

VIRTUAL TRANSFER FACTORS

JULIA GORDON AND THOMAS C. HALES

ABSTRACT. The Langlands-Shelstad transfer factor is a function defined on some reductive groups over a p -adic field. Near the origin of the group, it may be viewed as a function on the Lie algebra. For classical groups, its values have the form $q^c \text{sign}$, where $\text{sign} \in \{-1, 0, 1\}$, q is the cardinality of the residue field, and c is a rational number. The sign function partitions the Lie algebra into three subsets. This article shows that this partition into three subsets is independent of the p -adic field in the following sense. We define three universal objects (virtual sets in the sense of Quine) such that for any p -adic field F of sufficiently large residue characteristic, the F -points of these three virtual sets form the partition.

The theory of arithmetic motivic integration associates a virtual Chow motive with each of the three virtual sets. The construction in this article achieves the first step in a long program to determine the (still conjectural) virtual Chow motives that control the behavior of orbital integrals.

0. INTRODUCTION

0.1. The Langlands-Shelstad transfer factor. Langlands and Shelstad have introduced a function, called the *transfer factor*, on certain reductive groups over a p -adic field. The definition of the transfer factor involves the theory of endoscopy and various constructs of local class field theory.

The transfer factor is expected to figure prominently in the development of the Langlands program. The *fundamental lemma*, a conjectural system of identities between orbital integrals, is expressed by means of transfer factors. A proof of the fundamental lemma is needed for many applications of the trace formula.

The definition of the transfer factor has been simplified in special contexts by Hales [6], Kottwitz [8], and Waldspurger [14]. This article follows Waldspurger's treatment of transfer factors and draws heavily from [14]. He gives a simple definition of transfer factors in the special case of classical groups defined by quadratic or hermitian forms. He makes mild restrictions on the characteristic of the residue field. Near the identity element of the group, the transfer factor can be expressed as a function on the Lie algebra. Waldspurger gives an elementary definition of the transfer factor as a function on the Lie algebra. He proves that it is equivalent to the Langlands-Shelstad definition ([14, X]). The list of classical Lie algebras that we consider appears in Section 1.3. Waldspurger's definition will be recalled in Section 2.2.

Received by the editors December 6, 2002.

2000 *Mathematics Subject Classification*. Primary 11F85, 22E50.

©2003 Julia Gordon and Thomas C. Hales

In the case of the transfer factors that we consider, each value of the transfer factor is of the form

$$q^c \text{ sign},$$

where $\text{sign} \in \{-1, 0, 1\}$, q is the order of the residue field, and c is a rational number. The definition of the rational number c is elementary, given as the valuation of a certain explicit discriminant factor. The entire complexity of the transfer factor resides in its sign.

The main purpose of this article is to show that the Langlands-Shelstad transfer factor on the classical Lie algebras is given by a formula in the first order language of rings. At first glance, the result may appear to be obvious. (Can we not view the Langlands-Shelstad definition as a formula for the transfer factor?) The force of our result comes from the restrictive nature of the language we use. Most of the fundamental structures of p -adic analysis cannot be expressed in this language. In this language, there are no field extensions or residue fields, no Galois theory or local class field theory, no functions apart from addition and multiplication, no additive or multiplicative characters, no valuation or norm, and no uniformizing elements. In fact, there are no sets at all in this language. It is remarkable that the Langlands-Shelstad transfer factor can be expressed without any reference to Zermelo Fraenkel set theory.

Set theory is so entrenched in our usual way of talking about harmonic analysis on p -adic groups, that we are forced to make a long series of preliminary statements about the “set-free” definition of standard constructs such as Lie algebras, centralizers, orbits of elements, linear spaces, bases, norms, projection operators, and so forth.

The theory of arithmetic motivic integration allows us to associate a Chow motive over \mathbb{Q} to formulas in the first order language of rings. In this way, we show that the Langlands-Shelstad transfer factor is *motivic* in the sense of Section 1.11. The construction in this article achieves the first step in a lengthy program to determine the (still conjectural) virtual Chow motives that control the behavior of orbital integrals. The influence of Denef and Loeser’s work on motivic integration should be apparent throughout this article [1].

0.2. The first order language of rings. The first order language of rings is a formal language in the first order predicate calculus. The concepts of logic and model theory that we require in this article can be found in Enderton [2] or Fried and Jarden [3]. In brief, each element of a language is a finite sequence of letters from a fixed alphabet. The letters of the alphabet include countably many variable symbols x_i , constants symbols c_k indexed by a set K , symbols for equality, negation, disjunction, existential quantification, comma, parentheses, and brackets:

$$= \quad \neg \quad \vee \quad \exists \\ , \quad (\quad) \quad [\quad] .$$

There are additional letters in the alphabet for each of a specified set of function symbols and relation symbols. The finite sequences in the language are called expressions. For a finite sequence of letters in the alphabet to belong to the language, it must satisfy various syntactic constraints. The syntax is built in stages: symbols combine in terms, terms combine into atomic formulas, atomic formulas combine into formulas.

In the case of the first order language of rings, there are two constants (0 and 1) and two binary function symbols + (addition) and \times (multiplication).

We allow familiar abbreviations in writing formulas in the language of rings. We drop parentheses when they can be reinserted unambiguously. We write + as an infix operator rather than in the usual prefix notation of first-order logic:

$$\text{'0 + 1' for ' + (0, 1)'}$$

We write '2', '3', and so forth for '1 + 1', '1 + 1 + 1', and so forth. We drop the multiplication symbol and indicate multiplication as a juxtaposition of terms. Additive inverses may be introduced: ' $a - b$ ' for ' $a + (-1)b$ ', where ' -1 ' is given through an existential quantifier

$$(1) \quad \exists x(x + 1 = 0).$$

(Every formula with ' -1 ' can be rewritten without ' -1 ' by replacing -1 with a variable symbol x and conjoining the given formula with (1).) Division may be introduced in a similar manner. We use standard logical abbreviations such as the universal quantifier, conjunction, implication, biconditional:

$$\begin{array}{ll} \text{'}\forall x\text{' for} & \text{'}\neg\exists x\neg\text{'} \\ \text{'}a \wedge b\text{' for} & \text{'}\neg(\neg a \vee \neg b)\text{'} \\ \text{'}\phi \Rightarrow \psi\text{' for} & \text{'}\neg\phi \vee \psi\text{'} \\ \text{'}\phi \Leftrightarrow \psi\text{' for} & \text{'}(\phi \Rightarrow \psi) \wedge (\psi \Rightarrow \phi)\text{'}. \end{array}$$

We often use variable symbols that are more suggestive of meaning than the variable symbols x_i provided by the language. For example, if the context is an $n \times n$ matrix, we use variable symbols x_{ij} , y_{ij} , and so forth rather than labeling the variable symbols sequentially x_1, x_2, \dots . We will occasionally use a multi-indexing notation. For example, if X is the matrix (x_{ij}) of variable symbols, then $\exists X$ is an abbreviation of

$$\exists x_{11}\exists x_{12}\cdots\exists x_{nn}.$$

We write $\phi(x_1, \dots, x_n)$ to indicate a formula in the first order language of rings such that all free variables are among the variable symbols x_1, \dots, x_n . We use a multi-index notation here as well, for instance, writing $\phi(X)$, for $\phi(x_{11}, \dots, x_{nn})$, when X is a matrix of variable symbols x_{ij} .

0.3. First order language of rings with involution. We will also have occasion to use the first order language of rings with involution. It is constructed in the same way as the first order language of rings, except that it has an additional unary function symbol. We write this function symbol as a bar over the term t to which the function symbol is applied.

0.4. Virtual sets. The language of first order rings is a highly restrictive language with no notion of sets. In particular, the set membership predicate \in is absent. Following Quine, we introduce *virtual sets* into the language as abbreviations of various logical formulas.¹ Let ϕ be a formula in the first order language of rings.

¹Quine himself calls them *virtual classes*. He tends to use the word 'class' in contexts where mathematicians prefer the word 'set.' In Quine's system, "Basically, 'set' is simply a synonym of 'class' that happens to have more currency than 'class' in mathematical contexts... My own tendency will be to favor the word 'class' where 'class' or 'set' would do, except for calling the subject set theory [11, pp. 3 and 4]." Quine's virtual classes and classes are related to what others call classes and sets, respectively. See, for example, [13, page 10].

We write

$$'y \in \{x : \phi(x)\}' \text{ for } '\phi(y).'$$

The construct $\{x : \phi(x)\}$ is called a *virtual set*. Here, x is allowed to be a multi-variable symbol: $x = (x_1, \dots, x_n)$, so that we have

$$'(y_1, \dots, y_n) \in \{(x_1, \dots, x_n) := \phi(x_1, \dots, x_n)\}' \text{ for } '\phi(y_1, \dots, y_n)'$$

When we write $x \in \mathbf{A}$, it is to be understood that x is a vector of variable symbols, and that the length of that vector is the number of free variables in the defining formula of \mathbf{A} .

