Can p-adic integrals be computed?

Thomas C. Hales

December 5, 2002

Abstract

This article gives an introduction to arithmetic motivic integration in the context of p-adic integrals that arise in representation theory. A special case of the fundamental lemma is interpreted as an identity of Chow motives.

1 Introduction

This article raises a question in its title, and the short answer to the question is that it still has not been answered.[1][2][3] However, tools have now been developed to answer questions such as this, and this article gives an introduction to some of these tools.

This article will concentrate on a particular family of integrals that arise in connection with the representation theory of reductive groups. These are orbital integrals. The clear expectation is that these integrals can be computed, for reasons that will be explained below.

This article will also touch on the fundamental lemma, which is a conjectural identity that holds between certain orbital integrals. This article will include a statement of the fundamental lemma in a special case.

The first sections may seem misplaced because they describes some methods that are not in current use in representation theory, but by the end of the article, their relevance will be established.

The central question in my research for some time is the question of how to use a computer to prove theorems, particularly theorems in geometry. I hope to show that there is some interesting geometry that arises in connection with p-adic integration, and that computers can enhance our understanding of that geometry.

In Sections 2, 4, and 5, three major threads will be introduced: Tarski's decision procedure for the real numbers, p-adic integration, and motives. The other sections will tie these threads together in the context of the fundamental lemma and p-adic orbital integrals.

2 Tarski's decision procedure

Around 1930, Tarski proved a decision procedure for sentences in the elementary theory of real closed fields.[4]

Tarski's result can be formulated precisely in terms of a first-order language. The language is built from the fifteen symbols.

$$\begin{array}{cccc} 0 & 1 & + & * \\ (&) & = & < \\ \forall & \exists & x & ' \\ \wedge & \vee & \neg & \end{array}$$

We will not go into the details of the syntax of the language. [5] Each x is followed by zero or more primes, and primes only occur after x or another prime. We abbreviate x followed by n primes to x_n. The language contains variables x_n, and the constants 0, 1. The variables and constants can be added and multiplied (symbols $+$ and $*$). Polynomial expressions can be compared with the predicates $=$ and $<$. The quantifiers ($\forall$ and $\exists$) should be understood as ranging over the real numbers (or a complete ordered field). For example, the assertion that a quadratic polynomial has a root can be

[1] This article is based on a lecture at IAS, April 6, 2001 http://www.math.ias.edu/amf/

[2] I would like to thank Carol Olczak for her assistance in preparing this manuscript.

[4] An excellent introduction to this topic, including a reprint of Tarski's original article can be found in [3]. A survey of recent improvements in algorithms can be found at [29] and [2].

[5] The general syntactic conventions of first-order languages can be found in [12]. A treatment of syntax in the context of algebraic structures can be found in [14]

written in this formal language as

$$\neg(x' = 0) \wedge \exists x(x' * x * x + x'' * x + x''' = 0) \quad (1)$$

The formal language quickly becomes cumbersome, and we allow ourselves certain informal shorthand conventions, for example, writing Formula 1 as

$$a \neq 0 \wedge \exists x(ax^2 + bx + c = 0),$$

whenever a translation back into a formal statement of the language is clear.

Many things are noticeable absent from this little first-order language. There is no way to express particular real numbers in this language such as $\pi = 3.14159\ldots$, $e = 2.71828\ldots$, $\ln(2)$. There is no notion of set. There are no quantifiers that range over subsets of the real numbers (for example, there are no quantifiers over the integers). There are no transcendental functions such as the cosine function. There is no calculus or integration (except for formal derivatives of polynomials and the like).

Tarski's result can be expressed as an algorithm for the elimination of quantifiers in this first-order language. It takes a formula in this language and manipulates it by an entirely mechanical procedure into an equivalent form that contains no quantifiers ($\exists$ $\forall$). The formula that this procedure gives as output is equivalent to the input in the sense that the same n-tuples of real numbers satisfy the two formulas.

For example, if we apply Tarski's procedure to Formula 1, it returns something equivalent to the quantifier-free formula

$$\begin{array}{l}\neg(x' = 0)\wedge \\ (x'' * x'' - (1+1+1+1) * x' * x'' > 0 \\ \vee x'' * x'' - (1+1+1+1) * x' * x' = 0))\end{array}$$

or less formally,

$$a \neq 0 \wedge (b^2 - 4ac \geq 0).$$

In other words, Tarski's procedure determines that a quadratic equation has a real root if and only if the discriminant is non-negative. In a similar way, the truth value of all sentences in this language can be decided: the truth value of an equivalent sentence without quantifiers is trivially determined.

Here is a more difficult example, drawn from [3, page 7]. When is a quartic polynomial semidefinite? Tarski's algorithm takes the (formal translation of)

$$\forall x(x^4 + px^2 + qx + r \geq 0)$$

and returns a formula equivalent to

$$\begin{array}{ll}(256r^3 - 128p^2r^2 & +144pq^2r \\ & +16p^4r - 27q^4 - 4p^3q^2 \geq 0 \\ \wedge & \\ \quad 8pr - 9q^2 - 2p^3 & \leq 0) \\ \vee & \\ \quad (27q^2 + 8p^3 \geq 0 \wedge & 8pr - 9q^2 - 2p^3 \geq 0) \\ \wedge & \\ \quad r \geq 0 & \end{array}$$

Tarski's original algorithm is very slow, but in 1975 George Collins found a vastly improved method of quantifier elimination. Further improvements are mentioned in the survey article [3].

