix, we write $x = 1 - y/x_1$ to obtain a rational function $f_1(x_1, y) = f(x, y)$. One of the irreducible polynomial factors of $f_1(x_1, y)$ is of degree four in $x$ and quadratic in $y$. Completing the square (by a substitution

$y_1 = f_2(x_1) + f_3(x_1)y$, for suitable polynomials $f_2$ and $f_3$) we rewrite $f_1(x_1, y)$ in the form

$$y_1^2 - (a_0x_1^4 + a_1x_1^3 + a_2x_1^2 + a_3x_1 + a_4).$$

The constants $a_i$ are found by direct calculation to be

$$\begin{aligned}
a_0 &= t_2^2(-t_2 + t_3)^2,\\
a_1 &= 4t_2(-t_2 + t_3)(t_2^2 + t_1t_3),\\
a_2 &= 2(-t_1^2t_2^2 + 3t_2^4 - 3t_1^2t_2t_3 + 3t_1t_2^2t_3 + 2t_1^2t_3^2 - 3t_1t_2t_3^2 - t_2^2t_3^2),\\
a_3 &= 4(t_1 - t_2)(t_1t_2^2 + t_2^3 - t_1^2t_3 + t_1t_2t_3 + t_2^2t_3 - t_1t_3^2),\\
a_4 &= (-t_1 + t_2)^2(t_1 + t_2 + t_3)^2.
\end{aligned}$$

A standard formula for the $j$-invariant of an elliptic curve gives the $j$-invariant of the lemma. The other irreducible components of $Y(x, y) - y = 0$ are conics.

□

**Example 2.6.** The second example we consider is $G = SO(8)$. We write the four simple roots as $\beta_4 = t_4 - t_3$, $\beta_3 = t_3 - t_2$, $\beta_2 = t_2 - t_1$, and $\beta_1 = t_2 + t_1$. We select $\alpha = \beta_3$ as the distinguished simple root of the construction. The line $\mathbb{P}(\alpha, N)$ intersects three projective lines as before, and we arrange things so that the intersections of $\mathbb{P}(\alpha, N)$ with the lines of types $\beta_4$, $\beta_2$, and $\beta_1$ have coordinates 0, 1, and $\infty$, respectively. Fix coordinates $x$ and $x + y$ for $B_1$ and $B_2$ as in Example 2.3. Direct calculation shows that the birational maps $(B_1, B_2) \mapsto \sigma_\beta^{-1}\sigma_\beta^*(B_1, B_2)$, for $\beta$ simple, are given by

$$\begin{aligned}
(x, y) &\mapsto \left(x, \frac{(t_4 - t_2)y}{(t_3 - t_2) + y(t_3 - t_4)/x}\right), \quad \text{if } \beta = \beta_4,\\
&\mapsto (x + y, -y), \quad \text{if } \beta = \beta_3,\\
&\mapsto \left(x, \frac{(t_3 - t_1)y}{(t_3 - t_2) + y(t_1 - t_2)/(x - 1)}\right), \quad \text{if } \beta = \beta_2,\\
&\mapsto \left(x, \frac{(t_3 + t_1)y}{(t_3 - t_2)}\right), \quad \text{if } \beta = \beta_1.
\end{aligned}$$

We proceed as before, constructing the longest element

$$w_- = s_3s_4s_1s_3s_2s_1s_3s_1s_4s_3s_1s_2$$

(with $s_i = s_{\beta_i}$), the field $k_1^-$, and the rational function $Y(x, y) = \sigma_-(y)$.

Lemma 2.7. *Assume the nondegeneracy condition $t_i^2 \neq t_j^2$, for $i \neq j$. An irreducible component of $Y(x, y) - y = 0$ is an elliptic curve with $j$-invariant*

$$\frac{256\left(6\mu_1\mu_2\mu_3\mu_4 - \sum_{i<j<k}(\mu_i + \mu_j + \mu_k)(\mu_i\mu_j\mu_k) + \sum_{i<j}\mu_i^2\mu_j^2\right)^3}{(\mu_1 - \mu_2)^2(\mu_1 - \mu_3)^2(\mu_1 - \mu_4)^2(\mu_2 - \mu_3)^2(\mu_2 - \mu_4)^2(\mu_3 - \mu_4)^2},$$

*where* $\mu_i = t_i^2$, *for* $i = 1, 2, 3, 4$. *The other irreducible components of* $Y(x, y) - y$ *are rational.*

The elliptic curve $\epsilon y^2 = (1 - x\tau_1^2)(1 - x\tau_2^2)(1 - x\tau_3^2)(1 - x\tau_4^2)$, with $\epsilon \in k^\times \backslash k^{\times 2}$, has the same $j$-invariant, if we set $\mu_i = \tau_i^2$. This elliptic curve is the curve that should appear in $Sp(8)$ by the results of Lemma 4.10. This might well be expected, since $SO(8)$ is an endoscopic group of $Sp(8)$.

Proof. The same argument as in the proof of the previous lemma gives an elliptic curve. The calculations are even longer in this case. As with Example 2.3, they were obtained by computer and *Mathematica*. The elliptic curve obtained by completing the square is

$$y_1^2 = a_0 x_1^4 + a_1 x_1^3 + a_2 x_1^2 + a_3 x_1 + a_4,$$

with

$$\begin{aligned}
a_0 &= (-t_1 + t_2)^2 (t_1 + t_3)^2,\\
a_1 &= 4(t_1 - t_2)(t_1 + t_3)(t_1 t_2 - t_1 t_3 + t_2 t_3 - t_4^2),\\
a_2 &= 4(t_1^2 t_2^2 - 3t_1^2 t_2 t_3 + 3t_1 t_2^2 t_3 + t_1^2 t_3^2 - 3t_1 t_2 t_3^2 + t_2^2 t_3^2 + t_1^2 t_4^2 - 3t_1 t_2 t_4^2\\
&\qquad + t_2^2 t_4^2 + 3t_1 t_3 t_4^2 - 3t_2 t_3 t_4^2 + t_3^2 t_4^2),\\
a_3 &= 8(-t_2 + t_3)(t_1 t_2 t_3 - t_1 t_4^2 + t_2 t_4^2 - t_3 t_4^2),\\
a_4 &= 4(-t_2 + t_3)^2 t_4^2.
\end{aligned}$$

A standard formula for the $j$-invariant of an elliptic curve leads to the given $j$-invariant of the lemma. □

**Example 2.8.** Consider the group $G = SO(2n+1)$. We have the simple roots $\beta_n = t_n - t_{n-1}, \ldots, \beta_2 = t_2 - t_1$, and $\beta_1 = t_1$. Let the distinguished simple root $\alpha$ be $\beta_1$. The line $\mathbb{P}(\alpha, N)$ intersects two other projective lines $\mathbb{P}_1$ and $\mathbb{P}_2$ in $\mathfrak{B}_N$, and both of these lines are of type $\beta_2$. Assume that $N$ is chosen in such a way that the lines $\mathbb{P}_1$ and $\mathbb{P}_2$ are defined over $k$. Select a coordinate $x$ on $\mathbb{P}(\alpha, N)$ in such a way that $x = 0$ and $x = \infty$ define the intersection of $\mathbb{P}(\alpha, N)$ with $\mathbb{P}_1$ and $\mathbb{P}_2$. Let $x$ and $x + y$ be the coordinates of $B_1$ and $B_2$. The birational map $(B_1, B_2) \mapsto \sigma_\beta^{-1} \sigma_\beta^* (B_1, B_2)$ is given for simple roots $\beta$ by

$$\begin{aligned}
(x, y) &\mapsto (x + y, -y), \quad \text{if } \beta = \beta_1,\\
&\mapsto \left(x, \frac{2t_2 xy}{2t_1 x - t_2 y + t_1 y}\right), \quad \text{if } \beta = \beta_2,\\
&\mapsto (x, y), \qquad \text{if } \beta \neq \beta_1, \beta_2.
\end{aligned}$$

$k[\mathfrak{h}]$ is a graded ring. Let $t_x \in k[\mathfrak{h}] \subset k_1$ be an element of degree two that is Weyl group invariant (say $t_1^2 + \cdots + t_n^2$). Let $k_2/k_1$ be the quadratic field extension $k_2 = k_1[t_0]/(t_0^2 - t_x)$. The Weyl group action extends to $k_2$ with trivial action on $t_0$. The group of order two with generator $\sigma_0$ acts on $k_2$ by restricting trivially to

$k_1$ and $\sigma_0(t_0) = -t_0$. We extend the action of Lemma 2.2 to $S(k_2)$. Let $k_0 \subset k_1$ be the fixed field of $W$.

The centralizer $C_G(N)$ has two components. The group $C_G(N)$ acts on $\mathfrak{B}_N$, on $\mathbb{P}(\alpha, N)$, and diagonally on $S = \mathbb{P}(\alpha, N) \times \mathbb{P}(\alpha, N)$. This action commutes with the action of Lemma 2.2 and with the conjugation $\sigma_0$. Pick an involution $\iota$ of $S$ coming from the nonneutral component of $C_G(N)$. It has the form

$$(x, y) \mapsto \left(\frac{1}{cx}, \frac{-y}{cx(x+y)}\right),$$

for some constant $c \neq 0$ depending on the choice of $\iota$. We choose $\iota$ in such a way that $c = 1$. Let $\sigma_0^*$ be the involution $\iota\sigma_0$ of $S(k_2)$. We have an action of $\mathrm{Gal}(k_2/k_0)$ on $S(k_2)$ by the maps $\sigma_w^*$ and $\sigma_0^*$. By Galois descent, we obtain a variety $S^*$ defined over $k_0$ (or at least the birational equivalence class of a variety, since the Weyl group acts only by birational maps).

There are coordinates $y_1$ and $x_1$ on $S^*$ with the property that $x_1$ is a $k_0$-variable, $y_1$ is a $k_0(t_0)$-variable, and the condition for $(x_1, y_1)$ to define a point of $S^*(k_0)$ is

$$y_1\sigma_0(y_1) = (1 - x_1^2\tau_1^2)\cdots(1 - x_1^2\tau_n^2), \tag{2.9}$$

where $\tau_i = t_i/t_0$. We do not give a proof of these relations here. They are proved in a slightly different context in [**H5,1.2**]. We conclude that at points of $S^*(k_0)$, the rational function $\sigma_0(y_1) - y_1$ vanishes along the hyperelliptic curve $y_1^2 = f(x_1)$, where $f(x_1)$ is given by the right-hand side of Equation 2.9.

## 3. Relation to Shalika Germs

In this section we sketch the connection between Shalika germs and varieties over finite fields. As we have already mentioned, many of the proofs are long and are not given here. The purpose of this section is merely to orient the reader to a suitable conceptual framework. This framework is provided by the work of Denef, Igusa, Langlands, Shelstad, and others.