If \mathbf{A} and \mathbf{B} are virtual sets defined by formulas $\phi(x)$ and $\psi(x)$ respectively, we have a notion of subset, union, and intersection:

$$\begin{aligned} '\mathbf{A} \subset \mathbf{B}' & \text{ for } '\forall x(\phi(x) \Rightarrow \psi(x))' \\ '\mathbf{A} \cap \mathbf{B}' & \text{ for } '\{x : \phi(x) \wedge \psi(x)\}' \\ '\mathbf{A} \cup \mathbf{B}' & \text{ for } '\{x : \phi(x) \vee \psi(x)\}'. \end{aligned}$$

In the language there is a single sort of quantifier, a quantifier of ring sort. It is impermissible to write an expression such as $\forall \mathbf{A}$, where \mathbf{A} is a virtual set. (There are no variables ranging over virtual sets; variables range over elements of virtual sets.) The letters ' \mathbf{A} ' and ' \mathbf{B} ' above are meta-variables, which lie outside the formal language. Furthermore, it is impermissible to write one virtual set as an element of another.

Let $\phi(y, x)$ be a formula with free variables limited to $y = (y_1, \dots, y_n)$ and $x = (x_1, \dots, x_k)$. We define a *virtual set with parameters* x by

$$'u \in \{y : \phi(y, x)\}' \text{ for } '\phi(u, x)'$$

where $u = (u_1, \dots, u_n)$. (The usual cautions about the capture of free variables apply here.) We may speak of inclusion, intersections, and unions of virtual sets with parameters.

In this article, all formulas are taken to be formulas in the first order language of rings (or rings with involution). All virtual sets are understood as given by formulas in this language.

Remark 1. It is customary practice to adopt a realist point-of-view in the discussion of set theory. That is, mathematical discourse is framed as a discussion of sets as things, rather than as well-formed expressions in a formal language. We follow a similar practice in this paper with respect to the well-formed expressions in our formal language, and adopt a realist stance. That is, we write this paper as if the formal language names objects (such as Lie algebras, centralizers, and orbits).

1. VIRTUAL TRANSFER FACTORS

1.1. Linear algebra.

Definition 2. If \mathbf{V} is a virtual set, we let $\text{lin}(\mathbf{V})$ be the formula

$$\forall \lambda_1 \forall \lambda_2 \forall x_1 \forall x_2 (x_1, x_2 \in \mathbf{V} \Rightarrow \lambda_1 x_1 + \lambda_2 x_2 \in \mathbf{V}).$$

That is, $\text{lin}(\mathbf{V})$ asserts that \mathbf{V} is a linear space. Here λ_1 and λ_2 are variable symbols and x_1 and x_2 are vectors of variable symbols. The length of the vectors must equal the number of free variables of the virtual set \mathbf{V} .

Definition 3 (linear independence). If \mathbf{V} is a virtual set with N free variables, and if e_i , for $i = 1, \dots, n$, are vectors of terms, where each vector has length N , we let $\text{lin.ind}(e_1, \dots, e_n, \mathbf{V})$ be the formula

$$\forall c_1, \dots, c_n \left(\sum_{i=1}^n c_i e_i = 0 \Rightarrow c_1 \dots c_n = 0 \right).$$

That is, the formula asserts the linear independence of the elements e_1, \dots, e_n in \mathbf{V} .

Definition 4 (span). If \mathbf{V} is a virtual set, we let $\text{span}(e_1, \dots, e_n, \mathbf{V})$ be the formula

$$\forall v \in \mathbf{V} \exists \lambda_1, \dots, \lambda_n \left(v = \sum_{i=1}^n \lambda_i e_i \right).$$

The formula asserts that e_1, \dots, e_n span \mathbf{V} . The length of the vectors e_i must equal the number of free variables in \mathbf{V} . We write $\text{basis}(e_1, \dots, e_n, \mathbf{V})$ for the conjunction

$$\text{lin.ind}(e_1, \dots, e_n, \mathbf{V}) \wedge \text{span}(e_1, \dots, e_n, \mathbf{V}).$$

Definition 5. If \mathbf{V} a virtual set, we let $\text{dim}(\mathbf{V}, n)$ be the conjunction of the two formulas

$$\begin{aligned} &\text{lin}(\mathbf{V}), \\ &\exists e_1, \dots, e_n \in \mathbf{V} : \text{basis}(e_1, \dots, e_n, \mathbf{V}). \end{aligned}$$

That is, $\text{dim}(\mathbf{V}, n)$ asserts that \mathbf{V} is a linear space of dimension n .

Definition 6. We let \mathbf{L}^n be the virtual set

$$\mathbf{L}^n = \{(x_1, \dots, x_n) : \phi(x_1, \dots, x_n)\}$$

where ϕ is any formula with free variables x_1, \dots, x_n such that

$$\forall x_1 \dots \forall x_n (\phi(x_1, \dots, x_n))$$

is valid. For example, take

$$\text{'}\phi(x_1, \dots, x_n)\text{' to be } \text{'}(x_1 = x_1) \wedge \dots \wedge (x_n = x_n)\text{'}$$

We view this virtual set as the standard linear space of dimension n . (We use the notation \mathbf{L}^n because under the Denef-Loeser map from formulas to motives, the virtual set \mathbf{L}^n is mapped to the n th power of the Lefschetz motive \mathbb{L} .)

1.2. Polynomials. We distinguish between two types of polynomials. Polynomials in the variable symbols appear as terms in the first order language of rings. This type of polynomial is not of direct interest to us in this subsection.

The second type of polynomial is a polynomial in a meta-variable with coefficients that are terms in the first order language of rings. The properties of such polynomials are developed in this subsection.

It is necessary to work with polynomials whose coefficients are terms in the first order language of rings. We let the $n + 1$ -tuple of terms, (a_0, \dots, a_n) , represent the polynomial

$$\sum a_i \lambda^i.$$

Here, λ is a meta-variable, serving as a place holder for the terms a_i . We may then identify the virtual set $\text{monic}(n)$ of monic polynomials of degree n with \mathbf{L}^n . There is no virtual set of polynomials of arbitrary degree. If f , f_1 , and f_2 are monic polynomials, then we write

$$f = f_1 f_2$$

for the conjunction of identities obtained by equating coefficients:

$$a_k = \sum_{k=i+j} b_i c_j.$$

Similarly, we write

$$f = f_1 f_2 \cdots f_\ell$$

for a conjunction of identities of coefficients.

An expression such as

$$\exists f_1 \exists f_2 \quad f = f_1 f_2,$$

for monic polynomials f , f_1 , f_2 is to be interpreted as a disjunction

$$\bigvee_{n_1+n_2=n} \exists f_1 \in \text{monic}(n_1) \quad \exists f_2 \in \text{monic}(n_2) \quad (f = f_1 f_2).$$

A constraint on the degrees such as

$$f = f_1 f_2 \text{ with } \deg(f_1) \geq 2$$

should be interpreted as a constraint on the corresponding disjunction

$$\bigvee_{n_1+n_2=n, n_1 \geq 2} .$$

The formula

$$\exists f \in \text{monic}(n) \quad \phi(f)$$

is itself to be interpreted as a statement about its coefficients a_i :

$$\exists a_0, \dots, a_{n-1} \quad \phi(a_0, \dots, a_{n-1}).$$

Definition 7. If $f \in \text{monic}(n)$, we let $\text{irred}(f)$ be the negation of the formula

$$\exists f_1 \exists f_2, \quad f = f_1 f_2 \text{ with } \deg f_1 \geq 1, \quad \deg f_2 \geq 1.$$

$\text{irred}(f)$ asserts the irreducibility of f . Note that for each n , $\text{irred}(f)$ is a different formula. In particular, the number of free variables depends on n .

Definition 8 (even). If $f \in \text{monic}(2n)$, we let

$$\text{even-poly}(f)$$

be the formula $a_1 = a_3 \cdots a_{2n-1} = 0$ asserting that f is an even polynomial.

1.3. Lie algebras.

Definition 9. The virtual Lie algebra $\mathfrak{gl}(n)$: let

$$\mathfrak{gl}(n) = \{(x_{ij}) : \phi(x_{ij})\},$$

where ϕ is a formula in n^2 free variables such that

$$\forall x_{ij} (\phi(x_{ij}))$$

is valid, and i, j range from 1 to n .

In order to define the virtual classical Lie algebras, we consider a vector of variable symbols (to be understood as the underlying linear space) and a bilinear form (presented as a matrix of terms in the language). The classical Lie algebras will be defined as appropriate virtual subsets of the virtual set of endomorphisms of the linear space.

