ORBITAL INTEGRALS ARE MOTIVIC

THOMAS C. HALES

ABSTRACT. This article shows that under general conditions, p-adic orbital integrals of definable functions are represented by virtual Chow motives. This gives an explicit example of the philosophy of Denef and Loeser, which predicts that all "naturally occurring" p-adic integrals are motivic.

1. Introduction

[1] Denef and Loeser have introduced a theory of arithmetic motivic integration [3]. In this theory, general families of p-adic integrals can be calculated as the trace of a Frobenius operator on virtual Chow motives. This article shows that orbital integrals fit nicely into the general framework of Denef and Loeser. It describes a large class of orbital integrals that can be computed by a Frobenius operator on virtual Chow motives. Moreover, there is an effective procedure to compute the virtual Chow motive from the data defining the orbital integral. In this sense, this article gives an algorithm to compute a large class of orbital integrals.

The idea of using double cosets to compute motivic orbital integrals is taken from J. Gordon's recent thesis (and a suggestion of Julee Kim). The thesis proves that under general conditions, the character values of depth zero representations of a p-adic group can be represented as virtual Chow motives [7]. This note can be viewed as an extension of the methods of that thesis.

2. Double coset bounds

Recall that Pas has defined a first order language that is based on the theory of valued fields [11]. It is a three-sorted language in the sense of [5]. The models of the three sorts are a valued field, a residue field, and the additive group of integers (the value group), augmented by $+\infty$. The language has function symbols ord and ac that are interpreted as the valuation and angular component maps on a valued field. The valuation is a map from the valued field to $\mathbb{Z} \cup \{+\infty\}$. The angular component map is a function from the valued field to its residue field.

Let $\mathcal{K}$ be a set of models of Pas's language. We do not make any assumptions about the residual characteristic of the fields in $\mathcal{K}$. We do, however,

Date: December 5, 2002.

assume that each field is complete and Henselian. In fact, the only cases of interest to us are locally compact nonarchimedean fields (in brief, p-adic fields). For example, we could take $\mathcal{K}$ to be models corresponding to the set of p-adic fields $\mathbb{Q}_p$, or the set of fields $\mathbb{F}_p[[t]]$, or the set of all p-adic fields. We write θ^k for an interpretation of θ in the model k. If S is a finite set of prime numbers, let $\mathcal{K}_S$ be the set of $k \in \mathcal{K}$ for which the residual characteristic of k is *not* in S.

Let $\theta(m)$ be a formula in Pas's language. Assume that θ has no free variables of the valued field sort or of the residue field sort. Assume that its free variables of the additive sort are contained in $m = (m_1, \ldots, m_\ell)$.

Suppose that there exists a finite set S of prime numbers satisfying the following condition:

Condition 1. *For every $k \in \mathcal{K}_S$,*

$$\{m \in \mathbb{Z}^\ell \ : \ \theta^k(m)\}$$

is a bounded subset of $\mathbb{Z}^\ell$.

Theorem 2. *Under the stated conditions, there exists a finite set S' of prime numbers and a bounded subset $C \subset \mathbb{Z}^\ell$ such that for every $k \in \mathcal{K}_{S'}$ we have*

$$\{(m_1, \ldots, m_\ell) \in \mathbb{Z}^\ell \ : \ \theta^k(m_1, \ldots, m_\ell)\} \subset C.$$

In other words, by throwing away finitely many primes, the bound on the subset in Condition 1 can be made independent of the model.

Proof. Apply Pas's quantifier elimination on quantifiers of valued field sort in the formula θ. We obtain an equivalent formula that contains no variables of valued field sort. This formula is uniform in the sense that it is independent of the model $k \in \mathcal{K}$. Pas assumes that the residual characteristic is zero. We achieve equivalent results by throwing out finitely many residual characteristics.