Let $F$ be a $p$-adic field of characteristic zero. Igusa [**I**] established a general asymptotic expansion for families of integrals over $p$-adic manifolds. The asymptotic expansion of the family of integrals $I(\lambda)$, depending on a parameter $\lambda \in F^\times$, takes the general form of a *finite* sum of quasicharacters $\theta : F^\times \to \mathbb{C}^\times$ and powers of logarithms:

$$I(\lambda) \sim \sum_\theta \theta(\lambda)(\log|\lambda|)^m c_{\theta,m}$$

as $\lambda$ tends to zero. The expansion actually gives an exact formula for $I(\lambda)$ when $\lambda$ is sufficiently small. For each quasicharacter $\theta_0$, Igusa considers the Mellin transform

$$Z(\theta_0, s) = \int_{|\lambda|\le\epsilon} I(\lambda)\theta_0(\lambda)|\lambda|^s\,|d\lambda|, \quad \text{for } s \in \mathbb{C} \text{ and } \quad \Re(s) \gg 0,$$

for any small positive constant $\epsilon$. The Mellin transforms $Z(\theta_0, s)$ are rational functions of $q^{-s}$. As $\theta_0$ varies, the Mellin transforms determine the original asymptotic expansion. The functions $Z(\theta_0, s)$ are essentially examples of *Igusa's local zeta functions*. We refer the reader to Denef's survey article [**D2**].

Langlands and Shelstad showed how the asymptotic expansion of Shalika fits naturally into the framework of Igusa's theory. In Shalika's germ expansion there are no logarithmic terms: $c_{\theta,m} = 0$, for $m \neq 0$. In their work, the terms $c_{\theta,0}$ of the original asymptotic expansion (and so also the Shalika germs) are given as principal-value integrals on $p$-adic manifolds $X$ (see [**L**] and [**H3**]).

Denef proved that a large class of Igusa zeta functions have a description in terms of the number of points on varieties over finite fields [**D1**].

If we formulate Denef's argument in terms that mesh with the treatment of Shalika germs given by Langlands and Shelstad, then the strategy is to replace each of the $p$-adic manifolds $X$ with a scheme $X_0$ that is proper over $O_F$, the ring of integers of $F$. The integration over the analytic manifold $X$ is then to be replaced with integration over the $O_F$-points of $X_0$. Let $k$ be the residue field of $F$, and set $\bar{X}_0 = X_0 \times_{O_F} k$. There is a canonical map $\varphi : X_0(O_F) \to \bar{X}_0(k)$ to the set of points on the variety over the finite field. The integral of a measure $|\omega|$ over $X$ may then be written

$$\int_X |\omega| = \sum_{x\in\bar{X}_0(k)} \int_{\varphi^{-1}(x)} |\omega|.$$

If we knew, for instance, that the integral over the fiber $\varphi^{-1}(x)$ was a constant $c$ independent of $x$, then the integral over $x$ would become $c\,\#\bar{X}_0(k)$. In general, the most we can hope for is that the integral over the fiber will be independent of $x$, for $x$ in a Zariski open set $U \subset \bar{X}_0$. We then repeat the argument on the complement of $U$ in $\bar{X}_0$. The integral over $X$ is then eventually expressed as the sum of $c\,\#\bar{X}_0(k)$ and similar terms coming from a finite collection of closed subvarieties of $\bar{X}_0$.

This argument, when it can be carried out, expresses the Shalika germs in terms of points on varieties over finite fields. In the context of Shalika germs, the varieties $X$ and the accompanying data depend on a parameter $t$ in the Lie algebra, so that we actually obtain families of varieties. Typically, the constants $c$, independent of $t$, are elementary functions of $q$, the cardinality of the residue field. This paper deals with examples where $\bar{X}_0$ is a nonconstant family of elliptic or hyperelliptic curves. An important unsolved problem is to determine how generally Denef's argument applies to Shalika germs and other basic objects of harmonic analysis on $p$-adic groups. Are the Fourier transforms of nilpotent orbits and the Shalika germs always representable by points on varieties over finite fields?

The surface $S$ of the previous section is birationally equivalent to one of the irreducible components $S'$ of the surface $X$ that arises in the study of Shalika germs of subregular unipotent elements in a reductive group $G$. The Weyl group acts on $S'$, and this permits us to define a form of $S'$ for every Cartan subgroup $T$ of $G$. The Shalika germ is expressed as an integral over the twisted form of $S'$ and of the other irreducible components of the surface $X$. The fields $k$ and $k_1$ of Section 2 are to be a $p$-adic field $F$ of characteristic zero, and a splitting field $T$ of the Cartan subgroup.

Examples 2.3 and 2.6 of the previous section stem from the elliptic Cartan subgroup $T$ split by a ramified quadratic extension $E/F$, obtained by twisting the split Cartan subgroup by the longest element $w_-$. In this case, we may specialize the parameters $t_i$ so that $t_i/t_j \in F$ and $t_i \in E$. Assume that the parameters $t_i$ all have the same half-integral valuation, say $|t_i| = q^{-1/2}$, for $i = 1, 2, 3$. Let $\tau_i$ be the residue of the unit $t_i/\sqrt{\pi}$, where $\pi$ is a uniformizing parameter. The rational function $Y(x, y)$ descends to a rational function on the finite residue field, again denoted $Y(x, y)$: take $x, y \in k$ and use the fact that $Y(x, y)$ is homogeneous of degree zero in the coordinates $t_i$ to replace each $t_i$ by $\tau_i$. Consider the expression

$$\sigma_-(y) - y = Y(x, y) - y, \qquad \text{for } \sigma_- \in \mathrm{Gal}(E/F).$$

If $E/F$ is ramified, then this expression vanishes for $x$ and $y$ in the residue field $k$, because $\sigma_-$ acts trivially on the residue field. We conclude that $0 = Y(x, y) - y$, for $x, y \in k$.

The calculations of Examples 2.3 and 2.6 descend to the finite field without difficulty and give us an elliptic curve over the finite field. The $j$-invariants are obtained by replacing $t_i$ by $\tau_i$ in Lemmas 2.5 and 2.7. One part of the integral over the surface $X$ is then a constant times the number of points on the elliptic curve. This gives one term (the nonrational term) in the formula for the subregular Shalika germ of orbital integrals.

## 4. Examples

We establish some notation and conventions for Sections 4-7. Let $F$ be a $p$-adic field of characteristic zero and odd residual characteristic, with ring of integers $O_F$, algebraic closure $\bar{F}$, and residue field $k$ of cardinality $q$. Let $\pi$ be a uniformizer in $F$.

The Shalika germs, unless indicated to the contrary, are to be the germs of stable orbital integrals normalized by the usual discriminant factor (denoted $|\eta(X)|_{\mathfrak{p}}^{1/2}$ in [**HC**] and $D_{G^*}(\exp(X))$, for $X$ sufficiently small, in [**LS**]). We write it $D(X)$. The measures of orbital integrals are normalized as in [**L**]. We take the Shalika germs to be homogeneous functions on the Lie algebra, with the understanding that the germ expansion holds only for regular semisimple elements sufficiently close to the identity. Since the discriminant factor $D(X)$ is already included in the definition of germs, we omit the discriminant factor $\Delta_{IV}$ from the definition of the Langlands-Shelstad transfer factor $\Delta$.

Let $G$ be a reductive group over $F$. More specifically, we assume that $G$ is one of the groups $SU_E(n)$, $Sp(2n)$, or $SO(n)$. We assume that $G$ is defined by a matrix equation

$$^t g\, J\, \sigma(g) = J,$$

where the entries of the matrix $J$ satisfy $J_{ik} = 0$, for $i+k \ne n+1$, and $J_{ik} = \pm 1$ along the skew-diagonal. (Replace $n$ by $2n$ if $G = Sp(2n)$.) We assume that the nonzero entries of $J$ equal one, for the orthogonal group. We take $g \in SL(n,F)$ for $SO(n)$, $g \in SL(2n,F)$ for $Sp(2n)$, and $g \in SL(n,E)$ for $SU_E(n)$. We assume that $E/F$ is a fixed *ramified* quadratic extension, and $\sigma(g)$ denotes the matrix obtained by applying the nontrivial field automorphism of $E/F$ to each coefficient of $g$. We take $\sigma(g) = g$ in the orthogonal and symplectic groups.

Each regular semisimple element of the Lie algebra $\mathfrak{g}$ of $G$ is diagonalizable over $\bar{F}$. We write $t = [t_1, \dots, t_n] \in \mathfrak{g}(\bar{F})$ for a diagonal element. Specifically, we let $[t_1, \dots, t_n]$ denote the element

$$\begin{aligned}
&\mathrm{diag}(t_1, \dots, t_n), \quad \text{if } G = SU_E(n),\\
&\mathrm{diag}(t_1, \dots, t_n, -t_n, \dots, -t_1), \quad \text{if } G = Sp(2n) \text{ or } G = SO(2n),\\
&\mathrm{diag}(t_1, \dots, t_n, 0, -t_n, \dots, -t_1), \quad \text{if } G = SO(2n+1).
\end{aligned}$$

The elements $t_1, \dots, t_n$ lie in $\bar{F}$. We assume that the image of $[t_1, \dots, t_n]$ in $\mathfrak{h}/W$ (the diagonal subalgebra modulo the Weyl group) is an $F$-point. Extend the normalized absolute value on $F$ to $\bar{F}$.

Most of our examples come from a particular set of elliptic semisimple elements in the Lie algebra of our reductive group $G$, a set that we will call the half-integral set. We say that $t = [t_1, \dots, t_n]$ is *half-integral* if

$$|t_i| = |\alpha(t)| = q^{-1/2},$$

for all $i$ and every root $\alpha$ of $\mathfrak{h}$. For example, if $G = Sp(2n)$, this condition reads $|t_i| = |t_i \pm t_j| = q^{-1/2}$, for all $i$ and $j$. Given a half-integral element $t$, and a ramified quadratic extension $E/F$, we define elements $\tau_i$ in the algebraic closure $\bar{k}$ of the residue field $k$ of $F$. Let $\tau_i$ be the residue of $t_i/\pi_E$, where $\pi_E$ is a uniformizer of $E$ whose square lies in $F$. A different choice of uniformizer changes all the elements $\tau_i$ by the same element of $k^\times$. We write $\tau_E(t) = [\tau_1, \dots, \tau_n]$ for the array of elements obtained. Fix a unit $\epsilon \in k^\times$ that is not a square (occasionally we identify $\epsilon$ with a unit of $F$).

Assume that $t$ is half-integral and that a ramified quadratic extension $E/F$ has been fixed. The following hyperelliptic curves are then defined over $k$.