The methods have improved to the point that the algorithms are of practical importance. For instance, in robotics, quantifier elimination can be used to determine whether two moving objects will collide [3]. Mathematica 4.0 implements an experimental package in quantifier elimination [28]. There are highly nontrivial problems in discrete geometry that can be expressed in this little first-order language (for example, the dodecahedral conjecture [21]). The strategy is to squeeze non-trivial assertions into this little language, and then let the general algorithms prove the results.

3 Pas's language

This article is concerned, however, with p-adic quantifier elimination and not with Tarski's quantifier elimination over the reals. The first early results on quantifier elimination can be found in articles by Ax-Kochen and Ershov ([1] and [13]). The approach that we follow grows out of the article *Decision procedures for real and p-adic fields* by Paul J. Cohen in 1969 (see [4]). Cohen's work on p-adic quantifier elimination was refined and extended by various people (Denef [6], Macintyre [27], and Pas [30]). We will describe p-adic quantifier elimination as it is developed by Pas.

Pas defines a first-order language for complete Henselian rings that is analogous to Tarski's first-order language for the theory of complete ordered fields. It contains the following tokens

$$\begin{array}{cccccc} 0 & 1 & + & * & & \\ (&) & = & < & & \\ \forall & \exists & x & m & \xi & ' \\ \wedge & \vee & \neg & & & \\ \text{ord} & \text{ac} & & & & \end{array}$$

The language consists of syntactically well-formed formulas in this language. There are three sorts of variables x, x', x'' (which we abbreviate to x_0, x_1, etc.), m, m', m'' (which we abbreviate to m_i) and ξ, ξ', ξ'', etc. (which we abbreviate to ξ_i).

In the interpretations of this language, there are three algebraic structures: a valued field (such as a p-adic field), a value group (the target of the valuation, which will typically be the additive group of the integers), and a residue field. The variables x_i are of the valued-field sort, the variables m_i are of the additive group sort, and the variables ξ_i are of the residue field sort. Correspondingly, there are three sorts of quantification depending on the sort of variable the quantified is attached to. The constant 0 comes in three sorts: (0_x, 0_m, and 0_ξ). These are interpreted as the zero element in the valued field, the additive value group, and the residue field, respectively. The addition symbol + is overloaded in that it is interpreted as addition in the valued field, addition in the value group, or addition in the residue field, according to its arguments. (The syntax requires the arguments to + to be of the same sort.)

The function name *ord* is interpreted as the valuation on the field. If the model is a p-adic field, *ord* is interpreted as the normalized valuation on the field. The function name *ac* is interpreted as an angular component function. On the units in the ring of integers, the interpretation is the mapping from the units to its nonzero residue in the residue field. On general nonzero elements, it is interpreted as the function that scales its argument by a power of a uniformizer to make it a unit and then takes its image in the residue field. (Although a uniformizer is used to construct the interpretation of the function *ac*, the uniformizer itself does not appear in Pas's language.) Expressions involving "<" are restricted to the additive group sort.

One of the design requirements of this language is that it be small enough for there to be a quantifier elimination procedure. By results of Gödel, this would not be possible if the language were to encompass the full arithmetic theory of the integers [16]. For this reason, the language is restricted to the additive theory of the value group. That is, integer products such as $m * m'$ are prohibited in the language. Integer expressions may be compared through equality and inequality (= and <). According to a result proved by Presburger in 1929, a decision procedure exists for the additive theory of the integers ([31]).

Just as in the case of the first-order theory of the reals, much is missing from the language. For instance, there is no uniformizer in the language, so we cannot express p-adic expansions of numbers in the valued field. As in the case of the reals, there is no notation that would allow us to express sets in this language. It is impossible to express field extensions directly (only indirectly through polynomials defining the roots, for instance). Most of Galois theory and local class field theory will be inexpressible.

However, this language is small enough for there to be a procedure of quantifier elimination. In 1989, Pas, building on earlier results, proved that the quantifiers of the valued field sort can be eliminated, in the sense that an algorithm exists to produce an equivalent formula without quantifiers of the valued-field sort.[6] (Equivalence here means in the sense that for any complete henselian ring with a residue field of characteristic zero, the two formulas have the same set of solutions.[7])

One of the main applications of Pas's language and its quantifier elimination procedure has been to the theory of p-adic integration. For example, Pas's original article contains results about the Igusa local zeta function, which is a p-adic integral ([30]).