Definition 10. The virtual Lie algebra $\mathfrak{so}(n)$: If n is odd, let $J = (q_{ij})_{1 \leq i, j \leq n}$ be given by

$$q_{ij} = \begin{cases} (-1)^{i+1}/2, & \text{if } i + j = n + 1, \ i \neq j, \\ 0, & \text{if } i + j \neq n + 1, \\ (-1)^{i+1}, & \text{if } i = j = (n + 1)/2. \end{cases}$$

If n is even, set

$$q_{ij} = \begin{cases} 0, & \text{if } i + j \neq n + 1, \\ (-1)^{i+1}/2, & \text{if } i + j = n + 1, \ i < j, \\ (-1)^{j+1}/2, & \text{if } i + j = n + 1, \ j < i. \end{cases}$$

The matrix J is to be understood as a matrix of constant symbols in the formal language. Let X be an $n \times n$ matrix of variable symbols x_{ij} . Define the virtual orthogonal Lie algebra to be the virtual set

$$\mathfrak{so}(n) = \{X : {}^tXJ + JX = 0\}.$$

Definition 11. The virtual Lie algebra $\mathfrak{sp}(2r)$ is defined in the same way:

$$\mathfrak{sp}(2r) = \{X : {}^tXJ + JX = 0\}$$

by means of the matrix $J = (q_{ij})_{1 \leq i, j \leq r}$ with $q_{ij} = (-1)^i$ if $i + j = 2r + 1$, and zero otherwise.

Definition 12. The virtual Lie algebra $\mathfrak{u}(r)$ is defined similarly. It is a virtual set in the first order language of rings with involution $t \mapsto \bar{t}$. Let

$$\mathfrak{u}(r) = \{X : {}^t\bar{X}J + JX = 0\}$$

where J is the $r \times r$ matrix of constant symbols given by $J = (q_{ij})$, with $q_{ij} = 2(-1)^{i+1}$, if $i + j = r + 1$ and $q_{ij} = 0$, otherwise.

Remark 13. In general, we follow Waldspurger closely in our definitions, including our choices of bilinear forms [14, X.3]. However, in the hermitian case, Waldspurger introduces a p -adic element η in a quadratic extension of the p -adic field. Such an element is not definable in the language of rings with involution, and we are forced to make some slight adjustments in definitions.

The symbol \mathfrak{g} will be reserved for one of the classical virtual Lie algebras that we have defined, or for a direct sum of such algebras. In general, the bold script in notation indicates that we are talking about virtual sets.

1.4. Centralizers. Let \mathfrak{g} be a virtual Lie algebra, and let $X = (x_{ij}) \in \mathfrak{g}$. Let P_X be the characteristic polynomial

$$P_X(\lambda) = \det(\lambda Id - X),$$

where the determinant is expanded as an explicit polynomial in x_{ij} .

Definition 14 (regular semisimple). The virtual set \mathfrak{g}^{reg} of regular semisimple elements inside each classical Lie algebra except for the even orthogonal algebra is the virtual set defined by the property that the matrix X has distinct eigenvalues. Explicitly, it is given by the polynomial condition $\text{res}(P_X, P'_X) \neq 0$, where $\text{res}(f, g)$ stands for the resultant of two polynomials f and g (see, e.g., [5], Section 5.4).

The virtual set of regular semisimple elements inside $\mathfrak{so}(2r)$ is the union of two virtual subsets: the set of matrices in $\mathfrak{so}(2r)$ with distinct eigenvalues and the set \mathbf{B}

of matrices in $\mathfrak{so}(2r)$ with 0 as an eigenvalue of multiplicity 2 and other eigenvalues distinct:

$$\mathbf{B} = \{X \in \mathfrak{so}(2r) : P_X = \lambda^2 f \wedge \text{res}(f, f') \neq 0 \wedge f(0) \neq 0\}.$$

Definition 15. We may define stable orbits $\mathbf{O}^{st}(X)$ as virtual sets with parameters $X \in \mathfrak{g}^{reg}$ as follows. For the unitary, symplectic, and odd orthogonal Lie algebras, we define

$$\mathbf{O}^{st}(X) = \{Y \in \mathfrak{g} : P_X = P_Y\}.$$

In the case of the even orthogonal Lie algebra, if $X \in \mathfrak{so}(2r)^{reg}$, then JX is a skew symmetric matrix of variable symbols. A skew matrix has a Pfaffian $\text{pf}(JX)$ [4, page 627]. We then have

$$\mathbf{O}^{st}(X) = \{Y \in \mathfrak{g} : P_X = P_Y \wedge \text{pf}(JX) = \text{pf}(JY)\}.$$

Definition 16. Define the centralizer $\mathbf{C}(X)$ depending on the parameter $X \in \mathfrak{gl}(n)$ by

$$\{Y \in \mathfrak{gl}(n) : XY - YX = 0\}.$$

Similarly, for $X \in \mathfrak{g}$, define

$$\mathbf{C}_{\mathfrak{g}}(X) = \{Y \in \mathfrak{g} : XY - YX = 0\}.$$

1.5. Lie algebras considered. Let $\mathfrak{g} \oplus \mathfrak{h}$ be one of the following virtual Lie algebras:

$$\begin{aligned} &\mathfrak{so}(2r+1) \oplus \mathfrak{so}(2a+1) \oplus \mathfrak{so}(2b+1), \text{ with } a+b=r, \\ &\mathfrak{sp}(2r) \oplus \mathfrak{sp}(2a) \oplus \mathfrak{so}(2b), \text{ with } a+b=r, \quad (b \neq 1), \\ &\mathfrak{so}(2r) \oplus \mathfrak{so}(2a) \oplus \mathfrak{so}(2b), \text{ with } a+b=r, \quad (a \neq 1, b \neq 1, r \neq 1), \\ &\mathfrak{u}(n) \oplus \mathfrak{u}(a) \oplus \mathfrak{u}(b), \text{ with } a+b=n. \end{aligned}$$

Each Lie algebra is split except in the unitary case. In each case, the Lie algebra is a sum of three factors. We write (X, Y, Z) for an ordered triple of matrices of variable symbols corresponding to this direct sum decomposition. We refer to these four cases as the odd orthogonal, symplectic, even orthogonal, and unitary cases, respectively. We write \mathfrak{g} for the first factor ($\mathfrak{so}(2r+1)$, $\mathfrak{sp}(2r)$, and so forth), and \mathfrak{h} for the sum of the last two factors.

Remark 17. The origin of this list of Lie algebras is the following. Let F be a p -adic field. Let G be a classical quasi-split adjoint group over F and let H be an elliptic endoscopic group of G . Then the Lie algebras listed above are the Lie algebras of products $G \times H$. (In general, H is a product of two factors.) The list is not exhaustive. In particular, it does not include the nonsplit even orthogonal groups.

Remark 18. As the introduction to this article explains, the Langlands-Shelstad transfer factor for classical groups is a function on the (Lie algebra of) $G \times H$ taking values in the set

$$\{-1, 0, 1\}q^{\mathbb{Q}}.$$

The transfer factor thus partitions the Lie algebra of $G \times H$ into three subsets, corresponding to the possible values $(-1, 0, 1)$ of the sign. By definition, the transfer factor is zero on elements that are not regular semisimple. We will realize these three subsets as virtual subsets of the virtual Lie algebras. These virtual subsets are what we take as the definition of the *virtual transfer factor*.

1.6. The nonzero part of the transfer factor. We define a virtual subset of $\mathfrak{g} \oplus \mathfrak{h}$ corresponding to the set on which the transfer factor is nonvanishing. Let \mathfrak{g}^{reg} be the virtual subset of regular semisimple elements of \mathfrak{g} .

Definition 19. The virtual \pm -set of the virtual transfer factor is defined to be the virtual subset $(\mathfrak{g} \oplus \mathfrak{h})_{\pm}$ of $\mathfrak{g} \oplus \mathfrak{h}$ given by

$$\{(X, Y, Z) \in \mathfrak{g}^{reg} \oplus \mathfrak{h}^{reg} : P_X = P_Y P_Z\}$$

in the unitary and symplectic cases, by

$$\{(X, Y, Z) \in \mathfrak{g}^{reg} \oplus \mathfrak{h}^{reg} : \lambda P_X = P_Y P_Z\}$$

in the odd orthogonal case, and by

$$\{(X, Y, Z) \in \mathfrak{g}^{reg} \oplus \mathfrak{h}^{reg} : P_X = P_Y P_Z \wedge \text{pf}(JX) = (-1)^{ab} \text{pf}(JY) \text{pf}(JZ)\}$$

in the even orthogonal case ($\mathfrak{h} = \mathfrak{so}(2a) \oplus \mathfrak{so}(2b)$). The matrices J are of appropriate size (symmetric, skew, or hermitian, as appropriate), adapted to the size of the matrices X, Y, Z as given in Section 1.3.