The remaining terms of valued field sort are constants that are definable in Pas's language without quantifiers. Such a constant must be a rational number. Equalities in the valued field $a = b$ can be replaced with an equivalent statement with the angular component map: $\mathrm{ac}(a-b) = 0$. The infinite valuation condition $\mathrm{ord}(a) = +\infty$ can be replaced with $\mathrm{ac}(a) = 0$. Excluding finitely many primes, each rational number appearing in the formula can be assumed to be 0 or a unit; that is, it is an integer in each model. If $a \neq 0$, the condition $\mathrm{ord}(a) = m$ is then equivalent to the formula $m = 0$, and if $a = 0$ it is false (because we have already treated $\mathrm{ord}(a) = +\infty$). Similarly, the formula $\mathrm{ac}(a) = \xi$ is equivalent to $a' = \xi$, where a' is the element in the residue field that is the reduction of the integer a. In this way, we eliminate all terms of valued-field sort, all function symbols ac and ord.

Writing the formula in disjunctive normal form we find that θ is equivalent to

$$\bigvee_i (\psi_i \wedge L_i), \tag{1}$$

where ψ_i is a formula with no free variables and containing only constants and terms of the residue field sort, and L_i is a formula with free variables limited to m and whose constants and terms are of the value group sort. We may assume that $+\infty$ has been eliminated from the language, so that each L_i is a conventional Presburger formula [5].

We partition the finite set of indices i into two sets B and $\bar{B}$, where B is the set of indices for which L_i is a bounded subset of $\mathbb{Z}^\ell$ and $\bar{B}$ the set of indices for which L_i is unbounded. We can find a set $C \subset \mathbb{Z}^\ell$ that contains

$$\cup_{i\in B}\{m \ : \ L_i(m)\}.$$

Note that C is independent of the model.

Let S' be the union of S with the set of primes that were excluded by Pas's quantifier elimination, together with the primes that were excluded to make the rational constants in the valued field all units (or 0).

If $k \in \mathcal{K}_{S'}$, then θ is equivalent to Formula 1 in the interpretation k. By hypothesis, the set of solutions is bounded, which implies that each ψ_i^k, for $i \in \bar{B}$, is false. Hence all the solutions lie in C, as desired. □

3. Some virtual sets

We write

$$\theta(x_1, \ldots, x_\ell, m_1, \ldots, m_{\ell'}, \xi_1, \ldots, \xi_{\ell''})$$

for a formula in Pas's language, where all free variables are among those listed, and the variables are of the valued field sort x_i, value group sort m_i, and residue field sort ξ_i.

If $\theta(x_1, \ldots, x_\ell)$ is a formula in Pas's language with no free variables of residue field sort and no free variables of the value field sort, then we have the formula

$$\begin{aligned}&\exists m \ \forall y_1, \ldots, y_\ell, x_1, \ldots, x_\ell\\ &\quad (\theta(x_1, \ldots, x_\ell) \wedge (\mathrm{ord}(y_i - x_i) \geq m, \text{ for } i = 1, \ldots, \ell)\\ &\quad \Rightarrow \theta(y_1, \ldots, y_\ell).\end{aligned}$$

This formula does not contain any free variables. By quantifier elimination, this is equivalent to something of the shape of Formula 1. There are no free variables of the value group sort. By Presburger quantifier elimination, the formulas L_i can be replaced with "true" $1 = 1$ or "false" $0 = 1$. Thus, we may assume that the formula is a formula in the first order theory of the residue field sort. We say that $\theta(x_1, \ldots, x_\ell)$ is *stable* if the formula in the residue field sort is true for all pseudo-finite fields.[2] If the formula θ is stable,

[2] A field is pseudo-finite if it has a single extension of each degree and if each absolutely irreducible variety over the field has a rational point.

then by avoiding finitely many residue field characteristics, interpretations of $\{x : \theta(x)\}$ are stable definable sets. (*Stable* is meant in the sense of Denef and Loeser's motivic integration [3].)

A *virtual set* is a class construct

$$\{x : \theta(x)\},$$

where θ is a formula in Pas's language. See [8], where the corresponding notion for formulas in the first-order theory of rings is discussed.

Let $\mathfrak{g}$ be a virtual reductive Lie algebra in the sense of [8]; that is, a virtual set in Pas's language whose models are reductive Lie algebras in the traditional sense. Assume that $\mathfrak{g}$ is the Lie algebra of a virtual reductive Lie group G. (Again, this is to be interpreted as a virtual set whose models are reductive algebraic groups.) For example, each split reductive group over $\mathbb{Q}$ gives a virtual reductive group in Pas's language.