(4.1)
$$\epsilon y^2 = (1-x^2\tau_1^2)(1-x^2\tau_2^2)\cdots(1-x^2\tau_n^2), \quad (G = SO(2n+1)),$$
(4.2)
$$\epsilon y^2 = (1-x\tau_1^2)(1-x\tau_2^2)\cdots(1-x\tau_n^2), \quad (G = Sp(2n)),$$
(4.3)
$$\epsilon y^2 = x(1-x\tau_1^2)(1-x\tau_2^2)\cdots(1-x\tau_n^2), \quad (G = Sp(2n)),$$
(4.4)
$$\epsilon y^2 = (1+x\tau_1)(1+x\tau_2)\cdots(1+x\tau_n), \quad (G = SU_E(n), \quad n \text{ even}),$$
(4.5)
$$\epsilon y^2 = (x+\tau_1)(x+\tau_2)\cdots(x+\tau_n), \quad (G = SU_E(n), \quad n \text{ odd}).$$

We assume that the ramified extension $E/F$ used for $\tau_E$ is the splitting field of $SU_E(n)$ in the case of unitary groups. The half-integrality of $t$ implies that the polynomials on the right-hand side of these equations have distinct roots. Let $P(x)$ be a polynomial of degree $d$ with distinct roots. The genus $g$ of the complete nonsingular curve associated with $y^2 = P(x)$ is the integral part of $(d-1)/2$. By definition, a hyperelliptic curve is complete. A second coordinate patch, which includes the points at *infinity*, is described by the equation $y_1^2 = P_1(x_1)$, where $y_1 = y/x^{g+1}$, $x_1 = 1/x$, and $P_1$ is the polynomial $P_1(x) = x^{2g+2}P(1/x)$.

Let $C_i(\tau_E(t))$ denote the number of points in $k$ on the hyperelliptic curve of Equation 4.$i$, for $i = 1,2,3,4,5$. The number $C_i(\tau_E(t))$ depends on $E$, but not on the choice of uniformizer $\pi_E$ in $E$ (except for $C_5(\tau_E(t))$: see Lemma 4.15). The examples in this section will show how certain Shalika germs on the half-integral set of $G$ are expressed in terms of the number of points $C_i(\tau_E(t))$ on hyperelliptic curves.

LEMMA 4.6. *Half-integral elements are regular elliptic.*

PROOF. If $t$ is half-integral and not elliptic, then there exists a nonempty subset $I \subset \{1,\ldots,n\}$ and a choice of signs $\epsilon_i = \pm 1$, for $i \in I$, such that $\mathrm{Gal}(\bar{F}/F)$ acts on and even acts transitively on the set $\{t_i\epsilon_i : i \in I\}$ (see [**H5,**§**4**]). Fix a ramified quadratic extension $E/F$ and a uniformizing parameter $\pi_E \in E$. Write $\{t_i\epsilon_i/\pi_E : i \in I\} = \{s_1,\ldots,s_\ell\}$. The polynomial
$$(X-s_1)\cdots(X-s_\ell) = X^\ell + a_1X^{\ell-1} + \cdots + a_\ell$$
has coefficients in $O_E$. If $\sigma$ is the nontrivial element of $\mathrm{Gal}(E/F)$, then $\sigma(a_i) = (-1)^i a_i$. Since $E/F$ is ramified, $a_i$ is congruent to $(-1)^i a_i$ modulo the maximal ideal of $O_E$. If $\ell$ is odd, then $a_\ell$ is congruent to zero, and this contradicts the condition that $s_i$ are units. If $\ell$ is even, then the polynomial is congruent to a polynomial in $X^2$, and this means that for every $i$, there exists a $j$ such that $s_i$ is congruent to $-s_j$, or that $|t_i\epsilon_i + t_j\epsilon_j| < q^{-1/2}$. For $G = SO(n)$ or $G = Sp(2n)$,

clearly $t_i\epsilon_i + t_j\epsilon_j$ is a root $\alpha(t)$, and this inequality contradicts the condition of half-integrality.

For $SU_E(n)$ we divide our set into positive and negative pieces:

$$\{s_1, \dots, s_m\} = \{t_i/\pi_E : i \in I, \epsilon_i = +1\},\ \{s'_1, \dots, s'_m\} = \{t_i/\pi_E : i \in I, \epsilon_i = -1\}.$$

The polynomials

$$P(X) = (X - s_1)\cdots(X - s_m) \quad \text{and } P'(X) = (X - s'_1)\cdots(X - s'_m)$$

are defined over $E$, and $\sigma(P) = P'$, for $\sigma$ nontrivial in $\mathrm{Gal}(E/F)$. Thus, for every $i$ there exists a $j$ such that $s_i$ is congruent to $s'_j$, so that we again reach the contradiction $|\alpha(t)| < q^{-1/2}$ for some root $\alpha$. □

LEMMA 4.7. *Fix a ramified quadratic character $\eta$ of $F^\times$. Let $P(x)$ be a polynomial with coefficients in $O_F$. Assume that $P(x)$ reduces to a polynomial in the residue field whose roots are distinct. Assume that $P(0)$ is a unit and a square. Then*

$$\int_{\mathbb{P}^1(F)} \eta(P(x)) \left|\frac{dx}{x^2}\right| = \frac{-C(P)}{q},$$

*where $C(P)$ is the number of points on the hyperelliptic curve over the residue field $k$ obtained by reduction of the equation $\epsilon y^2 = P(x)$.*

PROOF. As in [**H5,2.2**], we may replace the integrand $\eta(P(x))$ by $\eta(P(x)) - 1$. For each residual point $x_0 \in \mathbb{P}^1(k)$, let $U(x_0)$ denote the set of $x \in \mathbb{P}^1(F) = \mathbb{P}^1(O_F)$ that reduce to $x_0$ under the canonical reduction map $\mathbb{P}^1(O_F) \to \mathbb{P}^1(k)$. Then it is easy to check that

$$\int_{U(x_0)} (\eta(P(x)) - 1) \left|\frac{dx}{x^2}\right|$$

is equal to 0, $-1/q$, or $-2/q$. We obtain 0 when $\eta(P(x)) = 1$ on $U(x_0)$, that is, $P(x)$ is a unit and a square. We obtain $-2/q$ when $\eta(P(x)) = -1$ on $U(x_0)$, that is, $P(x)$ is a unit but not a square. And we obtain $-1/q$ when $P(x)$ lies in the maximal ideal, giving a point of ramification on the hyperelliptic curve over the finite field. The points at *infinity* ($|x| > 1$) are treated similarly by using local coordinates $(x_1, y_1) = (1/x, y/x^{g+1})$, where $g$ is the genus of the hyperelliptic curve. The result now follows easily. □

On the group $SO(2n+1)$, the subregular unipotent classes are parameterized by the set $F^\times/F^{\times 2}$. For $a \in F^\times/F^{\times 2}$ and $t = [t_1, \dots, t_n]$, we let $\Gamma_a(t)$ be the stable subregular Shalika germ on the half-integral set of $SO(2n+1)$ associated with the class parameterized by $a$. The stable Shalika germs are well-defined up to a scalar multiple that depends on the normalization of measures.

Lemma 4.8. *With appropriate normalizations, the stable subregular Shalika germs of $SO(2n+1)$ on the half-integral set are*

$$\Gamma_a(t) = 1, \text{ if } a \text{ has even valuation,}$$
$$\Gamma_a(t) = C_1(\tau_E(t)), \text{ if } a \text{ has odd valuation.}$$

*Here $E$ is the ramified extension $E = F(\sqrt{a})$, and $C_1(\tau_E(t))$ is the number of points on the hyperelliptic curve in Equation 4.1.*

Proof. By [**H5,1.2**], the stable subregular Shalika germs are given by the following principal-value integrals:

$$\Gamma_a(t) = \int_F \log|(1-x^2t_1^2)\dots(1-x^2t_n^2)| \left|\frac{dx}{x^2}\right|, \text{ if } a = F^{\times 2},$$
$$\Gamma_a(t) = \int_{\mathcal{I}m(a)} \eta_a((1-u^2t_1^2)\cdots(1-u^2t_n^2)) \left|\frac{du}{u^2}\right|, \text{ if } a \neq F^{\times 2}, \tag{4.9}$$

where $\eta_a$ is the quadratic character of $F^\times$ associated with the extension $F(\sqrt{a})$, and $\mathcal{I}m(a)$ is the corresponding imaginary axis: $\sqrt{a}F \subset F(\sqrt{a})$.

If $a$ is even, then it is easy to see that these integrals are independent of $t$ on the half-integral set. Explicitly, we have

$$\Gamma_a(t) = n\int_F \log|(1-\pi x^2)| \left|\frac{dx}{x^2}\right| = \frac{n(q+1)}{q(q-1)}, \quad \text{if } a = F^{\times 2},$$
$$\Gamma_a(t) = \frac{-1+(-1)^n}{q}, \quad \text{if } a \neq F^{\times 2}.$$

(Compare [**H5,2.8**].) A change in normalizations gives $\Gamma_a(t) = 1$.

If $a$ has odd valuation, then these integrals are determined on the half-integral set by Lemma 4.7, under the substitution $u = x/\pi_E$, where $\pi_E$ is a uniformizer in $E$. Changing normalizations, we may eliminate the constant $-1/q$ appearing in Lemma 4.7. The result follows. □

For the group $PSp(2n)$, the subregular unipotent classes are also parameterized by the set $F^\times/F^{\times 2}$. For $a \in F^\times/F^{\times 2}$, we let $\Gamma_a(t)$ be the stable subregular Shalika germ on the half-integral set attached to the subregular unipotent element associated with $a$. It is well-defined up to a scalar multiple depending on the normalizations of measures.

Lemma 4.10. *Assume the conjectures of Kottwitz and Shelstad on the transfer of orbital integrals. With suitable normalizations, the stable subregular Shalika germs of $PSp(2n)$ on the half-integral set are*

$$\Gamma_a(t) = \gamma_a + C_2(\tau_E(t)), \quad \text{if } a \text{ has even valuation,}$$
$$\Gamma_a(t) = \gamma_a + C_3(\tau_E(t)), \quad \text{if } a \text{ has odd valuation.}$$

*Here $C_2(\tau_E(t))$ and $C_3(\tau_E(t))$ are the numbers of points on the hyperelliptic curves defined by Equations 4.2 and 4.3, and the $\gamma_a$ are (known) constants in $\mathbb{C}$ that are independent of $t$ (but dependent on $n$ and $q$). The ramified extension $E$ is given by $E = F(\sqrt{\pi})$.*

Proof. For the stable germs, there is no harm in working on the group $Sp(2n)$ instead of $PSp(2n)$. As [**H5,§1**] explains, the conjectures of Kottwitz and Shelstad lead to a conjectural duality between groups of type $C_n$ and groups of type $B_n$. Each stable Shalika germ on $B_n$ should be a linear combination of stable Shalika germs on $C_n$, and each stable Shalika germ on $C_n$ should be a linear combination of stable Shalika germs on $B_n$. We add superscripts $B$ and $C$ to the stable subregular germs on $B_n$ and $C_n$ to distinguish notation for these two groups. It is also convenient to begin with the normalization of germs given in [**H5,§2**], which we distinguish by adding a bar: $\bar\Gamma^B_a$, $\bar\Gamma^C_a$, and so forth. For stable subregular germs on the groups $B_n$ and $C_n$ of rank $n$, the theory of Kottwitz and Shelstad thus predicts the existence of an invertible $4 \times 4$ matrix relation:

$$\bar\Gamma^C_a(t) = \sum_{a'} L^{(n)}_{a,a'} \bar\Gamma^B_{a'}(t). \tag{4.11}$$

The matrix $L^{(n)}$ is independent of $t$. Equation 4.11 has been verified in rank two (see [**H5,2.1**]), and the matrix $L^{(2)}$ is uniquely determined. We have

$$L^{(2)} = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & s_q & -s_q \\ 1 & -1 & -s_q & s_q \end{pmatrix}.$$

Here $s_q = 1$, if $-1$ is a square in $F$, and $s_q = -1$ otherwise. The cosets have been put into the order $F^{\times 2}$, $\epsilon F^{\times 2}$, $\pi F^{\times 2}$, $\pi\epsilon F^{\times 2}$.