The virtual 0-set $(\mathfrak{g} \oplus \mathfrak{h})_0$ is defined to be the complement of the \pm -set in $\mathfrak{g} \oplus \mathfrak{h}$.

1.7. Projection operators. If $X \in \mathfrak{gl}(n)$, then we have the virtual set $\mathbf{C}(X)$ depending on parameters X . Let $\text{proj}(X)$ be the virtual set (with parameter X)

$$\text{proj}(X) = \{P = (p_{ij}) : \forall Y \in \mathbf{C}(X) (PY \in \mathbf{C}(X) \wedge PPY = PY)\}.$$

That is, it is the virtual set of matrices P (acting on the same underlying linear space as $\mathfrak{gl}(n)$) such that P acts as a projection operator on $\mathbf{C}(X)$.

Remark 20. Return for a moment to the world of set theory, rings, and modules. Let T be a linear transformation of \mathbb{C}^n with distinct eigenvalues, let $P_T \in \mathbb{C}[\lambda]$ be the characteristic polynomial. Let λ_i be an eigenvalue. Let $P^{(i)}$ be the characteristic polynomial of T divided by the factor $(\lambda - \lambda_i)$. Then

$$P^{(i)}(\lambda)/P^{(i)}(\lambda_i)$$

is a polynomial, which when evaluated at T , defines the projection operator onto the λ_i -eigenspace. This polynomial is uniquely characterized modulo multiples of P_T by this property.

More generally,

$$\sum_{i \in S} P^{(i)}(\lambda)/P^{(i)}(\lambda_i)$$

yields the projection operator onto the direct sum of the eigenspaces of $i \in S$. This polynomial is expressed by means of the resultant res in the form

$$\frac{\Pi(\lambda, f, \tilde{f})}{\text{res}(f, \tilde{f})}$$

for some

$$\Pi(\lambda, f, \tilde{f}) \in \mathbb{Z}[\lambda, a_1, \dots, a_s, b_1, \dots, b_u],$$

where

$$f(t) = t^s + a_{s-1}t^{s-1} + \dots + a_0 = \prod_{i \in S} (t - \lambda_i),$$

and

$$\tilde{f}(t) = t^u + b_{u-1}t^{u-1} + \dots + b_0 = \prod_{i \notin S} (t - \lambda_i).$$

The polynomial $\Pi(\lambda, f, \tilde{f})$ depends on T only through the coefficients of f and \tilde{f} .

Return to the world of virtual sets and formal languages. If $f \in \text{monic}(s)$ and $\tilde{f} \in \text{monic}(u)$, and $X = (x_{ij})$ are variable symbols, we have the matrix

$$\Pi(X, f, \tilde{f})$$

whose coefficients are terms in x_{ij} , a_i (the coefficients of f), and b_i (the coefficients of \tilde{f}).

1.8. The +1-set of sign. In this section we define the virtual +1-set of the transfer factor. The definition is slightly different for each case. In the unitary case, we must include the involution $t \mapsto \bar{t}$. To increase the uniformity of presentation, we define

$$t \mapsto \bar{t}$$

to be the identity map whenever \mathfrak{g} is not the unitary Lie algebra.

Definition 21. If X is a matrix of terms, let τ be the involution

$$\tau(X) = (J^{-1})({}^t\bar{X})J.$$

The matrix J is that which enters into the definition of \mathfrak{g} .

The lie algebra \mathfrak{g} can be identified with the fixed point set of $X \mapsto -\tau(X)$. Let $\mathfrak{gl}(n)$ be the linear space containing \mathfrak{g} in a natural way.

Definition 22. For each $k \geq 1$, let even_k be a boolean polynomial in k variables that is true iff an even number of the arguments are false. For example,

$$\text{even}_2(b_1, b_2) = (b_1 \wedge b_2) \vee (\neg b_1 \wedge \neg b_2).$$

In the odd orthogonal case, the characteristic polynomial of a semisimple element is an odd polynomial, but in the symplectic and even orthogonal cases, the characteristic polynomial is even. Again, for the sake of uniform presentation, for any matrix Z of terms, define

$$P_{Z,0}(\lambda) = \begin{cases} P_Z(\lambda)/\lambda, & \mathfrak{g} \text{ odd orthogonal,} \\ P_Z(\lambda), & \text{otherwise.} \end{cases}$$

Definition 23 (norms). Let $X \in \mathfrak{g}^{reg}$ be a matrix of terms, and f a monic polynomial. Let $\text{norm}(X, f, U)$ be the formula

$$\begin{aligned} \exists \tilde{f} \exists X_1 \in \mathbf{C}(X) \\ \left(P_X = f\tilde{f} \wedge U \in C(X) \wedge \Pi(X, f, \tilde{f})X_1\tau(X_1) = \Pi(X, f, \tilde{f})U \right). \end{aligned}$$

It asserts that the ‘ f -component’ of $U \in C(X)$ is a norm.

Definition 24 (trace form). Let $\text{trace-form}(X, c)$ be the formula

$$\begin{aligned} \exists e_1, \dots, e_n \quad \forall x_1, \dots, x_n, x'_1, \dots, x'_n \\ \text{basis}(e_1, \dots, e_n, C(X)) \wedge c \in C(X) \wedge \\ \text{trace}(\tau(\sum x_i e_i)(\sum x'_j e_j)c) = {}^t\bar{x}Jx'. \end{aligned}$$

Here, trace is the matrix trace. The formula asserts that there is a basis e_1, \dots, e_n of $\mathbf{C}(X)$, for which the trace form on $\mathbf{C}(X)$ (with constant $c \in C(X)$) is in agreement with the form defining \mathfrak{g} .

Definition 25 (even parity). Let $\phi(f, \dots)$ be a formula (or more accurately, a family of formulas indexed by the degree of f) whose free variables include a monic polynomial f . Let

$$\text{even-parity}(f, \phi)$$

be the formula given by

$$\bigvee_{\bigwedge_{i=1}^{\ell} \deg f_i \geq 1} \exists f_1, \dots, f_{\ell} \quad f = f_1 \cdots f_{\ell} \wedge \bigwedge_{i=1}^{\ell} \text{irred}(f_i) \wedge \text{even}_{\ell}(\phi(f_1, \dots), \dots, \phi(f_{\ell}, \dots)).$$

It asserts the even parity of the number of irreducible factors of f that fail to satisfy ϕ .

In the case of symplectic and odd orthogonal groups, we define the formula $\phi(f, \dots) = \phi(f, X, c')$ to be

$$\text{even-poly}(f) \implies \text{norm}(X, f, P'_X(X)c').$$

For even orthogonal, we take $\phi(f, X, c')$ to be

$$\text{even-poly}(f) \implies \exists X' \in \mathbf{C}(X) \quad XX' = 1 \wedge \text{norm}(X, f, P'_X(X)c'X').$$

If $X \in \mathfrak{u}(n)$, then we work systematically with the characteristic polynomial of $X\epsilon$ rather than that of X , where $\bar{\epsilon} = -\epsilon$. The characteristic polynomial of $X\epsilon$ has the property that each of its coefficients is fixed by the involution. For unitary, we take $\phi(f, X, c', \epsilon)$ to be

$$\text{norm}(X\epsilon, f, P'_X(X)c').$$

For symplectic and orthogonal groups, we define the virtual $+1$ -set $(\mathfrak{g} \oplus \mathfrak{h})_+$ to be the virtual subset of $(\mathfrak{g} \oplus \mathfrak{h})_{\pm}$ given by (X, Y, Z) satisfying the formula

$$\begin{aligned} \exists c, c' \in \mathbf{C}(X) \\ c c' = 1 & \qquad \qquad \qquad \wedge \\ \tau(c) = \chi c & \qquad \qquad \qquad \wedge \\ \text{trace-form}(X, c) & \qquad \qquad \qquad \wedge \end{aligned}$$

$$\text{even-parity}(P_{Z,0}, \phi(\cdot, X, c')).$$

The constant χ is ± 1 . It is $+1$ in each case except for $\mathfrak{g} = \mathfrak{sp}(2r)$ and even unitary. For $\mathfrak{sp}(2r)$ and even unitary, take $\chi = -1$.

In the unitary case, we replace ‘even-parity($P_{Z,0}, \phi(\cdot, X, c')$)’ with

$$‘\exists \epsilon \quad \epsilon \neq 0 \wedge \bar{\epsilon} = -\epsilon \wedge \text{even-parity}(P_{Z,\epsilon}, \phi(\cdot, X, c', \epsilon)).’$$

This completes the definition of the virtual $+1$ -set. We define the virtual -1 -set $(\mathfrak{g} \oplus \mathfrak{h})_-$ by the complement of the $+1$ -set in the \pm -set. This completes our definition of the virtual transfer factor.