4 p-adic integration

Let F be a p-adic field of characteristic zero. Let $\mathfrak{g}$ be a reductive Lie algebra defined over F, X a regular semisimple element of $\mathfrak{g}(F)$. Let f be a function of compact support on $\mathfrak{g}(F)$. We consider the stable orbit $O^{st}(X)$ of X (meaning the F-points of the orbit of X over an algebraic closure). We pick an invariant measure μ on the orbit. The integral of f over $O^{st}(X)$ is called an orbital integral. A fundamental problem is to compute

$$\int_{O^{st}(X)} f\, d\mu.$$

These integrals arise repeatedly in the represen-

[6] Pas's language gives quantifier elimination of quantifiers of the valued field sort. To eliminate all quantifiers, Pas's result must be combined with Presburger's quantifier elimination on the additive theory of the integers, and with the theory of Galois stratification for quantifiers of the residue field sort.

[7] Although Pas's procedure requires the residue field to have characteristic zero, Pas, Denef, and Loeser are able to apply these results to p-adic fields with residue fields of positive characteristic. This involves the use of ultrafilters and ultraproducts. Finitely many primes are discarded in the process.

tation theory of p-adic groups, in places such as the trace formula. The conjectural fundamental lemma (it will be discussed in Section 7.4) is an identity of orbital integrals. The fact that the fundamental lemma has resisted all efforts to prove it is closely related to the difficulty of computing orbital integrals.

4.1 An example in $so(5)$

An example, will illustrate the nature of these integrals. Let $\mathbb{F}_q$ be the residue field. Assume that its characteristic is not 2. Let $\mathfrak{g} = so(5)$. Assume that X has that property that the valuation of $\alpha(X)$ is independent of the root α. Assume that

$$|\alpha(X)| = q^{-r/2},$$

for an odd integer r. Viewing X as a linear transformation on a 5-dimensional vector space, the roots of the characteristic polynomial of X are

$$0, \pm t_1, \pm t_2.$$

Let R_X be the quadratic polynomial in $k[\lambda]$ with roots the reduction mod a uniformizer ϖ_F of

$$t_i^2/\varpi_F^r.$$

We have an elliptic curve E_X over the finite field k given by

$$y^2 = R_X(\lambda^2).$$

There are test functions f so that (for appropriate normalizations of measures) we have

$$\int_{O^{st}(X)} f\, d\mu = A(q) + B(q)|E_X(k)|, \qquad (2)$$

for some rational functions of q: A and $B \neq 0$. (See [19]). The rational functions A and B depend on f. This special case gives an indication of what orbital integrals can give.

What does it mean to calculate the orbital integral? The naive and completely unsatisfactory answer is that a calculation of an orbital integral is to take a particular p-adic field, a particular element X and to program a computer to find the complex number expressed on the right-hand side of Equation 2. A satisfactory answer to what it should mean to calculate the orbital integral is to find the rational functions A and B, and to give the elliptic curve E_X. In other words, what is really needed is a symbolic computation that gets at the underlying variety (in this case an elliptic curve). This is the sense in which I intend the question asked in the title "Can p-adic integrals be computed?"

If we examine this example more closely, we might ask what features of the problem made this calculation possible? The first obvious feature is that as we vary the parameter X, the elliptic curves do not change erratically; rather, they vary within a nice family of elliptic curves over the finite field.

The second noteworthy feature is that as we move from local field to local field, we obtain (in some sense) the "same family" of elliptic curves in each case. It is this consistency as we go from one local field to another that makes it reasonable to hope that a computer algorithm might be found to compute the orbital integrals for all local fields. We can view this as a single elliptic curve E that is defined over $\mathbb{Q}(a, b)$:

$$y^2 = x^4 + ax^2 + b,$$

or as a family parameterized by a and b. All elliptic curves E_X for all p-adic orbital integrals for all local fields come as various specializations of this family.

To carry this example farther, we might look at some of the identities that are predicted by Langlands's principle of functoriality. One such identity (that is needed for applications of the trace formula) predicts an equality of orbital integrals between $so(5)$ and $sp(4)$. It has the form

$$\int_{O^{st}(X),so(5)} f\, d\mu = \int_{O^{st}(Y),sp(4)} f'\, d\mu'.$$

The data for $sp(4)$ is similar to that data for $so(5)$. The elements X and Y are related through their characteristic polynomials P_X (resp. P_Y):

$$P_X(\lambda) = \lambda P_Y(\lambda).$$

(Note that 0 is always a root of P_X.) (The function f' has to be related to f in a suitable way.) When these integrals are computed we find elliptic curves for $sp(4)$ as well, and the identity of orbital integrals holds if and only if we have an identity of the following form

$$A(q) + B(q)|E_X(k)| = A(q) + B(q)|E'_Y(k)|.$$

It turns out that the elliptic curves E_X and E'_Y are not isomorphic (they have different j-invariants), but they can be proved to have the same number of points by producing an isogeny between E_X and E'_Y.

This isogeny can be expressed as a single isogeny between two elliptic curves E and E' over $\mathbb{Q}(a, b)$.

The conclusion of this discussion is that this particular identity of orbital integrals holds for all p-adic fields because of an identity of two Chow motives over $\mathbb{Q}(a,b)$: that is, E is isogenous to E'.

What this suggests is a general hope that there are global objects attached to p-adic integrals. The global object should be something like a Chow motive. Identities of p-adic integrals should be consequences of identities of Chow motives.