The stable Shalika germs $\bar\Gamma^C_a$ and $\bar\Gamma^B_a$, restricted respectively to Levi factors $\mathbb{G}_m^{n-2} \times Sp(4)$ and $\mathbb{G}_m^{n-2} \times SO(5)$, reduce to the stable Shalika germs on the rank-two groups $Sp(4)$ and $SO(5)$. This reduction is compatible with the normalization that we have given the germs. Since the restrictions are already linearly independent, the matrix $L^{(n)}$ is already determined by this restriction. Hence we must have $L^{(n)} = L^{(2)}$, for all $n$. Thus, Equation 4.11 gives an exact (conjectural) formula for the stable subregular Shalika germs of $C_n$. For instance, picking representatives 1, $\epsilon$, $\pi$, and $\pi\epsilon$ for the cosets of $F^\times/F^{\times 2}$, we should have

$$\bar\Gamma^C_1 = \frac{1}{2}(\bar\Gamma^B_1 + \bar\Gamma^B_\epsilon + \bar\Gamma^B_\pi + \bar\Gamma^B_{\pi\epsilon}),$$

where $\bar\Gamma^B_a$ is given by Equation 4.9. Lemma 4.8 shows that the term $\frac{1}{2}(\bar\Gamma^B_1 + \bar\Gamma^B_\epsilon)$ contributes a constant to the formula of the lemma. The term $\frac{1}{2}(\bar\Gamma^B_1 - \bar\Gamma^B_\epsilon)$ is also constant on the half-integral set.

To prove the lemma, we must show that up to constants $d_0, d_1, d_2, d_3$ independent of $t$ we have $\bar\Gamma^B_\pi + \bar\Gamma^B_{\pi\epsilon} = d_0 + 2d_2C_2(\tau_E(t))$ and $\bar\Gamma^B_\pi - \bar\Gamma^B_{\pi\epsilon} = d_1 + 2d_3C_3(\tau_E(t))$.

Set $E = F(\sqrt{\pi})$, and $E' = F(\sqrt{\pi\epsilon})$. The normalization constants, which relate $\bar\Gamma_a^B$ to the normalization of Equation 4.9, and Equation 4.9 to the normalization of Lemma 4.8, are the same for the cosets $a = \pi F^{\times 2}$ and $a = \pi\epsilon F^{\times 2}$. By Lemma 4.8, it will suffice to show that

$$C_1(\tau_E(t)) + C_1(\tau_{E'}(t)) = 2C_2(\tau_E(t)), \tag{4.12}$$

and

$$C_1(\tau_E(t)) - C_1(\tau_{E'}(t)) = 2(C_3(\tau_E(t)) - 1 - q). \tag{4.13}$$

Underlying these identities is the fact that the Jacobian of the curve $y^2 = (1 - x^2\tau_1^2)\cdots(1 - x^2\tau_n^2)$ is isogenous to the product of the Jacobians of $y^2 = (1 - x\tau_1^2)\cdots(1 - x\tau_n^2)$ and $y^2 = x(1 - x\tau_1^2)\cdots(1 - x\tau_n^2)$.

We check the identities directly as follows. To prove Identity 4.12, note that each point $(x, y)$ of the curve $\epsilon y^2 = (1 - x\tau_1^2)\cdots(1 - x\tau_n^2)$ leads to two points $(x_1, y_1) = (\pm\sqrt{x}, y)$ on the curve $\epsilon y_1^2 = (1 - x_1^2\tau_1^2)\cdots(1 - x_1^2\tau_n^2)$, if $x$ is a square, or to two points $(x_1, y_1) = (\pm\sqrt{x/\epsilon}, y)$ on the curve $\epsilon y_1^2 = (1 - x_1^2\tau_1^2\epsilon)\ldots(1 - x_1^2\tau_1^2\epsilon)$ otherwise. We may assume $\tau_{E'}(t) = \epsilon\tau_E(t)$. This proves Identity 4.12.

To prove Identity 4.13, we observe that there are two points on $y_1^2 = (1 - x_1^2\tau_1^2)\cdots(1 - x_1^2\tau_n^2)$ given by $(x_1, y_1) = (\pm\sqrt{x}, y/x_1)$, or two points on $\epsilon y_1^2 = (1 - x_1^2\tau_1^2\epsilon)\cdots(1 - x_1^2\tau_n^2\epsilon)$ given by $(x_1, y_1) = (\pm\sqrt{x/\epsilon}, y/(x_1\epsilon))$, for each point $(x, y)$ on $y^2 = x(1 - x\tau_1^2)\cdots(1 - x\tau_n^2)$. A twist $\epsilon y^2 = P(x)$ has $1 + q - b$ points if $y^2 = P(x)$ has $1 + q + b$ points. This completes the proof of Lemma 4.10. □

In the adjoint group of $U_E(2k)$ there is a single subregular conjugacy class. Stable germs may be grouped together according to the unipotent classes in the adjoint group [**H3,VII.5.4**].

LEMMA 4.14. *Assume that $E/F$ is a ramified quadratic extension. With suitable normalizations, the stable subregular Shalika germ of $U_E(2k)$ on the half-integral set is equal to $C_4(\tau_E(t))$, the number of points on the hyperelliptic curve of Equation 4.4.*

PROOF. We deduce the lemma from the results of Chapter VII of [**H3**]. The argument is nearly identical to the argument given in [**H5,§1**] for the group $SO(2n+1)$. In the notation of [**H3,page 124**], set $u = w/(-T_{-1}w + 1)$. The structure constants $e(\alpha, \beta)$ appearing in [**H3,V.6**] are $e(\alpha_i, \alpha_{i+1}) = 1$ and $e(\alpha_{i+1}, \alpha_i) = -1$. Then an easy calculation using [**H3,VII.5.6**] shows that $u$ is a Weyl group invariant coordinate, and that $\sigma_0(u) = -u$, where $\sigma_0$ denotes the nontrivial element of $\mathrm{Gal}(E/F)$. Let $[b] = (1 + uT_1)\cdots(1 + uT_k)$, considered as an $\bar F$-point of $U_E(1)$ depending on $u$. Consider the cocycle $a_\sigma$ of $\mathrm{Gal}(\bar F/F)$ with values in $\bar F$, given by [**H3,VII.5.6**]. Then $a_\sigma\,\sigma[b][b]^{-1}$ is equal to one, if the image of $\sigma$ in $\mathrm{Gal}(E/F)$ is trivial, and is equal to

$$1/((1 + uT_k)\cdots(1 + uT_1)(1 + uT_{-1})\cdots(1 + uT_{-k}))$$

otherwise. The nontrivial character of $H^1(\mathrm{Gal}(\bar F/F), U_E(1))$ evaluated on $a_\sigma$ is then

$$\eta((1+uT_k)\cdots(1+uT_{-k})),$$

where $\eta$ is the quadratic character of $F^\times$ attached to $E/F$. Shifting from the notation $T_i$ of [**H3**] back to our notation $t_i$, we find that this expression is equal to $\eta((1+ut_1)\cdots(1+ut_n))$ (because $\{t_1,\ldots,t_n\}=\{T_k,\ldots,T_{-k}\}$).

Now $|dw/w^2| = |du/u^2|$, and the stable germ is

$$\frac{1}{2}|\lambda|\int_{\mathcal{I}m}\eta((1+ut_1)\cdots(1+ut_n))\left|\frac{du}{u^2}\right|,$$

where $\mathcal{I}m$ is the set of elements $u\in E$ that satisfy $\sigma_0(u)=-u$. On the half-integral set, we take $\lambda=1$ and evaluate by Lemma 4.7 to obtain the theorem. □

Now consider the group $G=U_E(2k+1)$. On its adjoint group there are two subregular conjugacy classes, but their stable germs differ only by a sign if the appropriate normalizations of measures are chosen. (Compare [**H2,§5**].)

LEMMA 4.15. *Assume that $E/F$ is a ramified quadratic extension. With a suitable normalization of measures, the stable subregular Shalika germ of $U_E(2k+1)$ on the half-integral set is equal to $1+q-C_5(\tau_E(t))$, where $C_5(\tau_E(t))$ is the number of points on the hyperelliptic curve of Equation 4.5.*

As we have noted, the constant $C_5(\tau_E(t))$ depends on the choice of a uniformizer $\pi_E$. The lemma holds for every choice of uniformizer if we adapt the sign of the normalization of measures to $\pi_E$. In fact, if $\pi'_E=\pi_E\epsilon$, then with obvious notation $1+q-C_5(\tau_E(t)) = -(1+q-C_5(\tau'_E(t)))$.

PROOF. The argument is similar to the proof of the previous lemma. The structure constants are $e(\alpha_i,\alpha_{i+1})=1$ and $e(\alpha_{i+1},\alpha_i)=-1$ as before. We define $u$ by $u=w/(-T_0w+1)$. It is a Weyl group invariant coordinate, and $\sigma_0(u)=-u$ as before. This time we adjust the cocycle $a_\sigma$ by $\sigma[b][b]^{-1}$, where $[b]^{-1}=(1+uT_0)\cdots(1+uT_{-k})$. We find that the nontrivial character of $H^1(\mathrm{Gal}(\bar F/F),U_E(1))$ evaluated on $a_\sigma$ is equal to

$$\eta(x(\gamma))\eta((1+uT_k)\cdots(1+uT_0)\cdots(1+uT_{-k})) = \eta(x(\gamma)u(1+ut_1)\cdots(1+ut_n)),$$

where $\eta$ is the character of $F^\times$ attached to $E$ and $x(\gamma)$ is a constant in $F^\times$. The formula of [**H3,VII.5.5**] now shows that the germ is

$$\frac{1}{2}\eta(x(\gamma))\eta(\lambda)|\lambda|\int_{\mathcal{I}m(a)}\eta(u(1+ut_1)\cdots(1+ut_n))\left|\frac{du}{u^2}\right|.$$

$\eta(x(\gamma))$ is a sign depending on the subregular unipotent class. On the half-integral set, we take $\lambda=1$, and we use an adaptation of Lemma 4.7 to show that the germ is a multiple of the difference of $1+q$ and the number of points on the hyperelliptic curve

$$\epsilon y^2 = x(1+x\tau_1)\cdots(1+x\tau_n).$$

In fact, Lemma 4.7 does not hold because $P(0)$ is not a unit, and

$$\int_{U(0)} \eta(P(x)) - 1 \left|\frac{dx}{x^2}\right| = 1 = \frac{q+1}{q} - \frac{1}{q},$$

instead of the constant $-1/q$ occurring in the proof of the lemma. We pick up the term $(q+1)/q$, so the integral is $q^{-1}$ times $1+q-C_5(\tau_E(t))$. Under the substitution $(x,y)\mapsto(1/x, y/x^{(n+1)/2})$, we obtain the curve $\epsilon y^2 = (x+\tau_1)\cdots(x+\tau_n)$ as desired. □

The groups $Sp(6)$ and $SO(8)$ are treated in the following lemma. We do not give a proof here. The starting point of the proofs is contained in Lemmas 2.5 and 2.7. Recall that the subregular unipotent classes in $PSp(6)$ are parameterized by $F^\times/F^{\times 2}$. In $SO(8)$ there is a single subregular unipotent class.