1.9. Structures. There are structures (in the sense of model theory) for the first order theory of rings for every p -adic field. Let F be a p -adic field of characteristic zero. The domain of the structure is F . The binary operations $+$ and \times become addition and multiplication in F . A structure with domain F attaches a set $\mathbf{A}(F)$ to every virtual set \mathbf{A} (the set of F -points of \mathbf{A} , so to speak).

If we take the first order theory of rings with involution, then we have structures corresponding to separable quadratic extensions of p -adic fields E/F . In the domain E , the involution $t \mapsto \bar{t}$ becomes the nontrivial automorphism of E/F . If \mathbf{A} is a virtual set, and F is a p -adic field with uniquely defined unramified quadratic

extension E , we write $\mathbf{A}(F)$ for the elements of the interpretation of \mathbf{A} in the domain E with involution coming from E/F .

Remark 26. We write $\mathbf{A}(F)$ (rather than $\mathbf{A}(E)$) for the sake of uniformity of notation, as well as to suggest the analogy with the F -points of a variety (such as the F -points of the unitary group splitting over a quadratic extension E).

1.10. The Main Theorem. For the even orthogonal Lie algebra, the set of regular elements X with eigenvalue 0 is somewhat exceptional, and will be excluded from the following theorem. Such elements are excluded by restricting to elements X whose image in $\mathfrak{gl}(n)$ is regular.

Theorem 27. *Assume F is a p -adic field of characteristic zero of sufficiently large residue field characteristic. Let $\mathfrak{g} \oplus \mathfrak{h}$ be one of the Lie algebras introduced in Section 1.3. Let $\Delta(X, Y, Z)$ be the transfer factor. The set*

$$\{(X, Y, Z) \in \mathfrak{g}(F) \oplus \mathfrak{h}(F) : \Delta(X, Y, Z) = \sigma \wedge X \in \mathfrak{gl}(n)^{reg}\}$$

equals

$$\{(X, Y, Z) \in (\mathfrak{g} \oplus \mathfrak{h})_{\sigma}(F) : X \in \mathfrak{gl}(n)^{reg}\}$$

for $\sigma \in \{-1, 0, 1\}$.

This theorem will be proved in Section 3.2.

1.11. Motivic interpretation. By the theory of arithmetic motivic integration, developed by Denef and Loeser in [1], we may associate virtual Chow motives with virtual sets. (The word *virtual* is used here in two different senses.)

Let \mathbf{A} be a virtual set defined by a formula ϕ . The formula ϕ can be viewed as a formula in Pas's language, which is an extension of the first order language of rings. This extension has additional function symbols ac and ord , corresponding to the angular component function and the valuation function in p -adic analysis. For details, see [10].

A construction of Denef and Loeser [1, Section 6] attaches a virtual Chow motive to formulas in Pas's language. Orbital integrals are expected to count points on virtual Chow motives (see [7]). These virtual Chow motives are designed to be independent of the p -adic field. The construction in this article achieves the first step in a lengthy program to determine the virtual Chow motives that control the behavior of orbital integrals.

Denef and Loeser's construction gives the following corollary. A ring of virtual Chow motives $K_0^v(\text{Mot}_{\mathbb{Q}, \mathbb{Q}}) \otimes \mathbb{Q}$ over \mathbb{Q} is defined in [1]. For any number field K , and virtual Chow motive M , we obtain M_K by base change from \mathbb{Q} to K . Let K_v be the completion of K at the place v . Let O_v be the ring of integers of K_v . The virtual set $(\mathfrak{g} \oplus \mathfrak{h})_{\pm}$ is a subvariety (in the sense of being defined by polynomial equations) of $\mathfrak{g} \oplus \mathfrak{h}$ and it follows that there is a canonically defined Serre-Oesterlé measure vol_{so} on the set

$$(\mathfrak{g} \oplus \mathfrak{h})_{\pm}(O_v).$$

(See [9].)

Corollary 28. *Let \mathfrak{g} be symplectic or orthogonal. There exist virtual Chow motives $M(\sigma)$ over \mathbb{Q} , for $\sigma \in \{-1, 1\}$, such that for all number fields K and almost all places v of K we have*

$$\text{vol}_{so}((\mathfrak{g} \oplus \mathfrak{h})(O_v) \cap (\mathfrak{g} \oplus \mathfrak{h})_{\sigma} = (F)) = \text{trace } \text{Frob}_v M(\sigma)_K.$$

Remark 29. The trace of Frobenius is to be interpreted as the alternating trace on the ℓ -adic cohomology of the motive.

Proof. Let M be the virtual Chow motive attached to the virtual set

$$(\mathfrak{g} \oplus \mathfrak{h})_\sigma$$

in [1, 3.4]. The corollary is now the comparison theorem of Denef and Loeser, which states that the Serre-Oesterlé measure of definable sets is given by the trace of Frobenius against the corresponding motive [1, 8.3.1]. \square

1.12. Motives attached to unitary Lie algebras. In the case of the unitary Lie algebra, we obtain a similar statement, but we must work with the first order language of rings with involution. For simplicity, we will take the p -adic extensions E/F defining the unitary Lie algebras to be unramified.

We must confront the fact that the unitary Lie algebras are not definable in the first order language of rings. If E/F is an unramified quadratic extension of p -adic fields of characteristic zero, we may fix ϵ in E such that Galois conjugation in E/F negates ϵ :

$$\bar{\epsilon} = -\epsilon.$$

That is, ϵ is pure imaginary. With ϵ in hand, we may identify E (basis $1, \epsilon$) with the vector space F^2 (basis $(1, 0), (0, 1)$). Addition and multiplication are replaced with addition and multiplication expressed in components. Any formula in E that involves addition, multiplication, and conjugation can be replaced with a formula in twice the number of variables involving component-wise addition, multiplication expressed in components, and negation on the second factor of each pair (x, y) in F^2 representing $x + y\epsilon$ in E .

A similar approach allows us to replace a formula in the first-order theory of rings with involution with a formula in Pas's language. A formula in n free variables (z_1, \dots, z_n) becomes a formula in $2n + 1$ variables:

$$z_i \mapsto x_i + y_i \epsilon.$$

By equating real and imaginary parts, we may eliminate the variable ϵ from the equations, leaving only formulas involving $u = \epsilon^2$. The free variables of the resulting formula are $u, x_i,$ and y_i .

It is not possible to constrain u within the first order language of rings to be a particular element that is not a square. (-1 , for example, is a square in some rings and not in others, and we do not want to restrict the p -adic domains by assuming that it is a square.) But within Pas's language, we can constrain u to lie within a given definable set of nonsquares. Thus, we define $\phi(u)$ to be the formula with quantifier $\forall \xi$ of the residue field sort:

$$\forall \xi (\xi^2 \neq \text{ac}(u)) \wedge (\text{ord}(u) = 0).$$

This constrains u within a set that yields isomorphic unramified field extensions $F(\sqrt{u^F})$ for all interpretations u^F of u in F . The involution-free formula in $2n + 1$ variables defines a 1-parameter family of structures. The unitary Lie algebra, for example, is replaced by a 1-parameter family of isomorphic Lie algebras. Although each algebra is not individually definable, the 1-parameter family is.

To the formula in $2n + 1$ variables in Pas's language (conjoined with the constraint $\phi(u)$), we attach a virtual Chow motive as before over \mathbb{Q} . The trace of Frobenius

against this motives computes the Serre-Oesterlé measure within the 1-parameter family of isomorphic objects.

2. p -ADIC THEORY

Let F be a p -adic field; following Waldspurger, we assume that the residue field characteristic p is sufficiently large ($p \geq 3 \dim(\mathfrak{g}) + 1$).

In contrast to the previous section, here we consider the Lie algebras over the field F , not their virtual counterparts. We will use the notation of set theory in its traditional meaning here. We still think of the classical Lie algebras as defined by means of the same matrices J as in 1.3; however, in this section, elements are to be understood as actual matrices with entries in the p -adic field, not formal symbols.

2.1. Parametrization of regular semisimple orbits. We will need a parametrization of regular semisimple orbits in the classical Lie algebras. Here we quote it in detail from Waldspurger, [14, I.7].