5 Motives

We are finally in the position to give a precise definition of what it means to compute a p-adic integral. We state it as a thesis:

Thesis 5.1. *The computation of a p-adic integral is an effective algorithm to obtain the underlying virtual Chow motive.*

This thesis is incoherent unless virtual Chow motives are associated with general families of p-adic integrals. That this should be so was articulated by Loeser in Strasbourg in 1999 [25].

Principle 5.2. *(Denef-Loeser Principle) All "natural" p-adic integrals are motivic.*

Without committing Denef and Loeser to any particular definition of "natural," as representation theorists, we like to think that the important integrals that arise in representation theory are natural. We are thus led to an investigation of motivic underpinnings of p-adic integrals.

5.1 An Example of Motivic Integration

Motivic integration was introduced by Kontsevich in a lecture in Orsay in 1995 [22]. The properties of motivic integration have been developed in a series of fundamental articles by Denef and Loeser [8], [9], [10], [11]. In fact, my entire article is nothing but an application of the beautiful circle of ideas that they develop.

To describe the theory in a few words, I will describe motivic integration by analogy with p-adic integration. Consider the following elementary p-adic integral:

$$\begin{aligned}\int_{\mathbb{F}_q[[t]]} |x|^m\,dx &= \sum_{\ell=0}^{\infty} |\varpi^\ell|^{m+1} \int_{|u|=1} \frac{du}{|u|} \\ &= (1+q^{-(m+1)}+q^{-2(m+1)}\cdots)(1-q^{-1})\end{aligned}$$

The answer is independent of the field, so we are tempted to write for any field (say a field of characteristic zero):

$$\begin{aligned}\int_{k[[t]]} |x|^m\,dx &= \sum_{\ell=0}^{\infty} |\varpi^\ell|^{m+1} \int_{|u|=1} \frac{du}{u} \\ &= (1+q^{-(m+1)}+q^{-2(m+1)}\cdots)(1-q^{-1})\end{aligned}$$

The only difficulty is in the interpretation of q. Kontsevich supplies the answer with motivic integration: it is a symbol. More specifically, in the case of finite fields it is a symbol attached to the affine line $\mathbb{A}^1$, and for general fields we can continue to view it as a symbol attached to the affine line. To mark the change of context from p-adic fields to more general fields, we replace the symbol q with Ł (to suggest the Lefschetz motive).

5.2 Rings of virtual motives

Section 5.1 describes a simple example of motivic integration. You integrate much in the same way as with p-adic integration, but whenever in p-adic integration it becomes necessary to count points on a variety, with motivic integration you introduce a new symbol for that variety and move on. Although a single symbol (q or Ł) suffices for the one example that was shown, motivic integration in general will require a host of new symbols. Integration should be linear, so relations must be introduced among the symbols to make motivic integration linear. In that example, q (or Ł) occurs as a denominator, and this will require us to invert Ł in the ring we construct. In that example, the answer is a limit (that is, an infinite sum), and this will require us to complete the ring we construct.

6 Rings of motives

Let k be a field of characteristic zero. Let Sch_k be the category of varieties over k. Let $K_0(\mathrm{Sch}_k)$ be the Grothendieck ring of varieties over k. It is the commutative ring generated by symbols

$$[S]$$

for each variety S over k. The relations are

$$[S \times S'] = [S][S']$$

and if S' is closed in S, then

$$[S] = [S \setminus S'] + [S'].$$

We let Ł $= [\mathbb{A}^1]$. Let $K_0(\mathrm{Sch}_k)_{loc}$ be the ring obtained by inverting Ł.

We let $\mathrm{Mot}_{\mathrm{k},\bar{\mathbb{Q}}}$ be the category of Chow motives over k with coefficients in $\bar{\mathbb{Q}}$, an algebraic closure of $\mathbb{Q}$. (This category is described in detail in [32].) The objects in this category are triples

$$(S, p, n)$$

where S is a variety over k, p is a projection operator over $\bar{\mathbb{Q}}$, and n is an integer. This category is an additive category, but it is not abelian [32].

Let $K_0(\mathrm{Mot}_{\mathrm{k},\bar{\mathbb{Q}}})$ be the Grothendieck group of the additive category $\mathrm{Mot}_{\mathrm{k},\bar{\mathbb{Q}}}$. The generators of this group is the set of objects in $\mathrm{Mot}_{\mathrm{k},\bar{\mathbb{Q}}}$. By a fundamental result of Gillet and Soulet [15] and Guillén and Navarro Aznar [17], there is a homomorphism of rings

$$K_0(\mathrm{Sch}_k) \to K_0(\mathrm{Mot}_{\mathrm{k},\bar{\mathbb{Q}}})$$

that takes the symbol $[S]$ of a smooth projective variety S to the generator associated with $(S, \mathrm{id}, 0)$, where id is the identity projection operator. The image of Ł under this homomorphism is invertible. Thus, the homomorphism extends to $K_0(\mathrm{Sch}_k)_{loc}$. Let $K_0^v(\mathrm{Mot}_{\mathrm{k},\bar{\mathbb{Q}}})_{loc}$ be the image of this homomorphism.