Lemma 4.16. *Let $E/F$ be a ramified quadratic extension. Let $T$ belong to the stable conjugacy class of Cartan subgroups (in $G = Sp(6)$ or $SO(8)$) that splits over $E$ and is obtained by twisting the split Cartan subgroup by the longest element $w_-$ of the Weyl group.*

(1) *With appropriate normalizations, on the elements of the half-integral set of $Sp(6)$ in the Lie algebra of $T$, the stable Shalika germ for the subregular unipotent class indexed by the coset $F^{\times 2}$ has the form*

$$\gamma_0 + C_6(\tau_E(t)),$$

*where $\gamma_0$ is an elementary function of $t$ and $C_6(\tau_E(t))$ is the number of points on the elliptic curve obtained by replacing $t_i \in E$ by $\tau_i \in k$ in the curve of Lemma 2.5.*

(2) *With appropriate normalizations, the stable subregular Shalika germ on the half-integral set of $SO(8)$ has the form*

$$\gamma_1 + C_7(\tau_E(t)),$$

*where $\gamma_1$ is an elementary function of $t$ and $C_7(\tau_E(t))$ is the number of points on the elliptic curve obtained by replacing $t_i \in E$ by $\tau_i \in k$ in the curve of Lemma 2.7.*

## 5. The Unit Element of the Hecke Algebra

This section will analyze the orbital integrals of the unit element of the Hecke algebra on the group $SO(2n+1)$. Consider the stable orbital integral $D(\lambda t)\Phi^{st}(\exp(\lambda t), \mathbf{1}_K)$ of the unit element of the spherical Hecke algebra on $SO(2n+1)$ over the stable conjugacy class of $\exp(\lambda\, t)$, where $t$ belongs to the half-integral set. Let $E/F$ be a ramified quadratic extension, and let $C_2(\tau_E(t))$ be the number of points on the hyperelliptic curve of Equation 4.2.

THEOREM 5.1. *When $\lambda \in F^\times$ is sufficiently small, $D(\lambda t)\Phi^{st}(\exp(\lambda t), \mathbf{1}_K)$ is a linear combination of the functions*

$$1, \quad |\lambda|, \quad |\lambda| C_2(\tau_E(t)),$$

*and functions of higher degrees of homogeneity: $o(|\lambda|)$. In this linear combination, the coefficient of $|\lambda|C_2(\tau_E(t))$ is nonzero. In particular, the stable orbital integrals of the unit element of the Hecke algebra are not elementary on $SO(2n+1)$, for $n \geq 3$.*

A preliminary lemma must precede the proof. All subregular unipotent conjugacy classes in $SO(2n+1)$ lie in the same stable conjugacy class. We fix an invariant form on the stable subregular conjugacy class in $SO(2n+1)$. To be specific, let $e_{ij}$ denote the $(2n+1)\times(2n+1)$ matrix whose $ij$-coefficient is one, and whose other coefficients are zero. For every root $\gamma$, we fix a root vector $X_\gamma$ in the Lie algebra of $SO(2n+1)$ of the form $X_\gamma = e_{ij} - e_{i'j'}$, where $i > i'$. Let $\alpha_1$ denote the short simple root of $SO(2n+1)$. We endow a Zariski open set of the stable subregular unipotent class with coordinates by the equation $y^{-1}xy$, where

$$x = \prod_{\substack{\gamma\neq\alpha_1\\ \gamma>0}} \exp(x(\gamma)X_\gamma), \quad y = \prod_{\substack{\gamma\neq\alpha_1\\ \gamma>0}} \exp(y(\gamma)X_{-\gamma}), \quad \text{and } x(\gamma),\ y(\gamma) \in F. \tag{5.2}$$

(These products require a fixed linear order on the positive roots.)

An invariant measure on the stable subregular class is then $|\omega|$, where $\omega$ is the differential form

$$\bigwedge_{\gamma\neq\alpha_1} (dx(\gamma) \wedge dy(\gamma)).$$

This restricts to an invariant measure $\mu_a$, for $a \in F^\times/F^{\times\,2}$, on each subregular unipotent class. (Recall that the subregular unipotent classes in $SO(2n+1)$ are parameterized by $a \in F^\times/F^{\times\,2}$.)

LEMMA 5.3. *The integrals $\mu_a(\mathbf{1}_K)$ and $\mu_{a'}(\mathbf{1}_K)$ are equal for the two cosets $a, a'$ of odd valuation.*

PROOF. If $\theta : F^\times \to \mathbb{C}^\times$ is a quadratic character, let $\mu^\theta$ be the signed measure on the stable subregular conjugacy class given by

$$\mu^\theta = \sum_{a \in F^\times / F^{\times\, 2}} \theta(a)\mu_a.$$

To establish the lemma, it is enough to show that $\mu^\theta(\mathbf{1}_K) = \mu^{\theta'}(\mathbf{1}_K)$, if $\theta$ and $\theta'$ are the two ramified quadratic characters of $F^\times$. This we check by direct computation.

If $x$ is a subregular unipotent element of the form (5.2), then its conjugacy class has parameter

$$a = x(\alpha_1 + \alpha_2)^2 + 2x(\alpha_2)x(2\alpha_1 + \alpha_2) \text{ modulo } F^{\times\, 2},$$

where $\alpha_2$ is the long simple root adjacent to the short simple root $\alpha_1$. To see this, we recall how the parameterization is defined. The subregular unipotent class $\mathcal{O}_a$ with parameter $a$ has the characteristic property that every irreducible component of $\mathfrak{B}_u$, the variety of Borel subgroups containing a given unipotent element $u \in \mathcal{O}_a$, is defined over $F(\sqrt{a})$. More concretely $a$ is the discriminant (modulo squares) of the quadratic polynomial in $z$ determined by the condition

$$\exp(zX_{-\alpha_1})x \exp(-zX_{-\alpha_1}) \in N_2,$$

where we let $N_i$ denote the unipotent radical of the upper-block triangular parabolic subgroup associated with the short root $\alpha_i$. A short calculation shows that the quadratic polynomial is

$$z^2 x(2\alpha_1 + \alpha_2) + 2zx(\alpha_1 + \alpha_2) - 2x(\alpha_2) = 0,$$

whose discriminant gives $x(\alpha_1 + \alpha_2)^2 + 2x(\alpha_2)x(2\alpha_1 + \alpha_2)$ as desired.

According to the method of [**H4,3.9**], there is a constant $c$ independent of $\theta$, such that $\mu^{\theta,x} = c\mu^\theta$, where $\mu^{\theta,x}$ is the measure in Ranga Rao's normalization:

$$\mu^{\theta,x}(f) = \int_K \int_{N_1} f(k^{-1}xk)\theta(x(\alpha_1+\alpha_2)^2 + 2x(\alpha_2)x(2\alpha_1+\alpha_2)) \left| \prod_{\gamma \neq \alpha_1} dx(\gamma) \right| dk.$$

Here $dk$ is the Haar measure of mass one on the group $K = SO(2n+1, O_F)$.

We must check that $\mu^{\theta,x}(\mathbf{1}_K) = \mu^{\theta',x}(\mathbf{1}_K)$ for the two ramified characters $\theta, \theta'$ of order two on $F^\times$. For the unit of the Hecke algebra, the integral over $K$ is one, and the integral over each $|dx(\gamma)|$ is also one, for $\gamma \neq \alpha_1, \alpha_2, \alpha_1 + \alpha_2$, and $2\alpha_1 + \alpha_2$. We are left to show that the integral

$$\int_{|x|\le 1,\, |y| \le 1,\, |z| \le 1} \theta(x^2 + 2yz)|dx\, dy\, dz|$$

is independent of the ramified quadratic character $\theta$. This is an easy exercise that is left to the reader. Thus, our claim is established that $\mu_a(\mathbf{1}_K) = \mu_{a'}(\mathbf{1}_K)$ when $a$ and $a'$ are the two cosets of odd valuation. □

PROOF (THEOREM 5.1). The Shalika germ expansion of the stable orbital integral of the unit element of the Hecke algebra has the form

$$D(\lambda t)\Phi^{st}(\exp(\lambda t), \mathbf{1}_K) = \sum_{\mathcal{O}} \Gamma_{\mathcal{O}}(\lambda t)\mu_{\mathcal{O}}(\mathbf{1}_K),$$

where $\mathcal{O}$ ranges over the unipotent classes of $G$ and $t$ is half-integral in the Lie algebra of $G$. By [**HC**], the $r$-regular Shalika germs satisfy $\Gamma_{\mathcal{O}}(\lambda^2 t) = |\lambda|^{2r}\Gamma_{\mathcal{O}}(t)$, so the theorem calls for an analysis of the regular and subregular terms ($r = 0, 1$). By Shelstad [**Sh**], the stable regular Shalika germ is a constant, which with an appropriate normalization is simply the constant 1. Now consider the subregular terms. By the results of [**H3,VI.2**], we find that $\Gamma_{\mathcal{O}}(\lambda t) = |\lambda|\Gamma_{\mathcal{O}}(t)$ for the stable subregular germs of $SO(2n+1)$. By Lemma 4.8, each stable germ $\Gamma_{\mathcal{O}}(t)$ is a linear combination of the functions 1, $C_1(\tau_E(t))$, and $C_1(\tau_{E'}(t))$, where $E$ and $E'$ are distinct ramified quadratic extensions of $F$. The stable germs associated with the cosets $a, a'$ of even valuation are $\Gamma_a(\lambda t) = \Gamma_{a'}(\lambda t) = |\lambda|$. The cosets $a, a'$ of odd valuation give

$$\begin{aligned} &|\lambda|\Gamma_{\mathcal{O}_a}(t)\mu_a(\mathbf{1}_K) + |\lambda|\Gamma_{\mathcal{O}_{a'}}(t)\mu_{a'}(\mathbf{1}_K) \\ =&|\lambda|\mu_a(\mathbf{1}_K)(x_a C_1(\tau_E(t)) + x_{a'} C_1(\tau_{E'}(t))). \end{aligned}$$

The nonzero constants $x_a$ and $x_{a'}$ account for the different normalizations of measures. The normalization of $\Gamma_{\mathcal{O}_a}(t)$ comes from the measure $\mu_a$, and this is not the same as the normalization of Lemma 4.8.