Denote by (V, q_V) the vector space on which \mathfrak{g} acts by endomorphisms, with the quadratic form preserved by \mathfrak{g} . First, consider the case $\mathfrak{g} = \mathfrak{sp}(2r, F)$ or $\mathfrak{g} = \mathfrak{so}(2r + 1, F)$. Let X be a regular semisimple element in $\mathfrak{g}(F)$. Then the orbit of X corresponds to the following data:

- a finite set I ,
- a finite extension $F_i^\#$ of F for each $i \in I$,
- a 2-dimensional $F_i^\#$ -algebra F_i ,
- an element $a_i \in F_i^\times$,
- a collection of elements $c_i \in F_i^\times$, $i \in I$,

subject to the following conditions:

- For $i, j \in I$, $i \neq j$, there is no F -linear isomorphism between F_i and F_j taking a_i to a_j .
- a_i generates F_i over F .
- For all $i \in I$, denote by τ_i the unique nontrivial automorphism of $F_i/F_i^\#$. Then $\tau_i(a_i) = -a_i$.
- $\sum_{i \in I} [F_i : F] = \dim V = 2r$ in the case $\mathfrak{g} = \mathfrak{sp}(2r)$, $\sum_{i \in I} [F_i : F] = \dim V - 1 = 2r$ in the case $\mathfrak{g} = \mathfrak{so}(2r + 1)$.
- $\tau_i(c_i) = -c_i$ in the symplectic case; $\tau_i(c_i) = c_i$ in the orthogonal case.
- In the symplectic case, set $W = \bigoplus_{i \in I} F_i$ and let X_W be the element of end W defined by $X_W(\sum_{i \in I} w_i) = \sum_{i \in I} a_i w_i$. Then (V, q_V) is isomorphic to the space W endowed with the form

$$q_W \left(\sum_{i \in I} w_i, \sum_{i \in I} w'_i \right) = \sum_{i \in I} \text{trace}_{F_i/F}(\tau_i(w_i)w'_i c_i).$$

The isomorphism between V and W allows us to identify end W with end V , and X_W is identified with some $X \in \mathfrak{g}(F)$. (Note that our constants c_i differ from the ones in [14] by a factor of $[F_i : F]^{-1}$.)

In the odd orthogonal case, define (W, q_W) as in the previous case. There is an additional requirement that there exists a one-dimensional orthogonal space (W_0, q_0) over F , such that $(W_0 \oplus W, q_0 \oplus q_W)$ is isomorphic to (V, q_V) . The action of the element X_W on W is defined as above, and X_W acts by zero on W_0 .

- In the orthogonal case, when the space (W_0, q_0) exists, its class is determined uniquely.

A different choice of the isomorphism between (V, q_V) and (W, q_W) would identify X_W with an element in the same F -conjugacy class. The orbit $\mathcal{O}(X)$ is well defined and is denoted $\mathcal{O}(I, (a_i), (c_i))$. The correspondence between the orbits and the data is one-to-one if we identify the triples $(I, (a_i), (c_i))$ and $(I', (a'_i), (c'_i))$ subject to the following conditions:

- There is a bijection $\phi : I \rightarrow I'$.
- For all $i \in I$ there is an F -linear isomorphism $\sigma_i : F'_{\phi(i)} \rightarrow F_i$ such that $\sigma_i(a'_{\phi(i)}) = a_i$.
- For all $i \in I$, denote by $\text{sgn}_{F_i/F_i^\#}$ the quadratic character of $F_i^\#$ associated with the algebra F_i . Then $\text{sgn}_{F_i/F_i^\#}(c_i \sigma_i(c'_{\phi(i)}{}^{-1})) = 1$. (Notice that by definition of the c_i and c'_i , the product $c_i \sigma_i(c'_{\phi(i)}{}^{-1})$ is stable under τ_i , and therefore lies in $F_i^\#$).

The *stable* orbit of X does not depend on the constants c_i .

In the case $\mathfrak{g} = \mathfrak{so}(2r)$, the parametrization of the orbits needs to be modified as follows. The data $(I, (a_i), (c_i))$ are defined in the same way as in the odd orthogonal case. However, the correspondence between the data $(I, (a_i), (c_i))$ and the orbits is no longer one-to-one. First, the construction gives only the orbits that do not have the eigenvalue 0. Second, depending on the choice of the isomorphism between (W, q_W) and (V, q_V) , the element X_W maps into one of the two distinct orbits, which remain distinct even over the algebraic closure of F . They will be denoted by $\mathcal{O}^+(I, (a_i), (c_i))$ and $\mathcal{O}^-(I, (a_i), (c_i))$. Their union is denoted by $\mathcal{O}(I, (a_i), (c_i))$.

Suppose $X \in \mathfrak{so}(2r, F)$, $X \in \mathcal{O}(I, (a_i), (c_i))$ for some data $(I, (a_i), (c_i))$. It is possible to tell whether $X \in \mathcal{O}^+$ or $X \in \mathcal{O}^-$, using the Pfaffian of the matrix JX . Assume that A is skew-symmetric. Recall the properties of Pfaffian that we need [4, B.2.6]:

- $\text{pf}(A)^2 = \det A$.
- If $g \in GL(2r, F)$, then $\text{pf}({}^t g A g) = \det(g) \text{pf}(A)$.
- Let A and B be two skew-symmetric matrices of sizes $2a$ and $2b$, respectively. Let $A \oplus B$ be the block-diagonal matrix with the diagonal blocks A and B . Then $\text{pf}(A \oplus B) = \text{pf}(A) \text{pf}(B)$.

We will also need the following embedding ψ of $\mathfrak{so}(2a, F) \oplus \mathfrak{so}(2b, F)$ into $\mathfrak{so}(2(a+b), F)$: for $A \in \mathfrak{so}(2a, F)$, $B \in \mathfrak{so}(2b, F)$ let $\psi(A, B)$ be the block matrix

$$\begin{pmatrix} B_1 & 0 & B_2 \\ 0 & A & 0 \\ B_3 & 0 & B_4 \end{pmatrix}, \quad \text{where } B = \begin{pmatrix} B_1 & B_2 \\ B_3 & B_4 \end{pmatrix}.$$

Lemma 30. 1. The function $\theta(X) = \text{pf}(JX)$ is constant on each one of the sets $\mathcal{O}^+(I, (a_i), (c_i))$ and $\mathcal{O}^-(I, (a_i), (c_i))$ in $\mathfrak{so}(2r, F)$, and takes distinct values on these two sets.

2. Let ψ be the embedding of $\mathfrak{so}(2a, F) \oplus \mathfrak{so}(2b, F)$ into $\mathfrak{so}(2(a+b), F)$. Then $\theta(\psi(A, B)) = \theta(A)\theta(B)(-1)^{ab}$.

Proof. 1. Suppose $X, X' \in \mathcal{O}(I, (a_i), (c_i))$, and suppose $X = g^{-1}X'g$. Then $JX = Jg^{-1}X'g = {}^t g JX'g$, so $\text{pf}(JX) = \det(g) \text{pf}(JX')$. Hence, $\text{pf}(JX) = \text{pf}(JX')$ if and

only if $\det g = 1$. That is, X and X' are conjugate within the special orthogonal group.

2. In order to use the properties of the Pfaffian, we need to bring the matrix $\psi(A, B)$ to block-diagonal form. This is done by conjugating in $GL_{2a+2b}(F)$ by the permutation matrix

$$\sigma = \begin{pmatrix} 0 & \text{Id}_{2a \times 2a} & 0 \\ \text{Id}_{b \times b} & 0 & 0 \\ 0 & 0 & \text{Id}_{b \times b} \end{pmatrix}.$$

Note $J_{2a+2b} = \psi((-1)^b J_{2a}, J_{2b})$ by Definition 10. Then

$$\begin{aligned} \theta(\psi(A, B)) &= \text{pf}(J_{2a+2b}\psi(A, B)) = \text{pf}(\psi((-1)^b J_{2a}A, J_{2b}B)) \\ &= \det \sigma \text{pf}((-1)^b J_{2a}A \oplus J_{2b}B) = \theta(A)\theta(B)(-1)^{ab}, \end{aligned}$$

since $\det \sigma = 1$. □

The remaining case is the unitary group, $\mathfrak{g} = \mathfrak{u}(n)$. The orbits in $\mathfrak{u}(n)$ are parametrized similarly with the data $(I, (a_i), (c_i))$. However, F_i is obtained by a different construction. $F_i^\#$ is an extension of the base field F as before, but F_i now equals the algebra $F_i^\# \otimes_F E$, where E is the quadratic extension of F used to define the given unitary Lie algebra. In the unitary case, our form differs from that in Waldspurger by a constant $\eta \in E$ that he chooses. Our constant c_i also differs from his by a factor of η .

As before, in the unitary case the parameters a_i and c_i lie in F_i^\times ; they are subject to the following conditions:

- For any $i \in I$, a_i generates F_i over E .
- There is no E -linear isomorphism of F_i onto F_j taking a_i to a_j for $i \neq j$.
- Let $x \mapsto \bar{x}$ denote the unique nontrivial element of $\text{Gal}(E/F)$; and for each $i \in I$ let τ_i be the automorphism $\text{id} \otimes (\bar{\cdot})$. Then $\tau_i(a_i) = -a_i$, $\tau_i(c_i) = c_i$, $i \in I$.
- $\sum_{i \in I} [F_i : E] = r$.