There is a filtration $F^m K_0^v(\mathrm{Mot}_{\mathrm{k},\bar{\mathbb{Q}}})_{loc}$ on this group given by $S/Ł^i \in F^m$ iff $\dim S - i \leq -m$. We let $\hat{K}_0^v(\mathrm{Mot}_{\mathrm{k},\bar{\mathbb{Q}}})_{loc}$ be the completion of with respect to this filtration. This is the ring in which motivic integrals take their values (or sometimes its tensor product with $\mathbb{Q}$).

6.1 Arithmetic motivic integration

In 1999, Denef and Loeser developed an arithmetic theory of motivic integration in [7]. (This theory is distinct from a geometric theory of motivic integration that was developed earlier.) In their article, that Denef and Loeser describe the three threads introduced in Sections 2, 4, and 5, and show how they relate to one another. In their article, they make two fundamental discoveries:

1. Motives can be attached to formulas in Pas's language.
2. The trace of Frobenius on the motive equals the p-adic integral over the p-adic set defined by the formula.

The process is represented schematically in Figure 1. A formula in Pas's language can be interpreted two ways, leading to two different integrals. First the formula can be interpreted over a p-adic field. The p-adic set of points that satisfy the formula has a volume. The formula can also be interpreted over a henselian field (such as $\mathbb{C}((t))$). The set of points that satisfy the formula has a motivic volume (an element of the ring $\hat{K}_0^v(\mathrm{Mot}_{\mathrm{k},\bar{\mathbb{Q}}})_{loc}$).

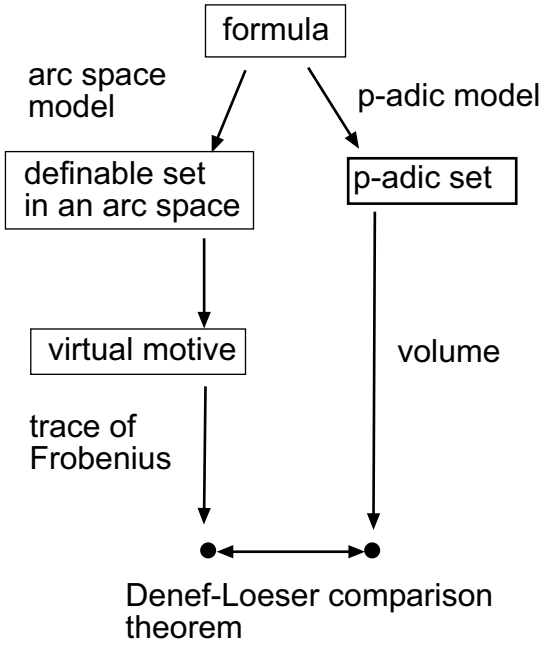

Figure 1: The Denef-Loeser comparison theorem

The comparison theorem of Denef and Loeser asserts that the trace of Frobenius against this virtual motive is equal to the p-adic volume of the p-adic set. In particular, if a p-adic set has the special form given by the set of points satisfying a formula in Pas's language, then a motive can be attached to it. It is this comparison theorem that will permit us to show that interesting p-adic integrals have a motivic interpretation.

7 The fundamental lemma

All the sections until now have been an extended introduction to provide context for the results I am about to describe. Roughly speaking, I have found that orbital integrals can be placed into the framework of Denef and Loeser.

7.1 Strips

Let F be a p-adic field of characteristic 0. Let k be the residue field of F. Fix parameters n, k, and r satisfying the following conditions.

- n is a positive integer.
- k is an integer $k \leq n$.
- r is a rational number. Write it as $r = \ell/h$, with ℓ and h relatively prime.

Let $\mathfrak{g} = so(2n+1)$. There are endoscopic Lie algebras

$$\mathfrak{h} = so(2k+1) \times so(2n-2k+1).$$

That is, we take a product of two orthogonal Lie algebras, whose ranks add up to that of $\mathfrak{g}$. (Endoscopy was originally defined in terms of groups, but it has become common practice to follow the practice of Waldspurger and to pass to the Lie algebras.)

We define a subset of $\mathfrak{g}$ that I will call a strip. It depends on the parameter r. Define strip(r) to be the set of all $X \in \mathfrak{g}$ such that $|\alpha(X)| = q^{-r}$ for all roots α. These elements are called elements *equal valuation.*

Write the characteristic polynomial $P_X(\lambda)$ as

$$P_X(\lambda) = \lambda P_X^0(\lambda).$$

Let $\bar{\mathbb{F}}_q$ be an algebraic closure of $\mathbb{F}_q$. Let R_X be the separable polynomial in $\mathbb{F}_q[\lambda]$ with roots in $\bar{\mathbb{F}}_q$ given by the reduction of the elements

$$t_i^h/\omega_F^\ell,$$

where t_i are the nonzero roots of P_X (that is, the roots of P_X^0). The elements t_i^h have been multiplied by an appropriate power of the uniformizer, so that they become units. As a result, the roots of R_X are nonzero.

7.2 Aside on Equal Valuation

In this article, we do not justify our restriction to this special kind of elements. Without going into the details, it seems to me that the study of orbital integrals can be divided into two quite different parts. The part discussed in this article is that of elements of equal valuation. It seems that geometric methods such as motivic integration are very important for this part.