The constants $x_a$ and $x_{a'}$ are equal. To see this, we must track down the constants of normalization that we have ignored in going from $\Gamma_{\mathcal{O}_a}$ to $C_1(\tau_E(t))$. In the proof of [**H5,1.2**], the constant $\frac{1}{2}\int |d\xi/\xi|$ was discarded, where $\int |d\xi/\xi|$ is the integral over the elements in $F(\sqrt{a})$ of norm one. This integral is $2/q$ for every ramified extension. The constant $-1/q$ in the statement of Lemma 4.7 was discarded in the proof of Lemma 4.8. There is also a factor of $\sqrt{q}$ in the proof of Lemma 4.8 arising from a change of coordinates: $u = x/\pi_E$, and $\sqrt{q}|du/u^2| = |dx/x^2|$. No other constants were dropped.

With $x_a = x_{a'}$, Equation 4.12 shows that the term coming from cosets of odd valuation is

$$2|\lambda| C_2(\tau_E(t)) x_a \mu_a(\mathbf{1}_K).$$

Finally, we note that the constant $x_a\mu_a(\mathbf{1}_K)$ is nonzero. In fact, the factor $\mu_a(\mathbf{1}_K)$ is positive, being the positive measure of a characteristic function on the orbit $\mathcal{O}_a$. The conclusion follows. □

## 6. Fourier Transforms and Characters

Results of Arthur, Harish-Chandra, and Kazhdan allow us to draw some conclusions about characters and Fourier transforms of invariant measures supported on nilpotent orbits from our work on stable Shalika germs.

Harish-Chandra has shown that the Fourier transform $\hat{\mu}_{\mathcal{O}}$ of the invariant measure on a nilpotent conjugacy class $\mathcal{O}$ is represented by a locally integrable function that is locally constant on the regular semisimple set [**HC**]. Let $T_X$ be the Cartan subgroup corresponding to a given regular elliptic element $X$, and let $A$ be the split component of $G$. Let $\mathrm{vol}(T_X/A)$ be the volume of $T_X/A$ computed with respect to the measure used to define the algebraic measure on $G/T$ used to compute Shalika germs in [**L**].

On the regular elliptic set, these Fourier transforms are related to the unstable Shalika germs $\Gamma^{un}_{\mathcal{O}}(X)$ and discriminant $D(X)$ by the identity [**HC**]

$$\sum_{\mathcal{O}} D(X)\hat{\mu}_{\mathcal{O}}(X)\Gamma^{un}_{\mathcal{O}}(Y)\,\mathrm{vol}(T_Y/A) = \sum_{\mathcal{O}} D(Y)\hat{\mu}_{\mathcal{O}}(Y)\Gamma^{un}_{\mathcal{O}}(X)\,\mathrm{vol}(T_X/A), \tag{6.1}$$

($X, Y$ regular elliptic), where the sum runs over nilpotent conjugacy classes. (It is harmless to shift the indexing set back and forth from nilpotent classes to unipotent classes.) We view this equation as giving for each $Y$ a linear relation between Fourier transforms and the Shalika germs on the elliptic set.

A *cuspidal* linear combination of Shalika germs $\sum x_{\mathcal{O}}\Gamma^{un}_{\mathcal{O}}(X)$ is defined to be a linear combination that vanishes on all nonelliptic elements. Kazhdan has shown that the space of cuspidal linear combinations of Shalika germs coincides with the span of Fourier transforms of nilpotent orbits [**K**]. For every regular elliptic $Y$, the right-hand side of Equation 6.1 is a cuspidal linear combination of Shalika germs, and as $Y$ varies, we span the space of cuspidal linear combinations of Shalika germs. In other words, Harish-Chandra's identity (6.1) gives a transition matrix from one spanning set of functions to another. As a result, if cuspidal linear combinations of Shalika germs are not elementary, then neither are certain Fourier transforms.

Results showing that Fourier transforms of nilpotent orbits are not elementary carry over to characters of admissible representations. Harish-Chandra proved that every character $\chi_\pi$ of an irreducible admissible representation of a reductive $p$-adic group has an expansion parameterized by nilpotent orbits $\mathcal{O}$

$$\chi_\pi(\exp(X)) = \sum_{\mathcal{O}} c_{\mathcal{O}}(\pi)\hat{\mu}_{\mathcal{O}}(X), \tag{6.2}$$

for some collection of constant $c_{\mathcal{O}}(\pi)$ whenever the regular semisimple element $X$ is sufficiently small. If a nilpotent orbit $\hat{\mu}_{\mathcal{O}'}(X)$ is known not to be elementary, then the local expression for $\chi_\pi(\exp(X))$ is not elementary either except in the degenerate cases when the particular coefficients $c_{\mathcal{O}}(\pi)$ cancel the nonrational behavior from Equation 6.2. Although cancellation may occur for particular representations, it cannot happen in general because Equation 6.2 may be inverted.

LEMMA 6.3. *Assume the center of $G(F)$ is compact. Each Fourier transform of an invariant nilpotent measure is, on the regular elliptic set, a finite linear* *combination of irreducible admissible characters:*

$$\hat{\mu}_{\mathcal{O}}(X) = \sum_{\pi} \hat{c}_{\mathcal{O}}(\pi)\chi_{\pi}(\exp(X)),$$

*for $X$ sufficiently small.*

Proof. Kazhdan [**K,§2**] proves that there is a cuspidal function $f$ whose orbital integrals on the regular elliptic set equal $\hat{\mu}_{\mathcal{O}}(X)$. Arthur [**A,5.1**] has used the local trace formula to express the orbital integrals of a cuspidal function as a linear combination of elliptic characters (again on the regular elliptic set). These two results combine to give the lemma. □

Thus, the nonrationality of cuspidal linear combinations of Shalika germs implies that characters admit no general elementary description. A cuspidal linear combinations of subregular Shalika germs is identically zero – except when the rank of the group is small. As a result, other unipotent classes must be studied to prove general nonrationality results for characters. Nevertheless, the subregular Shalika germs give nonrationality results for the characters on some groups of small rank, and it is worthwhile to consider these examples.

Our first example will be the group $G = SO(5)$. Let $C_3(\tau_E(t))$ denote the number of points on the elliptic curve of Equation 4.3, with $t = [t_1, t_2]$ in the half-integral set.

Theorem 6.4. *Fix any ramified quadratic extension $E/F$. The space of Fourier transforms of subregular nilpotent classes in $SO(5)$ restricted to the elliptic set is two-dimensional. A basis of this space on the half-integral set is given by the two functions*

$$A_T, \qquad A_T C_3(\tau_E(t)),$$

*for some collection of nonzero constants $A_T$ depending only on the stable conjugacy class of Cartan subgroups $T$ containing (a conjugate of) $t$.*

Corollary. *The characters of admissible representations of $SO(5)$ (and $GSp(4)$, $Sp(4)$, and so forth) are not elementary in general.*

Proof. The local character expansion on the half-integral set will in general contain the term $C_3(\tau_E(t))$ of Theorem 6.4. □

If we select a different ramified extension $E'$, we obtain a different function $C_3(\tau_{E'}(t))$, but the vector space spanned remains unchanged.

The discriminant factor $D(X)$ is constant on the half-integral set, so that it does not matter whether we include it or not in the normalizations of the Fourier transforms.

Murnaghan [**M1**] has identified a family of supercuspidal representations on $GSp(4)$ for which the the local character expansions are elementary. The subregular term of this family lies in the one-dimensional subspace $(A_T)$ of the two-dimensional space of the theorem.

Proof (Theorem 6.4). We write the four Shalika germs of subregular unipotent elements as $\bar\Gamma_1^{un}$, $\bar\Gamma_\epsilon^{un}$, $\bar\Gamma_\pi^{un}$, and $\bar\Gamma_{\pi\epsilon}^{un}$, using the representatives 1, $\epsilon$, $\pi$, and $\pi\epsilon$ of cosets $F^\times/F^{\times\,2}$. The bar indicates that we are using the normalization of [**H5**] (compare Lemma 4.10). The superscript *un* reminds us that we are now using ordinary (unstable) Shalika germs, and no longer the stable germs used throughout Sections 4 and 5. We write $\bar\Gamma_a^{T,\kappa}$ for the $\kappa$-combination of Shalika germs on the restriction to a particular Cartan subgroup $T$, for any character $\kappa$ of the cohomology group $H^1(\mathrm{Gal}(\bar F/F),T)$.

Suppose that we have a cuspidal linear combination of Shalika germs

$$\sum_a x_a \bar\Gamma_a^{un}.$$

Each $\kappa$-combination of Shalika germs is a linear combination of unstable Shalika germs. Thus, cuspidality implies that

$$\sum x_a \bar\Gamma_a^{T,\kappa} = 0, \tag{6.5}$$

for every nonelliptic Cartan subgroup $T$ and every $\kappa$. Since each unstable Shalika germ is a linear combination of the $\kappa$-germs, we see that Condition 6.5 for all $(T,\kappa)$ implies cuspidality.

The stable germs of $SO(5)$ are given in Equation 4.9. The split torus $T$ gives no constraints on cuspidality. Suppose first that $T$ is a product $T_1 \times T_2$, with parameter $t_i$ in the Lie algebra of $T_i$, for $i = 1,2$. In this case $T$ has an endoscopic group $SO(3)\times SO(3)$ (and this is the only nontrivial endoscopic group of $SO(5)$), so we may consider $\kappa$-orbital integrals. Let $\Delta^{T,\kappa}$ be the transfer factor of Langlands and Shelstad, which we write as a function of $t_1$ and $t_2$. The transfer to the endoscopic group (proved in [**H1,5.25**] and [**H1,page 243,Cor3**]) forces each germ $\Delta^{T,\kappa}\bar\Gamma_a^{T,\kappa}$ to be a linear combination of $\bar\Gamma_a(t_1,0)$ and $\bar\Gamma_a(t_2,0)$, where $\bar\Gamma_a(t_1,0)$ is equal up to a constant to the integral of Equation 4.9, specialized to $t_2 = 0$, and similarly for $\bar\Gamma_a(t_2,0)$. The constants relating the normalizations $\bar\Gamma_a$ and $\Gamma_a$ are given in [**H5,§2**]. Looking at the two extreme cases – first when $T_1$ is split, then when $T_2$ is split – we find that $\Delta^{T,\kappa}\bar\Gamma_a^{T,\kappa} = \bar\Gamma_a(t_1,0) + \bar\Gamma_a(t_2,0)$. As [**H5,2.3**] points out, the integral $\bar\Gamma_a(t_i,0)$ is independent of $a$. This is, in fact, the purpose of shifting to the normalization $\bar\Gamma_a$. Thus, the given linear combination $\sum_a x_a\bar\Gamma_a^{T,\kappa}$ becomes

$$(x_1 + x_\epsilon + x_\pi + x_{\pi\epsilon})(\bar\Gamma_a(t_1,0) + \bar\Gamma_a(t_2,0))/\Delta^{T,\kappa}(t_1,t_2).$$

The vanishing condition of cuspidality forces $x_1 + x_\epsilon + x_\pi + x_{\pi\epsilon} = 0$. But when this sum is zero, the $\kappa$-germ vanishes on all Cartan subgroups (associated with the endoscopic group) – not just the nonelliptic ones. It follows that the cuspidal linear combinations of Shalika germs are essentially stable: on each Cartan subgroup, the unstable germ is a multiple (determined by the number

$h_T$ of conjugacy classes in the stable class) of the stable germ. Thus, we may drop the superscripts *un* and work directly with stable germs.