We define the space of *locally constant virtual functions* on $\mathfrak{g}$ to be the $\mathbb{Q}$-linear combinations of characteristic functions of stable virtual sets in $\mathfrak{g}$. More precisely, take the Grothendieck group generated by stable formulas in Pas's language, and tensor with $\mathbb{Q}$. Excluding finitely many primes, there is a map from this ring to the ring of locally constant $\mathbb{Q}$-valued functions on $\mathfrak{g}^k$ for p-adic field models k.

Let ℓ be the rank of $\mathfrak{g}$. Let $\mathrm{span}(Y, e_1, \ldots, e_\ell)$ be the formula in the first-order language of rings asserting that Y lies in the span of the e_i. The set of regular elements $\mathfrak{g}^{reg}$ is defined as a virtual set of elements in $\mathfrak{g}$

$$\{X \ : \ \exists e_1, \ldots, e_\ell\ \forall Y. \quad [X, Y] = 0 \ \Rightarrow\ \mathrm{span}(Y, e_1, \ldots, e_\ell)\}.$$

(The quantifiers in this formula have been extended to range over elements of $\mathfrak{g}$, as was done in [8].)

The set of nilpotent elements in $\mathfrak{g}$ is a subvariety, hence a virtual subset. A regular semisimple element is defined as a regular element that has 0 as the only nilpotent element in the centralizer. This condition is given by a formula, hence regular semisimple elements form a virtual set $\mathfrak{g}^{reg,ss}$.

In a split reductive algebra over $\mathbb{Q}$, we have a finite list of definable subsets of $\mathfrak{g}$ giving all of the proper parabolic subgroups P up to conjugacy. The virtual set of regular semisimple elliptic elements is given by

$$\cap_P \{X \in \mathfrak{g}^{reg,ss} \ : \ \text{There does not exist } g \in G \text{ such that } \mathrm{Ad}\, g(X) \in P\}.$$

Example 3. Consider the virtual set in $GL(2)$:

$$Z = \{\begin{pmatrix} a & b \\ ub & a \end{pmatrix} : \mathrm{ord}(u) = 0 \wedge \mathrm{ord}(a) \geq 0 \wedge \mathrm{ord}(b) \geq 0 \wedge a^2 - ub^2 \neq 0 \wedge b \neq 0\}.$$

This is a virtual subset of the set of regular semisimple elements. The condition for ellipticity for $X \in Z$ is

$$\exists A.\ AZ - ZA \in \begin{pmatrix} * & * \\ 0 & * \end{pmatrix}.$$

This is equivalent (excluding the prime 2) to the virtual subset of Z given by the condition

$$\exists \xi.\ \mathrm{ac}(u) = \xi^2.$$

4. An integration formula

Let $G = \sqcup_t KtK$ be the Cartan decomposition of the set G of p-adic points of a split reductive group over a p-adic field. Assume $t \in T$ the set of points of a split torus. The method of Cartier gives the following integration formula for functions supported on a single double coset KtK.

Theorem 4. *Let dk be a Haar measure on K. Let dg be a Haar measure on G. Then there exists a constant $c(KtK)$ such that for all $f \in C_c(KtK)$.*

$$c(KtK) \int_{K\times K} f(k_1 t k_2) dk_1\, dk_2 = \int_G f(g) dg.$$

Proof. Follow Cartier [2]. □

The constant can be obtained by taking f to be the characteristic function of KtK. We find that

$$c(KtK)\mathrm{vol}(K, dk)^2 = \mathrm{vol}(KtK, dg).$$

Pick dg so that its restriction to K is dk, and normalize dk so that

$$\mathrm{vol}(K, dk) = |G(\mathbb{F}_q)| q^{-\dim(G)}.$$

Let $[G]_q$ be the constant defined by the right-hand side of this equation.