As in the other cases, set $W = \bigoplus_{i \in I} F_i$. It is a vector space over E . The hermitian form q_W on W is defined by

$$q_W \left(\sum_{i \in I} w_i, \sum_{i \in I} w'_i \right) = \sum_{i \in I} \text{trace}_{F_i/E}(\tau_i(w_i)w'_i c_i).$$

Note that as before, our c_i differ from Waldspurger's by a factor of $[F_i : E]$. The rest of the construction remains the same; it gives all orbits, and the correspondence is one-to-one with the same definition of data $(I, (a_i), (c_i))$ and $(I', (a'_i), (c'_i))$ as in the symplectic case, except to change ' F -linear isomorphism' to ' E -linear isomorphism'.

2.2. The function sign. Recall Waldspurger's description of the sign function in detail. Here we are again quoting from [14, X.8]. Let $P_X \in F[\lambda]$ be the characteristic polynomial of X , as before. Let sign be the function on $\mathfrak{g} \oplus \mathfrak{h}$ from the definition of the transfer factor.

The function $\text{sign}(X, Y, Z)$ takes the value 0 unless $X \in \mathfrak{g}$ and $(Y, Z) \in \mathfrak{h}$ are regular semisimple, and the stable conjugacy classes of X and Y correspond. This means that the condition of Definition 19 is fulfilled (cf. Lemma 30).

Suppose that X and (Y, Z) are regular semisimple elements of $\mathfrak{g}(F)$ and $\mathfrak{h}(F)$, respectively, and their stable conjugacy classes correspond. Suppose that $Y \in \mathcal{O}(I_1, (a_{i,1}), (c_{i,1}))$, $Z \in \mathcal{O}(I_2, (a_{i,2}), (c_{i,2}))$ (Section 2.1). Let $I = I_1 \cup I_2$, and let

(a_i) be the join of the lists $(a_{i,1})$ and $(a_{i,2})$. Since the stable conjugacy classes of (Y, Z) and X correspond, there exists a family (c_i) , such that $X \in \mathcal{O}(I, (a_i), (c_i))$. Define constants C_i (upper case) by

$$C_i = \begin{cases} c_i^{-1} a_i^{-1} P'_X(a_i) & \text{if } \mathfrak{g} \text{ is even orthogonal,} \\ c_i^{-1} P'_X(a_i) & \text{otherwise.} \end{cases}$$

The elements C_i lie in $F_i^\#$ for all $i \in I$.

Theorem 31 (Waldspurger, [14], Section X.8).

$$\text{sign}(X, Y, Z) = \prod_{i \in I_2^*} \text{sgn}_{F_i/F_i^\#}(C_i),$$

where I_2^* is the set of all indices $i \in I_2$ such that $F_i/F_i^\#$ is a field extension.

3. PROOF OF THE MAIN THEOREM

3.1. A few p -adic lemmas. As above, let F be a p -adic field, I —a finite set, $F_i^\#$, $i \in I$ —a collection of finite extensions of F , F_i —a 2-dimensional $F_i^\#$ -algebra for every $i \in I$. Let τ_i be the unique nontrivial automorphism of $F_i/F_i^\#$, and let $\text{sgn}_{F_i/F_i^\#}$ be the quadratic character of $F_i^\#$ associated with the algebra F_i . The indexing set I is a union of two sets I^* and I^0 , where F_i is a field extension of F for $i \in I^*$, and F_i is a direct sum of two copies of $F_i^\#$ for $i \in I^0$. For $i \in I^*$, τ_i is the nontrivial Galois automorphism of $F_i/F_i^\#$; for $i \in I^0$, τ_i exchanges the two copies of $F_i^\#$ in F_i . We observe that the character $\text{sgn}_{F_i/F_i^\#}$ is nontrivial if and only if $i \in I^*$.

Let $W = \bigoplus_{i \in I} F_i$. Let ϕ be the isomorphism from Section 2.1 between (W, q_W) (or, in the odd orthogonal case, $(W \oplus W_0, q_W \oplus q_{W_0})$) and (V, q_V) . Let ϕ_* be the isomorphism $\phi_*: \text{end } W \rightarrow \text{end } V$ induced by ϕ . The map ϕ_* induces an isomorphism from centralizer of X_W in $\text{end } W$ onto $C(X)$.

Let $L_i: F_i \rightarrow \text{end}(F_i)$ be the linear map that takes $w \in F_i$ to the operator that acts by multiplication by w on the left on F_i . (Generally, end should be understood as end_F ; except, in the unitary case, where it should be understood as end_E .) Let $L: W \rightarrow \text{end } W$ be the direct sum of the maps L_i .

Definition 32. Let X be a regular semisimple element in a classical Lie algebra \mathfrak{g} . Define the involution τ on $C(X)$ by $\tau(g) = (J^{-1})^t g J$ with the appropriate matrix J in the symplectic and orthogonal cases, and by $\tau(g) = (J^{-1})^t \bar{g} J$ in the unitary case.

Lemma 33. Let τ_i be the involutions on F_i from Section 2.1. Let τ_W be the involution on W that acts by τ_i on each F_i , $i \in I$. For all $a \in W$,

$$\phi_* \circ L(\tau_W(a)) = \tau(\phi_* \circ L(a)).$$

Proof. First, observe that $\dim W = \dim C(X)$. It follows that $\phi_* \circ L$ is an isomorphism of F -algebras (E -algebras in the unitary case). Consider the two involutions on $C(X)$: τ and $\tau_* = (\phi_* \circ L) \circ \tau_W \circ (\phi_* \circ L)^{-1}$. We show that they coincide.

It will be more convenient to consider $-\tau$ and $-\tau_*$. It suffices to show that the involutions have the same set of fixed points. The set of fixed points of $-\tau$ is precisely $C_{\mathfrak{g}}(X)$. Let $Y \in C(X)$ be a fixed point of $-\tau_*$, and let $a = (\phi_* \circ L)^{-1}(Y)$.

Then $\tau_W(a) = -a$, since Y is a fixed point of $-\tau_*$. By definition of the form q_W , the condition $\tau_W(a) = -a$ is equivalent to the condition

$$q_W(L(a)w', w'') + q_W(w', L(a)w'') = 0 \quad \text{for all } w', w'' \in W.$$

Since $\phi(q_W) = q_V$, the latter condition is equivalent to $\tau(Y) = -Y$; that is, to the condition $Y \in C_{\mathfrak{g}}(X)$. □

We will need the following observation.

Remark 34. Let $w = (c_i)_{i \in I} \in W$ be part of the data from Section 2.1. Then $c = \phi_* \circ L(w)$ is an invertible element in $C(X)$, possessing the following property.

There exists a basis e_1, \dots, e_r of $C(X)$ such that for all $x = (x_1, \dots, x_r)$ and $x' = (x'_1, \dots, x'_r)$,

$$\text{trace} \left(\tau \left(\sum_{i=1}^r x_i e_i \right) \left(\sum_{i=1}^r x'_i e_i \right) c \right) = {}^t x J x'$$

(or ${}^t \bar{x} J x$, if unitary). Indeed, the existence of the basis is the same condition as the existence of the isomorphism ϕ . The matching of the quadratic forms follows from the definition of ϕ , the previous lemma, and the fact that the trace of an element of a field is equal to the trace of the endomorphism defined by left multiplication by that element. The invertibility of c follows from the nondegeneracy of the quadratic form defined above.

Lemma 35. *Let I be part of the data for $C(X)$ as above, and let $i \in I$. Let $z = z_i \in F_i^\#$ be an arbitrary element. Then the following conditions are equivalent:*

- (1) $\text{sgn}_{F_i/F_i^\#}(z_i) = 1$.
- (2) *Let w be an arbitrary element of W such that $w_i = z_i$. Let P be the projector from $C(X)$ onto $\phi_* \circ L(F_i)$. Then there exists $X_1 \in C(X)$ such that $PX_1\tau(X_1) = P(\phi_* \circ L)(w)$.*

Proof. If $F_i/F_i^\#$ is a field extension and if $z_i \in F_i^\#$, then $\text{sgn}_{F_i/F_i^\#}(z_i) = 1$ if and only if z_i is a norm of an element of F_i . The condition that an element z_i is a norm can be written as $\exists y \in F_i: z_i = \tau_i(y)y$. In the case when F_i is an algebra, both conditions $\text{sgn}_{F_i/F_i^\#}(z_i) = 1$ and $z_i = \tau_i(y)y$ for some $y \in F_i$ hold for all $z_i \in F_i$.