The constraint $\sum_a x_a = 0$ comes from one of the parabolic subgroups. The constraint for the other proper parabolic subgroup comes from the duality of [**H5,2.1**]. This condition is $x_1 = 0$. The cuspidal linear combinations are made up of the two-dimensional space

$$(x_\epsilon \bar\Gamma_\epsilon + x_\pi \bar\Gamma_\pi + x_{\pi\epsilon}\bar\Gamma_{\pi\epsilon})/h_T, \quad \text{with } x_\epsilon + x_\pi + x_{\pi\epsilon} = 0.$$

By the explicit results of [**H5,§2**] and Equation 6.1, this gives an explicit basis for the Fourier transforms of subregular orbits on elliptic elements. By [**H5,2.8**], the germ $\bar\Gamma_\epsilon$ is identically zero on the half-integral set, giving us arbitrary linear combinations of $\bar\Gamma_\pi$ and $\bar\Gamma_{\pi\epsilon}$. The theorem now follows from Equations 4.12 and 4.13. The curve of Equation 4.2 has genus zero in rank two. It follows that the term $C_2(\tau_E(t))$ appearing in Equation 4.12 is independent of $t$. This gives the desired basis. The constants $A_T$ are $A_T = \mathrm{vol}(T/A)/h_T$, where $h_T \in \{1,2\}$ is the number of conjugacy classes of Cartan subgroups in the stable conjugacy class of $T$. □

We give one more example. Consider the group $G = U_E(3)$ split over a ramified quadratic extension $E/F$. There are two subregular unipotent conjugacy classes, parameterized by $F^\times$ modulo the norms of $E$. Let $\eta$ be the ramified quadratic character of $F^\times$ associated with $E/F$.

THEOREM 6.6. *The Fourier transforms of subregular nilpotent measures on $U_E(3)$ span a two dimensional space on elliptic elements. A basis of this space on the half-integral set is formed by the functions*

$$A_T\, \eta((t_1 - t_2)(t_2 - t_3)) \quad \textit{and } B_T\,(1 + q - C_5(\tau_E(t))),$$

*where $C_5(\tau_E(t))$ is the number of points on the elliptic curve $\epsilon y^2 = (x+\tau_1)(x+\tau_2)(x+\tau_3)$ of Equation 4.5. The constants $A_T$ and $B_T$ depend only on the conjugacy class of Cartan subgroup containing the given half-integral element. The constant $A_T$ is nonzero if and only if $T$ is stably conjugate to a Cartan subgroup in*

$$H = \left\{ \begin{pmatrix} * & & * \\ & * & \\ * & & * \end{pmatrix} \right\}.$$

*The constant $B_T$, defined for every elliptic Cartan subgroup $T$ meeting the half-integral set, is nonzero for every such $T$. If $T$ and $T'$ are stably conjugate but not conjugate, then $A_T + A_{T'} = 0$ and $B_T = B_{T'}$.*

Corollary. *The characters of representations on $U_E(3)$ are not in general elementary.*

Proof. This follows easily from the results of [**H2**]. We sketch the argument. There is only one nonelliptic Cartan subgroup up to conjugacy, and all subregular orbital integrals vanish on it. Thus, every subregular germ is cuspidal, and the subregular cuspidal space is two-dimensional.

There are either one or two conjugacy classes of Cartan subgroups in the stable conjugacy class of $T$. If there is only one, then there is no difference between the unstable germ and the stable germ. We obtain the lemma in this case from Lemma 4.15 with $A_T = 0$.

If there are two conjugacy classes, then $H$ is the endoscopic group. If $t'$ is stably conjugate (but not conjugate) to $t$, we set $\Gamma_a^{T,st}(t) = \Gamma_a^{un}(t) + \Gamma_a^{un}(t')$ and $\Gamma_a^{T,\kappa}(t) = \Gamma_a^{un}(t) - \Gamma_a^{un}(t')$, for $t \in Lie(H)$. The germ is expressed in terms of the $\kappa$-germs as $\Gamma_a^{un}(t) = \frac{1}{2}(\Gamma_a^{T,st}(t) + \Gamma_a^{T,\kappa}(t))$. Multiplying $\Gamma_a^{T,\kappa}$ by the transfer factor $\eta((t_1 - t_2)(t_2 - t_3))$ of [**H2,2.1**] and transferring the $\kappa$-germ to the endoscopic group, we find that $\eta((t_1 - t_2)(t_2 - t_3))\Gamma_a^{T,\kappa}(t)$ is equal to the stable germ on $H$, which is a constant $A_T$ on the half-integral set [**Shk,2.2.2**]. Clearly $\Gamma_a^{T,\kappa}(t') = -\Gamma_a^{T,\kappa}(t)$, if $t$ and $t'$ are stably conjugate but not conjugate. Thus, $A_T + A_{T'} = 0$. Also $\Gamma_a^{T,\kappa} = \Gamma_{a'}^{T,\kappa}$ with the normalizations of [**H2,§5**].

The stable germ $\Gamma_a^{T,st}$ is given by Lemma 4.15. With the normalizations of [**H2,§5**], the two subregular stable germs differ by the sign $\eta(x(\gamma))$ (appearing in the proof of Lemma 4.15). The sign is positive on one of the subregular classes and negative on the other. Hence $\Gamma_a^{T,st} + \Gamma_{a'}^{T,st} = 0$. Finally

$$\Gamma_a^{un}(t) + \Gamma_{a'}^{un}(t) = \Gamma_a^{T,\kappa}(t) = A_T\eta((t_1 - t_2)(t_2 - t_3))$$

and $\Gamma_a^{un}(t) - \Gamma_{a'}^{un}(t) = \Gamma_a^{T,st}(t) = B_T(1 + q - C_5(\tau_E(t)))$ as desired. □

## 7. Proofs and Conclusion

The proofs of Theorems 1.1, 1.2, and 1.3 are now nearly complete. Lemma 6.3, Theorem 6.4, and Theorem 6.6 prove that there is no general elementary formula for the Fourier transform of nilpotent orbits, and that there is no general elementary formula for characters. Sections 4 and 5 treat Shalika germs and the unit element of the Hecke algebra.

To prove that the Langlands principle of functoriality is not elementary, we rely on the main example of [**H5**]. The embedding of $L$-groups

$$^LSO(5) = Sp(4, \mathbb{C}) \to GL(4, \mathbb{C}) = {}^LGL(4)$$

leads to conjectures relating twisted stable characters on $GL(4, F)$ and stable characters on $SO(5, F)$ (see [**KS1**]). Expressed dually in terms of orbital integrals, the twisted orbital integrals on $GL(4)$ should be related to stable orbital integrals on $SO(5)$. Concrete calculations on the half-integral set of $GL(4)$ give points on the elliptic curve

$$y_1^2 = 1 + ax_1^2 + bx_1^4, \quad \text{for } a, b \in k,$$

over the residue field $k$ of $F$. On $SO(5)$, we find the elliptic curve

$$y_2^2 = 1 - 2ax_2^2 + (a^2 - 4b)x_2^4, \quad \text{for } a, b \in k.$$

For details see [**H5,2.8**]. These curves have different $j$-invariants. The theory of endoscopy then predicts that these two elliptic curves have the same number of points. This follows from the pair of dual isogenies between the curves:

$$\begin{aligned} \phi^* x_2 &= x_1/y_1, \qquad & \phi^* y_2 &= (1 - bx_1^4)/y_1^2, \\ \psi^* x_1 &= 2x_2/y_2, \qquad & \psi^* y_1 &= (1 - (a^2 - 4b)x_2^4)/y_2^2. \end{aligned}$$

The theory of endoscopy and functoriality, formulated as correspondences between varieties over finite fields, will be a vast generalization of this pair of dual isogenies. We conclude the principle of functoriality is not generally elementary. The proof of Theorem 1.1 is now complete.

Turn to the proofs of Theorems 1.2 and 1.3. The stable invariant theory on the quasisplit groups $SU_E(n)$ for $n \geq 3$, $Sp(2n)$ for $n \geq 2$ (assuming transfer), and $SO(2n+1)$, for $n \geq 2$, is not elementary by the results of Section 4. The inner forms of $SO(2n+1)$ and of $SU_E(2k)$ do not have elementary theories because of [**H3,VII.4.1**], which asserts that the stable subregular Shalika germs are affected only by a sign in passing to the inner form. The groups $Sp(6)$ and $SO(8)$ are treated in Lemma 4.16.

For the quasisplit form of the group $SO(2n)$, for $n \geq 5$, we make use of the standard endoscopic group $H$ that is a quasisplit form of $SO(8) \times SO(2n-8)$, with $SO(8)$ split. (see [**H5,VII.1.4**]). The following lemma will complete the proof of Theorems 1.2 and 1.3.

LEMMA 7.1. *Assume the transfer of Shalika germs from the quasisplit forms $G_{adj}$ of $SO(2n)$ to the endoscopic group $H$ given above. Then the Shalika germs of $\kappa$-orbital integrals of $SO(2n)$ on the half-integral set are not in general elementary.*

PROOF. There is a single subregular conjugacy class in $G_{adj}$, for $n \geq 3$. The transfer of germs implies that the $\kappa$-combinations of subregular germ, multiplied by the Langlands-Shelstad transfer factor [**LS**], is a linear combination of stable germs on the endoscopic groups. Since $H$ is a product, the stable subregular germs on $H$ are linear combinations of the stable subregular germs on the two factors $SO(8)$ and $SO(2n-8)$. To determine the particular linear combination that arises in the transfer, we look at the Cartan subgroups in the Levi factors $\mathbb{G}_m^{n-4} \times SO(8)$ and $SO(2n-8) \times \mathbb{G}_m^4$. For such Cartan subgroups, the $\kappa$-combination is already stable, the Langlands- Shelstad transfer factor is one (since the discriminant has already been removed), and the transfer to the endoscopic group degenerates to ordinary Levi descent. From this, we see that the transfer gives a *nontrivial* linear combination of the stable subregular germs on $SO(8)$ and $SO(2n-8)$. In particular, the stable subregular germ of $SO(8)$ contributes a nonzero term to the $\kappa$-orbital integrals on $G$. The other term coming from $SO(2n-8)$ cannot cancel this, because they are functions of independent sets of parameters in the Lie algebra. By Lemma 4.16, the Shalika germ is not elementary on the half-integral set of $SO(8)$. Thus, it cannot be elementary on $SO(2n)$ either. □

---

Objects such as the Fourier transform of nilpotent orbits, Shalika germs, orbital integrals (especially the orbital integrals of the unit element of the Hecke algebra) have been studied extensively, and many interrelationships between these basic objects have been obtained. Yet despite persistent efforts, explicit formulas have been produced for these objects only in special cases such as $GL(n)$, and we are led to suspect that the general theory is profoundly different from these special cases.