5. The Main Result

Let $\mathfrak{g}$ be a split reductive group over $\mathbb{Q}$. Let G be a split reductive group over $\mathbb{Q}$ with Lie algebra $\mathfrak{g}$. We take $\mathfrak{g}$ and G to be represented explicitly as matrices in $\mathfrak{gl}(n)$ and $GL(n)$, respectively. Let O_v be the ring of integers of a completion L_v of a number field $L/\mathbb{Q}$. We may assume that $G(O_v) = GL(n, O_v) \cap G(L_v)$ is a hyperspecial maximal compact subgroup for almost all places v of L.

View $\mathfrak{g}$ and G as virtual subsets of the virtual sets $\mathfrak{gl}(n)$ and $GL(n)$. Let $\mathfrak{gl}(n, O)$ be the virtual subset of $\mathfrak{gl}(n)$ given by

$$\{(x_{ij})\ :\ \mathrm{ord}(x_{ij}) \ge 0,\ \forall i, j\}.$$

Set $\mathfrak{g}(O) = \mathfrak{gl}(n, O) \cap \mathfrak{g}$.

Let f be a locally constant virtual function on $\mathfrak{g}$. Let E be a stable virtual set of regular semisimple elliptic elements. (Recall that 'stable' is used here in the sense of stability in motivic integration, and not in the sense of stable conjugacy in group theory.) Assume that $E \subset \mathfrak{g}(O)$.

If L is a finite extension of $\mathbb{Q}$, and v is a place of L, the completion L_v at v is (the domain of) a model of Pas's language. Let O_v be the ring of integers of L_v. We write f_v for the locally constant function in that model. We write E_v for the definable subset of $\mathfrak{g}(O_v)$ obtained from the virtual set E. Assume that for almost all L_v, E_v is a compact set. (By 'almost all' here and in what follows, we mean all but finitely many residue field characteristics for L_v.)

A ring $K_0^v(\mathrm{Mot}_{\mathbb{Q},\bar{\mathbb{Q}}})_{\mathrm{loc},\mathbb{Q}}$ of virtual Chow motives is constructed by Denef and Loeser in [3]. The ring $K_0^v(\mathrm{Mot}_{\mathbb{Q},\bar{\mathbb{Q}}})_{\mathrm{loc},\mathbb{Q}}$ is defined as the image of a ring $K_0(\mathrm{Sch}_{\mathbb{Q}})_{\mathrm{loc}}$ in the Grothendieck ring of the category of Chow motives over $\mathbb{Q}$. The ring $K_0(\mathrm{Sch}_{\mathbb{Q}})_{\mathrm{loc}}$ is the Grothendieck ring of Chow motives over $\mathbb{Q}$, localized by inverting the class $\mathbb{L} = [\mathbb{A}^1_{\mathbb{Q}}]$ of the affine line. See [3] for details. In this paper, a *virtual Chow motive* M will always mean an element of this ring.

If v is a place of L, then there is a Frobenius operator Frob_v that acts on the ℓ-adic cohomology groups of M. See [3, 3.3]. We write the alternating trace of Frobenius on the cohomology as

$$\mathrm{trace}(\mathrm{Frob}_v, M) \in \bar{\mathbb{Q}}_\ell.$$

We fix measures on G_v (the set of p-adic points of G), and $\mathfrak{g}_v$ (the set of p-adic points of $\mathfrak{g}$) by fixing differential forms of top degree defined over $\mathbb{Q}$ on G and $\mathfrak{g}$. Normalize dX so that $\mathrm{vol}(\mathfrak{g}(O_v)) = 1$. Normalize dg to restrict to dk on $G(O_v)$. Normalize dk as in Section 4.

Theorem 5. *For each f and E, there is a virtual Chow motive $M(f, E)$ over $\mathbb{Q}$ and a finite set S of primes with the following property with the following property: If L is a finite extension of $\mathbb{Q}$ and v is a place of L that does not lie over any $p \in S$, then*

$$\mathrm{vol}(K, dk) \int_{E_v} \int_{G_v} f_v(g^{-1} X_v g)\, dg\, dX = \mathrm{trace}(\mathrm{Frob}_v, M(f, E)).$$

Remark 6. In general, a single elliptic element X in a p-adic field is not definable and the conjugacy class $O(X)$ is not definable. Thus, it is not reasonable to ask for a virtual Chow motive to represent the integral, except when averaged over E.