For elements of nonequal valuation, it seems that a quite different set of methods will be relevant. Here issues such as homogeneity (generalizing the results of Waldspurger [33] and DeBacker [5]) and descent for orbital integrals [24] should be relevant.

This is currently merely speculation, but it is the reason that I am restricting to elements of equal valuation. It seems that different groups could study these two different kinds of orbital integrals with little interaction and few shared methods.

7.3 A hope

Conjecture 7.1. *If X and X' are elements in* strip(r) *such that $R_X = R_{X'}$, then their orbital integrals are equal.*

We represent strip(r) schematically as a long rectangular strip (a union of semisimple orbits). Around the conjugacy class of X we can draw a tube (a thickened neighborhood) of all the elements in the strip with the same reduced characteristic polynomial R_X. (Figure 2.) The function $X \mapsto R_X$

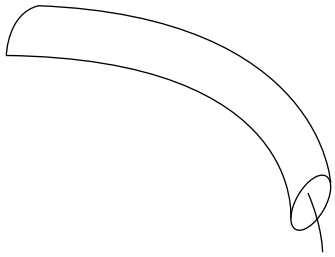

Figure 2: A tube

thus partitions strip(r) into tubes.

7.4 A p-adic fundamental lemma

Langlands and Shelstad define a transfer factor $\Delta(X,Y,Z)$ on $so(2n+1) \times so(2k+1) \times so(2(n-k)+1)$. On the strip r it has the form

$$q^c \text{sign}(X,Y,Z)$$

for some constant $c = c(n,k,r)$ and some function sign taking values in $\{0,1,-1\}$. Let O_F be the ring of integers of the p-adic field F. They conjecture that for appropriate normalizations of measures [20], we have the following special case of the fundamental lemma

Conjecture 7.2. *(Langlands-Shelstad) For all Y and Z regular semisimple such that there exists a regular semisimple X in $\mathfrak{g}$ such that $P_X^0 = P_Y^0 P_Z^0$, we have*

$$q^c \sum_X \int_{O(X) \cap \mathfrak{g}(O_F)} \text{sign}(X,Y,Z) \quad = \quad \int_{O^{st}(Y) \times O^{st}(Z) \cap \mathfrak{h}(O_F)} 1.$$

The sum runs over representatives of all regular semisimple conjugacy classes. The function $\mathrm{sign}(X,Y,Z)$ is zero unless $P^0_X = P^0_Y P^0_Z$. It is enough to restrict the sum to such representatives.

Proposition 7.3. *If F is a field of sufficiently large residual characteristic, then the sign of the transfer factor in $so(2n+1)$,*

$$\mathrm{sign}^{-1}(x), \text{ for } x \in \{0, 1, -1\},$$

is given by a formula in the language of rings.

The proof will be given in a separate article. The surprising thing about this calculation is that the full strength of Pas's language is not required. That is, the transfer factor is expressed without the functions ord and ac, and without quantifiers over the additive group and residue field. This means that we can define a transfer factor for any field.

The formula for $\mathrm{sign}^{-1}\{-1, 1\}$ does not require quantifiers. It is the set of elements (X, Y, Z) with

$$\lambda P_X = P_Y P_Z$$

for which X is regular (which is expressed as the nonvanishing of the resultant

$$\mathrm{resultant}(P_X, P'_X) \neq 0.$$

The starting point for the proof of the proposition is Waldspurger's simplified formula for the transfer factors on the Lie algebra of classical groups [34].

From this proposition, the Denef-Loeser construction gives us a $+1$-motive in $\hat{K}^v_0(\mathrm{Mot}_{\mathrm{k},\bar{\mathbb{Q}}})_{loc}$. It also gives a -1-motive in the same set. In this sense, we can affirm that the Langlands-Shelstad transfer factor is a motive.

7.5 Orbital integrals

A serious difficulty that we encounter in the study of orbital integrals is that individual orbits of semisimple elements are not given by a formula in Pas's language. In fact, the characteristic polynomial

$$P_X \in F[\lambda]$$

has p-adic coefficients, which cannot be expressed in the language. (Without a uniformizer in the language, we cannot express the p-adic expansion of the coefficients.)

Our only hope is to use the fact that orbital integrals are locally constant. We place each orbit into a larger tube, where the tube is large enough to be defined by a formula in Pas's language. Each tube is defined by the set of elements with a given reduced characteristic polynomial with coefficients in the residue field (see Section 7.1):

$$R_X \in \mathbb{F}_q[\lambda].$$

To patch these together into a global object, we let k be a finite extension of $\mathbb{Q}$, with ring of integers O_k. Each polynomial R_X is a specialization of a polynomial

$$\dot{R}_X \in S[\lambda],$$

where S is the coordinate ring over O_k of the set of regular orbits

$$Z = Z_r = \mathfrak{a}/\mathrm{Ad}\, A$$

on an appropriate Lie algebra $\mathfrak{a}$ and group A, defined over O_k. We can then use $\dot{R}_X$ to define a formula in

$$\mathcal{L}_{pas}(S).$$

(This denotes the Pas's language extended by a symbolic constant for each element of S, as described in [14, Section 6.3].)