Suppose the condition (1) holds. Then let y_i be the element of F_i such that $\tau_i(y_i)y_i = z_i$. Let y be the element of W whose j th component is y_i if $j = i$, and 0 if $j \in I \setminus \{i\}$. Let $X_1 = \phi_* \circ L(y)$. Then, by Lemma 33, $\tau(X_1) = \phi_* \circ L(\tau_W(y))$. Hence, $\tau(X_1)X_1 = \phi_* \circ L(\tau_W(y)y)$. The observation that $P(\phi_* \circ L)(\tau_W(y)y) = P(\phi_* \circ L)(w)$, since $\tau_W(y)y$ and w have the same i th component, completes the proof of the implication (1) \Rightarrow (2). The converse is proved by reversing all the steps. □

3.2. Proof of the Main Theorem. Let $\mathfrak{g} \oplus \mathfrak{h}$ be a virtual Lie algebra as in Section 1.3. Let F be a p -adic field of sufficiently large residue field characteristic. Let $\mathfrak{g}(F) \oplus \mathfrak{h}(F)$ be the Lie algebra over F attached to the virtual Lie algebra $\mathfrak{g} \oplus \mathfrak{h}$. The transfer factor $\Delta(X, Y, Z)$ is defined on $\mathfrak{g}(F) \oplus \mathfrak{h}(F)$.

First, consider the zero set of Δ , that is, $\sigma = 0$. It is immediately clear by comparison of the definition of the transfer factor in Section 2.2 with Definition 19 that $\Delta(X, Y, Z) \neq 0$ if and only if (X, Y, Z) satisfies all the conditions of Definition 19, that is, $(X, Y, Z) \notin (\mathfrak{g} \oplus \mathfrak{h})_0(F)$.

Now let $\sigma = 1$. Suppose that $(X, Y, Z) \in (\mathfrak{g} \oplus \mathfrak{h})_{\pm}(F)$. We need to check that $\text{sign}(X, Y, Z) = 1$ if and only if the formula from Section 1.8 evaluated at (X, Y, Z) is true in the interpretation provided by F . The virtual centralizer $\mathbf{C}(X)$ becomes the actual centralizer of the element X in $\mathfrak{gl}(n, F)$. We keep the notation of Section 2.1.

Let $Y \in \mathcal{O}(I_1, (a_{i,1}), (c_{i,1}))$, $Z \in \mathcal{O}(I_2, (a_{i,2}), (c_{i,2}))$. Recall from Section 2.2 that then there exists an element $(c_i) \in W$ such that $X \in \mathcal{O}(I, (a_i), (c_i))$, where $I = I_1 \cup I_2$, and (a_i) is the direct sum of $(a_{i,1})$ and $(a_{i,2})$ as elements of the vector space W .

By Lemma 33 and Remark 34, the existence of $(c_i)_{i \in I}$ such that $X \in \mathcal{O}(I, (a_i), (c_i))$ and the c_i satisfy all the requirements of Section 2.1, is equivalent to the conjunction of the following statements:

- The elements c_i satisfy $\tau_i(c_i) = \chi c_i$, where $\chi = -1$ if \mathfrak{g} is symplectic or even unitary, and $\chi = 1$ otherwise. Let $c = \phi_* \circ L((c_i)_{i \in I})$. By Lemma 33, this condition is equivalent to $\tau(c) = \chi c$.
- There exists $w = (c_i) \in W$ and a basis e_1, \dots, e_n of $C(X)$, satisfying the conditions of Remark 34. This condition can be written in the terms of logic as

$$\exists c \in \mathbf{C}(X) \quad \text{trace-form}(X, c).$$

Now we need to check that Waldspurger’s condition,

$$\prod_{i \in I_2^*} \text{sgn}_{F_i/F_i^\#}(C_i) = 1,$$

is equivalent to our condition even-parity($P_{Z,0}, \phi(\cdot, X, c')$).

In the unitary case, observe that we may take the product over all of I_2 instead of I_2^* , since the sgn character is trivial if $F_i/F_i^\#$ is not a field extension. Let $X_W = (a_i)_{i \in I} \in W$. In the nonunitary case, an irreducible factor of $P_{Z,0}$ is an even polynomial iff the corresponding algebra F_i is a field. Thus, the antecedent

$$\text{even-poly}(f) \implies \dots$$

correctly distinguishes between I_2^* and I_2 .

Since $\phi_* \circ L$ is an isomorphism of F -algebras (E -algebras in the unitary case), we have $(\phi_* \circ L)(p(X_W)) = p(\phi_* \circ L(X_W))$ for any polynomial p with coefficients in F . We will use this observation with $p = P'_X$.

Let $M = \phi_* \circ L((C_i)_{i \in I})$ (it is well defined since $C_i \in F_i^\#$). In the symplectic, unitary, and odd orthogonal cases,

$$M = \phi_* \circ L((c_i^{-1} P'_X(a_i))_{i \in I}) = c' P'_X(X).$$

The last equality holds by the definition of c , c' , and $X = \phi_* \circ L((a_i)_{i \in I})$. In the even orthogonal case, the right-hand side of the above formula will have an extra factor of X^{-1} .

Suppose that $\prod_{i \in I_2} \text{sgn}(C_i) = 1$. Then $\text{sgn}(C_i) = -1$ for an even number of indices $i \in I_2$. Let $P_{Z,0}(\lambda) = f_1 \dots f_m$ (here m equals the cardinality of I_2) be the factorization of the characteristic polynomial of Z into irreducibles. By Lemma 35, for each $i = 1, \dots, m$, the condition $\text{sgn}_{F_i/F_i^\#}(C_i) = 1$ is equivalent to the existence of a matrix X_i such that $\Pi(X, f_i, \tilde{f}_i) \tau(X_i) X_i = \Pi(X, f_i, \tilde{f}_i) M$. The calculation of M shows that $\text{sgn}_{F_i/F_i^\#}(C_i) = 1$ if and only if the condition $\text{norm}(X, f, \dots)$ holds, where $c'c = 1$. By definition of the condition even-parity($P_{Z,0}, \phi(\dots)$), it holds if

and only if the number of $\text{norm}(X, f, \dots)$ that fail is even, that is, if and only if $\Delta(X, Y, Z)$ is positive. (In the unitary case, we must take the factorizations to be of $P_{X\epsilon}$ and $P_{Z\epsilon}$.) This completes the proof.

REFERENCES

- [1] J. Denef, F. Loeser, *Definable sets, motives, and p -adic integrals*, J. Amer. Math. Soc. **14**, no. 2, 429-469 (2001). MR **2002k**:14033
- [2] H. B. Enderton, *A mathematical introduction to logic*. Second edition. Harcourt/Academic Press, Burlington, MA, **2001**. MR **2001h**:03001
- [3] M. D. Fried, M. Jarden, *Field arithmetic*. Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], **11**. Springer-Verlag, Berlin, 1986. MR **89b**:12010
- [4] R. Goodman, N. R. Wallach, *Representations and Invariants of the Classical Groups*, Encyclopedia of Mathematics and its Applications, 68, Cambridge University Press, **1998**. MR **99b**:20073
- [5] N. Jacobson, *Basic Algebra I*, W.H. Freeman and Co., New York, **1996**.
- [6] T. C. Hales, *A Simple Definition of Transfer Factors for Unramified Groups*, Contemporary Math., **145** (1993), 109-134. MR **94e**:22020
- [7] T. C. Hales, *Can p -adic integrals be computed?*, math.RT/0205207, to appear.
- [8] R. Kottwitz, *Transfer factors for Lie algebras*, Representation Theory **3**, (1999) 127-138. MR **2000g**:22028
- [9] J. Oesterlé, *Réduction modulo p^n des sous-ensembles analytiques fermés de \mathbb{Z}_p^N* , Inv. Math. **66** (1982) 325-341. MR **83j**:12014
- [10] J. Pas, *Uniform p -adic cell decomposition and local zeta functions*. J. Reine Angew. Math. **399** (1989), 137-172. MR **91g**:11142
- [11] W. V. O. Quine, *Set Theory and its Logic*, Harvard University Press, Cambridge, MA, **1969**. MR **43**:37
- [12] J.-P. Serre, *Quelques applications du théorème de densité de Chebotarev*, Inst. Hautes Études Sci. Publ. Math. **54** (1981) 323-401. MR **83k**:12011
- [13] G. Takeuti, W. M. Zaring, *Introduction to Axiomatic Set Theory*. Second edition. Graduate Texts in Mathematics, **1**, Springer-Verlag, New York, 1982. MR **85b**:03003
- [14] J.-L. Waldspurger, *Intégrales orbitales nilpotentes et endoscopie pour les groupes classiques non ramifiés*. Astérisque No. **269** (2001). MR **2002h**:22014

THE FIELDS INSTITUTE, 222 COLLEGE ST., TORONTO, ONTARIO, M5T 3J1, CANADA
E-mail address: `julygord@umich.edu`

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF PITTSBURGH, PITTSBURGH, PENNSYLVANIA
 15260
E-mail address: `hales@pitt.edu`