Remark 7. The same conclusion holds if we take our models to be $\mathbb{F}_q((t))$ instead of L_v. The Chow motive $M(f, E)$ is the same in both cases. Hence, we find as a corollary that the orbital integrals are "the same" in zero characteristic and positive characteristic.

Proof. In the course of the proof we increase the size of the finite set S of primes several times without a change in notation.

For any given L_v, the integral over G_v is a sum of integrals over KtK, as we run over all double cosets. For any given $X \in E_v$, there are only finitely many double cosets involved (because X is elliptic). The collection of double cosets required is locally constant in X, so there is a neighborhood of X that on which the finite set of cosets is the same as for X. By compactness on E_v, there is a finite cover by such neighborhoods. It follows that there is a finite set of double cosets depending only on E_v (and f_v).

For simplicity, we may assume that f_v is a characteristic function at L_v of a virtual set D. Let $m = (m_1, \dots, m_\ell)$ be a tuple of integers with ℓ equal to the reductive rank. Let T be a split torus that gives at each p-adic place the split torus that appears in the Cartan decomposition. Let $\phi : \mathbb{G}_m^{\times \ell} \to T$ be an isomorphism (defined over $\mathbb{Q}$) between a product of multiplicative groups and the diagonal torus T. Extend ord to $\mathrm{ord} : T \to \mathbb{Z}^\ell$ by

$$T \to \mathbb{G}_m^\ell \to^{\mathrm{ord}^\ell} \mathbb{Z}^\ell.$$

Let $\psi(m, k_1, k_2, X)$ be the formula in Pas's language given by

$$\begin{aligned} \exists t.\quad & X \in E \ \wedge\ \mathrm{Ad}(k_1 t k_2) X \in D \\ & \wedge\ \mathrm{ord}_v(t) = m \\ & \wedge\ k_1, k_2 \in \mathfrak{g}(O). \end{aligned}$$

Being in Pas's language, the formula is independent of the model (L, v). Let $\psi(m)$ be the formula

$$\exists\, k_1\, k_2\, X.\ \psi(m, k_1, k_2, X).$$

The formula $\psi(m)$ has a bounded number of solutions in each model θ_v. By Theorem 2, there is a finite set $C \subset \mathbb{Z}^\ell$ that contains the solutions in m for almost all models L_v. This implies that we can pick a finite collection of double cosets that works simultaneously for almost all models L_v. By the Cartan decomposition, we may assume that $m_1 \geq m_2 \geq \cdots$ for $m = (m_1, \dots, m_\ell) \in C$. Write K_m for the double coset

$$K\phi(\pi^m)K.$$

By the Cartier-style integration formula 4, the integral of the theorem can be written as

$$\sum_{m \in C} [K_m : K] \int_{E_v \times K \times K} \mathrm{char}(\psi(m, k_1, k_2, X)) dk_1\, dk_2\, dX.$$

By the main theorem of Denef and Loeser [3], for each m in this finite sum, there is a motive M_m such that the trace of Frobenius at v computes this volume. In their theorem, the p-adic volume is to be computed with respect to the Serre-Oesterlé measure on the group

$$G(O_v) \times G(O_v) \times \mathfrak{g}(O_v).$$

This measure is invariant under analytic isomorphisms of the set. In particular, it is invariant under the group action of

$$G(O_v) \times G(O_v) \times \mathfrak{g}(O_v)$$

on itself. Hence it is a Haar measure.

To work out the normalization of the Haar measure, we note that the Serrre-Oesterlé measure coincides with the counting measure modulo a uniformizer, scaled by $q^{-\dim(X)}$. Thus, the volume of this group is

$$[G]_q \times [G]_q.$$

For the normalization of dk and dX chosen in Section 4, the measure is also $[G]_q \times [G]_q$. Hence the Serre-Oesterlé measure coincides with the chosen Haar measure on this group.