The formula for the set of elements in the tube with transfer factor equal to $+1$ gives, by the construction of Denef and Loeser, a Chow motive

$$\Theta^{G,+}_{n,k,r}.$$

The negative part of the tube gives a second Chow motive

$$\Theta^{G,-}_{n,k,r}.$$

The tube on the endoscopic groups gives a third Chow motive

$$\Theta^{H,st}_{n,k,r}.$$

Recall that the p-adic transfer factor has the form

$$\pm q^c$$

for some constant $c = c(n,k,r)$. We are thus able to formulate a motivic fundamental lemma:

Conjecture 7.4. *Given n, k, and r, we have*

$$L^c(\Theta^{G,+}_{n,k,r} - \Theta^{G,-}_{n,k,r}) = \Theta^{H,st}_{n,k,r}$$

in

$$\hat{K}^v_0(M_{\mathbb{Q}(Z_r),\bar{\mathbb{Q}}})_{loc,\mathbb{Q}}$$

This single identity of Chow motives governs the fundamental lemma over the entire strip(r) at almost all places.

Remark 7.5. The Denef-Loeser comparison theorem relates the trace of Frobenius on these motives to the traditional fundamental lemma. The Denef-Loeser comparison theorem in its current form is not quite strong enough to deduce the fundamental lemma from its motivic form. However, I hope that these are relatively minor obstacles that future research should be able to surmount.

First of all, we need the Denef-Loeser comparison theorem for the finitely generated extension $\mathbb{Q}(Z_r)/\mathbb{Q}$. Denef and Loeser give two comparison theorems, one for p-adic integration on local fields of positive characteristic, and another on local fields in characteristic zero. The comparison theorem in characteristic zero assumes that the field is a finite extension of $\mathbb{Q}$ and hence it cannot be applied to $\mathbb{Q}(Z_r)$.[8]

The second restriction of the Denef-Loeser comparison theorem is that if R is a normal domain with field of fractions $\mathbb{Q}(Z_r)$, then the comparison theorem holds at all closed points x of Spec R_f for some non-explicit element f of R. It is possible that f blocks a comparison of some elements of the p-adic field.

Remark 7.6. One of the most interesting aspects of this calculation is that it shows that there are two local-global pathways. The local-global pathway connecting automorphic representation theory with the representation theory of local fields is a well-established part of the Langlands program. It generalizes the pathway between global and local class field theory. The Denef-Loeser apparatus gives a genuinely new pathway between global and local objects. (To see that it is a different pathway, observe that a global regular semisimple element in a reductive group

$$\gamma \in G(\mathbb{Q})$$

lies in an unramified Cartan subgroup at almost every place. However, the Denef-Loeser construction quite often globalizes local data that is everywhere ramified.)

Thus, we have global problems in automorphic representation theory that are localized by the first pathway, and then globalized again by the second pathway to obtain conjectural identities of Chow motives.

[8] Denef and Loeser (private communication) have informed me that they can relax this restriction for p-adic fields of characteristic zero that are unramified over $\mathbb{Q}$. This is expected to be sufficient for applications to the fundamental lemma.

8 Open Problems

We conclude this article with four problems that are raised by the study of p-adic integrals from the vantage point of motivic integration.

Problem 8.1. *Give effective algorithms to find the Chow motives*

$$\Theta^{*,*}_{n,k,r}.$$

By solving this problem, we succeed in computing p-adic orbital integrals in the sense proposed in this article. The quantifier elimination procedures (Pas's algorithm [30], Presburger's algorithm [12], and Galois stratification [14]) are entirely algorithmic. Thus, I hope that this first problem can be settled.

Problem 8.2. *Prove the hope of Conjecture 7.1: if $R_X = R_{X'}$, then the orbital integrals of $O^{st}(X)$ and $O^{st}(X')$ are equal.*

In unpublished work, Clifton Cunningham has made progress toward a solution of this second problem.

Problem 8.3. *Extend the results to degenerate elements X that do not lie in any strip r. In particular, find finitely many motives over finitely generated extensions of $\mathbb{Q}$ that govern the fundamental lemma for all $X \in \mathfrak{g}$ over almost all completions of any number field.*

This seems to me to be a difficult problem. As an earlier section states (see 7.2), the methods involved here seem to be methods of generalized homogeneity laws in the spirit of Waldspurger and DeBacker ([33] and [5]).

Problem 8.4. *Prove the motivic fundamental lemma.*

If the first three problems can be solved, then we have an algorithm to compute the Chow motives that govern the fundamental lemma for a given group. However, more is needed. First there is the problem of equality: given two Chow motives, is there an algorithm to determine if they are equal?

Second, there is the problem of induction. Even if we have an algorithm to check the fundamental lemma for one group, how do we give a proof for all reductive groups at once? Here it seems to me that we need to develop a deeper understanding of the motives that arise in connection with the fundamental lemma.

9 Conclusion

The Denef-Loeser apparatus of arithmetic motivic integration seems to mesh well with certain p-adic integrals that arise in representation theory.