Experts have long harbored vague feelings that harmonic analysis on reductive $p$-adic groups is not elementary. This paper quantifies some of the complexities long felt to exist and explains why previous efforts have encountered such difficulty: certain methods treat invariant harmonic analysis as a rational theory, and have only been successful for *rational groups*. Any approach to harmonic analysis on $p$-adic groups that is not equipped to deal with nonrational geometry is ill-fated.

The principle of functoriality, as envisioned by Langlands and elaborated by many, predicts relationships between the basic objects of invariant harmonic analysis of pairs of reductive groups whose $L$-groups are related. To the extent that these basic objects are described by varieties over finite fields, we may reformulate the principle of functoriality geometrically and seek to prove it by geometrical methods.

This paper has given a series of examples of nonrational varieties arising in harmonic analysis. These results are tentative in the sense that the fundamental problems in this nascent theory remain largely unformulated and yet unsolved. I conclude with three problems that I see as essential to the future progress of harmonic analysis on $p$-adic groups. First, to establish the proper foundations for this theory, some general structure theorems are required. For example, give general arguments that show that the basic objects of invariant harmonic analysis are described by the number of points on varieties over finite fields. Second, identify the family of varieties attached to a given group. The examples of the paper involve hyperelliptic curves. What other nonrational varieties arise

– if any? Third, produce the morphisms or correspondences of varieties predicted by the principle of functoriality. The isogeny of elliptic curves described in this section should be an isolated example within a much larger theory yet to be developed.

## Appendix

In this appendix, we list some rational functions that are used in Example 2.3. These rational functions give an elliptic curve. We follow the notation of Example 2.3 for the group $Sp(6)$. A symbolic computer calculation shows that on $S^*(k_1^-)$ we have $\sigma_-(x) = X(x,y)$ and $\sigma_-(y) = Y(x,y)$, where

$$X(x,y) - x = \frac{(t_2+t_3)yb_1}{b_2b_3}, \qquad Y(x,y) - y = \frac{yb_1b_4}{b_2b_5b_6},$$

and

$$\begin{aligned}
b_1 &= -2t_1^2x^2 + 4t_1t_2x^2 - 2t_2^2x^2 + 4t_1^2x^3 - 8t_1t_2x^3 + 4t_2^2x^3 - 2t_1^2x^4 + 4t_1t_2x^4 \\
&\quad - 2t_2^2x^4 - 3t_1^2xy + 4t_1t_2xy - t_2^2xy + t_1t_3xy - t_2t_3xy + 6t_1^2x^2y \\
&\quad - 12t_1t_2x^2y + 6t_2^2x^2y - 3t_1^2x^3y + 8t_1t_2x^3y - 5t_2^2x^3y - t_1t_3x^3y + t_2t_3x^3y \\
&\quad - t_1^2y^2 + t_1t_2y^2 + t_1t_3y^2 + 2t_1^2xy^2 - 6t_1t_2xy^2 + 2t_2^2xy^2 - t_1^2x^2y^2 \\
&\quad + 5t_1t_2x^2y^2 - 4t_2^2x^2y^2 - t_1t_3x^2y^2 + 2t_2t_3x^2y^2 - t_1t_2y^3 \\
&\quad + t_1t_2xy^3 - t_2^2xy^3 + t_2t_3xy^3, \\
b_2 &= -t_1^2x + 2t_1t_2x - t_2^2x + t_1^2x^2 - 2t_1t_2x^2 + t_2^2x^2 - t_1^2y + t_1t_2y \\
&\quad + t_1^2xy - 2t_1t_2xy + t_2^2xy + t_1t_3xy - t_2t_3xy - t_1t_2y^2 - t_2t_3y^2, \\
b_3 &= -t_1x + t_2x + t_1x^2 - t_2x^2 - t_1y + t_1xy - t_2xy + t_3xy + t_3y^2, \\
b_4 &= -t_1^2x + 2t_1t_2x - t_2^2x + t_1^2x^2 - 2t_1t_2x^2 + t_2^2x^2 - t_1^2y + t_1t_2y + t_1^2xy \\
&\quad - 2t_1t_2xy + t_2^2xy + t_1t_3xy - t_2t_3xy + t_1t_3y^2 + t_3^2y^2, \\
b_5 &= -t_1x + t_2x + t_1x^2 - t_2x^2 - t_1y + t_1xy - t_2xy + t_3xy, \\
b_6 &= -t_1x + t_2x + t_1x^2 - t_2x^2 - t_1y + t_1xy - t_2xy + t_3xy + t_3y^2.
\end{aligned}$$

It is clear that $b_i = 0$ defines a rational curve for $i \neq 1$. The polynomial $b_1$ becomes, under the substitution $x = 1 - y/x_1$, the product of $y^2/x_1^4$ and the polynomial

$$\begin{aligned}
b_1' &= -2t_1^2x_1^2 + 4t_1t_2x_1^2 - 2t_2^2x_1^2 - 4t_1t_2x_1^3 + 4t_2^2x_1^3 + 2t_1t_3x_1^3 - 2t_2t_3x_1^3 - 2t_2^2x_1^4 \\
&\quad + 2t_2t_3x_1^4 + 4t_1^2x_1y - 8t_1t_2x_1y + 4t_2^2x_1y - 3t_1^2x_1^2y + 12t_1t_2x_1^2y - 9t_2^2x_1^2y \\
&\quad - 3t_1t_3x_1^2y + 3t_2t_3x_1^2y - 4t_1t_2x_1^3y + 6t_2^2x_1^3y + 2t_1t_3x_1^3y - 4t_2t_3x_1^3y - t_2^2x_1^4y \\
&\quad + t_2t_3x_1^4y - 2t_1^2y^2 + 4t_1t_2y^2 - 2t_2^2y^2 + 3t_1^2x_1y^2 - 8t_1t_2x_1y^2 + 5t_2^2x_1y^2 \\
&\quad + t_1t_3x_1y^2 - t_2t_3x_1y^2 - t_1^2x_1^2y^2 + 5t_1t_2x_1^2y^2 - 4t_2^2x_1^2y^2 - t_1t_3x_1^2y^2 \\
&\quad + 2t_2t_3x_1^2y^2 - t_1t_2x_1^3y^2 + t_2^2x_1^3y^2 - t_2t_3x_1^3y^2.
\end{aligned}$$

This polynomial is quadratic in $y$. By completing the square it may be brought into the form $y_1^2 - f(x_1)$. The resulting elliptic curve is given in the proof of Lemma 2.5.

## References


[A] J. Arthur, *On Elliptic Tempered Characters*, Acta Mathematica **171** (1993), 73–138.

[BDKV] J. Bernstein, P. Deligne, D. Kazhdan and M.-F. Vignéras, *Représentations des groupes réductifs sur un corps local*, Hermann, Paris, 1984.

[CH] L. Corwin, and R. Howe, *Computing characters of tamely ramified $p$-adic division algebras*, Pacific. J. Math. **73** (1977), 461–477.

[CS] L. Corwin, and P. Sally, *Discrete Series Characters for Division Algebras and $GL_n$*, in preparation.

[D1] J. Denef, *On the Degree of Igusa's Local Zeta Function*, Amer. J. Math. **109** (1987), 991–1008.

[D2] J. Denef, *Report on Igusa's Local Zeta Function*, n° 741, Séminaire Bourbaki (1990–1991).

[H1] T. Hales, *Shalika Germs on $GSp(4)$*, Astérisque **171–172** (1989), 195–256.

[H2] T. Hales, *Orbital integrals on $U(3)$*, The Zeta Function of Picard Modular Surfaces (R. Langlands and D. Ramakrishnan, eds.), CRM, 1992.

[H3] T. Hales, *The Subregular Germ of Orbital Integrals*, vol. 476, Memoirs AMS, 1992.

[H4] T. Hales, *Unipotent orbits and unipotent representations on $SL(n)$*, Amer. J. Math. **115:6** (1993), 1347–1383.

[H5] T. Hales, *The Twisted Endoscopy of $GL(4)$ and $GL(5)$ : Transfer of Shalika germs*, Duke Math. J. (1994) (to appear).

[HC] Harish-Chandra, *Admissible invariant distributions on reductive $p$-adic groups*, Queen's Papers in Pure and Applied Math. **48** (1978), 281–347.

[Ho] R. Howe, *The Fourier Transform and Germs of Characters (Case of $GL_n$ over a $p$-adic Field)*, Math. Ann. **208** (1974), 305-322.

[I] J.-I. Igusa, *Lectures on forms of higher degree*, Tata Institute of Fundamental Research, Bombay, 1978.

[KLB] D. Kazhdan, and G. Lusztig, *Fixed Point Varieties on Affine Flag Manifolds*, Appendix by J. Bernstein and D. Kazhdan, *An example of a non-rational variety $\hat{\mathfrak{B}}_N$ for $G = Sp(6)$*, Israel Journal of Math. **62:2** (1988), 129–168.

[K] D. Kazhdan, *Cuspidal Geometry of $p$-adic Groups*, J. d'Analyse Math. **47** (1986), 1-36..

[KS1] R. Kottwitz, and D. Shelstad, *Twisted Endoscopy I: Definitions, Norm Mappings and Transfer Factors*, preprint.

[KS2] R. Kottwitz, and D. Shelstad, *Twisted Endoscopy II: Basic Global Theory*, preprint.

[L] R. Langlands, *Orbital Integrals on Forms of $SL(3)$, I*, Amer. J. Math (1983), 465–506.

[LS] R. Langlands, and D. Shelstad, *On the Definition of Transfer Factors*, Math. Ann. **278** (1987), 219–271.

[M1] F. Murnaghan, *Asymptotic behaviour of supercuspidal characters of $p$-adic $GSp(4)$*, Comp. Math. **80** (1991), 15–54.

[M2] F. Murnaghan, *Local character expansions and Shalika germs for $GL(n)$*, preprint.

[Shk] J. Shalika, *A theorem on semi-simple $\mathfrak{p}$-adic groups*, Annals of Math. **95** (1972), 226–242.

[Sh] D. Shelstad, *A formula for regular unipotent germs*, Astérisque **171–172** (1989), 275–277.

[W1] J.-L. Waldspurger, *Sur les intégrales orbitales tordues pour les groupes linéairies: un lemme fondamental*, Canad. J. Math **43:4** (1991), 852-896.

[W2] J.-L. Waldspurger, *Quelques résultats de finitude concernant les distributions invariantes sur les algèbres de Lie $p$-adiques*, preprint.

[W3] J.-L. Waldspurger, *Homogénéité de certaines distributions sur les groupes $p$-adiques*, preprint.



Department of Mathematics, University of Michigan, Ann Arbor, Michigan

*E-mail address*: hales@math.lsa.umich.edu