The constant $[K_m : K]$, the number of cosets, is a polynomial in q with rational coefficients by MacDonald's formula [10, sec. 3.2]. This can be converted to a motive by replacing q with $\mathbb{L}$.

By summing over the finite set of $m \in C$, we obtain the result. □

6. Effective Calculations

Theorem 8. *The virtual Chow motive $M(f, E)$ is effectively computable from the data f and E.*

Remark 9. More precisely, we compute the virtual Chow motive as an explicit linear combination of classes $[h(X)]$, where each X is a smooth projective scheme over $\mathbb{Q}$, $h(X)$ is the virtual Chow motive associated with X, and $[h(X)]$ is its class in $K_0^v(\mathrm{Mot}_{\mathbb{Q},\bar{\mathbb{Q}}})_{\mathrm{loc},\mathbb{Q}}$. See [3, sec. 1.3]. Each scheme X is presented through a finite number of coordinate patches. Each patch is given by an explicit list of polynomials $f_1, \ldots, f_k$ in n variables such that the affine patch is isomorphic to $\mathbb{Q}[x_1, \ldots, x_n]/(f_1, \ldots, f_k)$. The maps between coordinate patches are given by explicit polynomials.

Proof. It is enough to prove the result when f is the characteristic function of a stable virtual set D in $\mathfrak{g}$.

Pas's algorithm is an effective procedure [11]. In fact, although Pas assumes for simplicity that the residue field has characteristic zero, the finite set of prime characteristics that must be avoided (for a given formula in the language) can be effectively calculated from his algorithm.

The Presburger algorithm is an effective procedure [5].

Combining Pas's algorithm and the Presburger algorithm, we have an effective procedure for determining effective bounds on the solutions of each L_i of Formula 1, for each $i \in B$. Thus, the set C is effectively computable. This means that an effective bound can be obtained on the number of double cosets that must be considered.

Lemma 10. *For each m, the set*

$$\{(k_1, k_2, X) : \psi(m, k_1, k_2, X)\}$$

is a stable virtual subset of $G(O) \times G(O) \times \mathfrak{g}(O)$. The level of stability is effectively computable.

Proof. Fix m. For each model L_v, it follows directly from compactness of E_v, K_m, and the stability of D_v and E_v that the corresponding p-adic set is a stable subset of $G(O_v) \times G(O_v) \times \mathfrak{g}(O_v)$. (This is an expression of the well-known fact that orbital integrals are locally constant on the set of regular semisimple elements.)

Extend ord to a function symbol on matrices $X = (x_{ij})$ by defining

$$\mathrm{ord}(X) = \min_{ij} \mathrm{ord}(x_{ij})$$

Let $\theta(n) = \theta_m(n)$ be the formula in Pas's language given by

$$\begin{array}{l} \forall k_1\, k_2\, k_1'\, k_2'\, X\, X'. \\ \quad (\psi(m, k_1, k_2, X) \\ \quad \wedge \mathrm{ord}(k_1 - k_1') \geq n \wedge \mathrm{ord}(k_2 - k_2') \geq n \wedge \mathrm{ord}(X - X') \geq n) \\ \quad \Rightarrow \psi(m, k_1', k_2', X'). \end{array}$$

The formula asserts the stability ψ at level n. Let $\theta'(n)$ be the formula in Pas's language given by

$$\theta(n) \;\wedge\; \left(\forall n' < n.\ \neg\theta(n')\right).$$

It asserts that n is the least level for which it is stable. By the stability of each model L_v and Theorem 2, we find that there is a level n at which almost all models are stable. This level is effective for the same reasons that the set C above is. □

Now we continue with the proof that $M(f, E)$ is effectively computable. By quantifier elimination, for each m, the formula $\psi(m, k_1, k_2, X)$ can be replaced by an explicit special formula (in the sense of [3, sec. 5.3]). Let n be the level of stability. Truncation $\tau_n(\psi)$ at level n gives a formula in $\mathcal{L}_n(G \times G \times \mathfrak{g})$ (the truncated arc-space of [3, sec. 5.4]), or equivalently the formula

$$\psi' = \tau_n(\psi) \wedge (x \in G \times G \times \mathfrak{g}).$$

This formula may be considered as a formula in the first-order theory of rings. (More explicitly, we work in the model $\mathbb{Q}[[t]]$. We replace quantification of k_1, k_2, X with quantifiers over the matrix coefficients, and each matrix coefficient is expanded as a truncated power series $x_{ij} = z_0 + z_1 t + z_2 t^2 + \cdots$.)