We should investigate how far motives permeate representation theory of p-adic groups. If we believe with Denef and Loeser that all natural p-adic integrals are motivic, then the influence of the motivic point of view will be far-reaching. One can speculate that many of the basic objects of representation theory (such as Harish-Chandra characters) have a motivic nature.

The hope is that the motivic interpretation will allow us to calculate p-adic integrals that have resisted all efforts until now.

References

[1] J. Ax and S. Kochen, Diophantine problems over local fields, I, II, Amer. J. Math 87 (1965), 605-648; III, Ann. Math. 83 (1966), 437–456.

[2] S. Basu, R. Pollack, and M.-F. Roy, On the combinatorial and algebraic complexity of Quantifier Elimination, In Procedings of the Foundations of Computer Science, pp. 632–641, 1994.

[3] B.F. Caviness and J.R. Johnson (eds.) Quantifier Elimination and Cylindrical Algebraic Decomposition, Springer, 1998.

[4] P. J. Cohen, Decision procedures for real and p-adic fields, Comm. Pure Appl. Math. 22 (1969), 131-151.

[5] S. DeBacker, Homogeneity Results for Invariant Distributions of a Reductive p-adic Group, preprint.

[6] J. Denef, p-adic semi-algebraic sets and cell decomposition, J. reine angew. Math. 369 (1986), 165–166.

[7] J. Denef and F. Loeser, Definable Sets, Motives, and p-adic Integrals, [math.AG/9910107], Journal of the Amer. Math. Soc. 14, 429-469 (2001).

[8] J. Denef and F. Loeser, Germs of arcs on singular algebraic varieties and motivic integration, Inventiones Mathematicae 135, 201-232 (1999).

[9] J. Denef and F. Loeser, Motivic Igusa zeta functions, Journal of Algebraic Geometry 7, 505-537 (1998).

[10] J. Denef and F. Loeser, Motivic exponential integrals and a motivic Thom-Sebastiani Theorem, Duke Mathematical Journal, 99, 285-309 (1999).

[11] J. Denef and F. Loeser, Motivic integration, quotient singularities and the McKay correspondence, to appear in Compositio Math.

[12] H. Enderton, A mathematical introduction to logic, Academic Press, 1972.

[13] Ju. L. Eršov, On the elementary theory of maximal normed fields, Soviet Math. Dokl. 6 (1965), 1390–1393.

[14] Michael D. Fried and Moshe Jarden, Field Arithmetic, Springer, 1986.

[15] H. Gillet and C. Soulé, Descent, motives, and K-theory, J. Reine Angew. Math., 478 (1996), 127-176.

[16] K. Gödel, On Formally Undecidable Propositions Of Principia Mathematica And Related Systems, Dover reprint edition, (1972).

[17] F. Guillén and V. Navarro Aznar, Un critère d'extension d'un foncteur défini sur les schémas lisses, preprint.

[18] T. Hales, Can p-adic integrals be computed, slides and video of a lecture at IAS, 6 Apr 2001, http://www.math.ias.edu/amf/.

[19] T. Hales, Harmonic analysis and hyperelliptic curves, in Representation Theory and Analysis on Homogeneous Spaces, ed. by S. Gindikin, et al., Comtemp. Math, AMS, 1994.

[20] T. Hales, A simple definition of transfer factors, Contemporary Math. 145 (1993), 109-134.

[21] T. Hales, Some algorithms arising in the proof of the Kepler conjecture, to appear.

[22] M. Kontsevich, lecture at Orsay, 7 Dec 1995.

[23] R. P. Langlands and D. Shelstad, On the definition of transfer factors, Math. Ann. 278 (1987), 219-271.

[24] R.P. Langlands and D. Shelstad, Descent for Transfer Factors, in The Grothendieck Festscrift, vol II, ed. by R. Cartier et al., 1991.

[25] F. Loeser, lecture at Strasbourg, 1999.

[26] Eduard Looijenga, Motivic Measures, arXiv.math.AG/0006220 v2 21 Oct 2000.

[27] Macintyre, On definable subsets of p-adic fields, J. Symb. Logic 41 (1976), 605–610.

[28] Quantifier Elimination – from MathWorld, http://mathworld.wolfram.com/QuantifierElimination.html

[29] B. Mishra, Computational Real Algebraic Geometry, Handbook of Discrete and Computational Geometry, CRC Press, 1997.

[30] Johan Pas, Uniform p-adic cell decomposition and local zeta functions, J. reine angew. Math. 399 (1989), 137-172.

[31] M. Presburger, Über die Vollständigkeit eines gewissen Systems der Arithmetik ganzer Zahlen, in welchem die Addition als einzige Operation hervortritt, Comptes-rendus du I Congrès des Mathématiciens des Pays Slaves, Warsaw, 1929, pp 92-101, 395.

[32] A. Scholl, Classical Motives, in Motives, U. Jannsen, S. Kleiman, J.-P. Serre Ed., Proc. Symp. Pure Math., Vol 55 Part 1 (1994), 163-187.

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

[34] J.-L. Waldspurger, Intégrales orbitales nilpotentes et endoscopie pour les groupes classiques non ramifiés, Astérisque, vol. 269, SMF, 2001.

version 5/19/02.
Research supported in part by the NSF