By the definitions in [3], we have

$$M(f, E) = \chi_c(\psi')\mathbb{L}^{-(n+1)d},$$

where d is the dimension of $G \times G \times \mathfrak{g}$.

To conclude the proof, we check that χ_c can be made effective for presented formulas ψ' in the first order theory of rings. The procedure is as follows. We write ψ' in prenex normal form to get a Galois formula as in [3, sec. 2.2]. Quantifier elimination transforms the Galois formula into a Galois stratification. This procedure is effective [6, ch. 26]. (See also [3, 2,3,3].) The Galois group is presented as an explicit subgroup of a symmetric group. Part of the data obtained from the Galois stratification is a central function on the Galois group.

By [6, 26.12], Artin induction is effective, giving the central function as an explicit rational combination of characters induced from the trivial character on cyclic subgroups. (Fried and Jardin state the lemma for $\mathbb{Q}$-valued characters, but in our case the characters are take values in a cyclotomic extension of $\mathbb{Q}$. The degree of the cyclotomic extension is effectively computable from the degree of the Galois cover. We can then extend the Fried-Jardin result by picking an explicit $\mathbb{Q}$-basis for the cyclotomic extension.)

By refining the Galois stratification as necessary, we may assume that the Galois stratification is affine, that is each C/A is a ring cover in the sense of [6]. Artin induction and the properties of χ_c established in [3] reduce the problem to computing $\chi_c(X/H)$, where X is affine with a cyclic group action H, and the data (X, H) are explicitly given. The calculation of the quotient amounts to computing the invariants of $\mathbb{Q}[X]$ under the finite group H. There are several implementations of algorithms to compute this ring of invariants. (A survey of implementations appears for example in [4, page 2].)

To compute the class $\chi_c(X)$ where X is an affine variety, embed it in a smooth projective variety $\tilde{X}$. By constructive resolution of singularity algorithms [1], $\tilde{X}$ can be effectively computed from X. By the properties of the map χ_c,

$$\chi_c(X) = [h(\tilde{X})] - \chi_c(D),$$

where $[h(\cdot)]$ is as in Remark 9. The divisor D has lower dimension. Part of the constructive resolution of singularities gives a description of the irreducible components of D. By induction on dimension, we may assume that $\chi_c(D)$ is known.

This completes the proof that $M(f, E)$ can be effectively computed. □

References

[1] G. Bodnár and J. Schicho, A computer program for the resolution of singularities, preprint 1999.

[2] P. Cartier, Representations of p-adic groups: a survey, in Automorphic Forms, Representations, and L-functions, Corvallis, Symp. in Pure Math, AMS XXXIII, part 1, 1977.

[3] J. Denef, F. Loeser, *Definable sets, motives, and p-adic integrals*, Journal of the AMS, **14**, No. 2, 429-469 (2001).

[4] H. Derksen, Constructive Invariant Theory and the Linearization Problem, Ph. D. thesis, University of Basel, 1997, http://www.math.lsa.umich.edu/ hderksen/preprint.html.

[5] H. B. Enderton, A mathematical introduction to logic. Second edition. Harcourt/Academic Press, Burlington, MA, **2001**.

[6] 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.

[7] J. Gordon, thesis, University of Michigan, 2002.

[8] J. Gordon and T. Hales, Virtual Transfer Factors, http://xxx.lanl.gov/abs/math.RT/0209001, preprint 2002.

[9] T. C. Hales. Can p-adic integrals be computed? to appear.

[10] I. G. MacDonald, Spherical Functions on a Group of p-adic Type, Publ. of the Ramanujan Inst. Number 2, 1971.

[11] J. Pas, *Uniform p-adic cell decomposition and local zeta functions.* J. Reine Angew. Math. **399** (1989), 137–172.