

Algebra & Number Theory

Volume 14
2020
No. 5

Mixed Tate motives and the unit equation II

Ishai Dan-Cohen



Mixed Tate motives and the unit equation II

Ishai Dan-Cohen

Over the past fifteen years or so, Minhyong Kim has developed a framework for making effective use of the fundamental group to bound (or even compute) integral points on hyperbolic curves. This is the third installment in a series whose goal is to realize the potential effectivity of Kim’s approach in the case of the thrice punctured line. As envisioned by Dan-Coehn and Wewers (2016), we construct an algorithm whose output upon halting is provably the set of integral points, and whose halting would follow from certain natural conjectures. Our results go a long way towards achieving our goals over the rationals, while broaching the topic of higher number fields.

1. Introduction	1175
2. Conjectures and theorems	1185
3. Construction of arithmetic algorithms	1195
4. Construction of geometric algorithms	1215
5. Construction of analytic algorithm	1217
6. Numerical approximation	1219
7. The equation-solving algorithm	1231
8. Beyond totally real fields	1233
Appendix: A minor erratum	1235
Acknowledgements	1235
References	1235

1. Introduction

1.1. This is the third installment in a series [Dan-Cohen and Wewers 2015; 2016]¹ devoted to what may reasonably be described as *explicit motivic Chabauty–Kim theory*. “Chabauty–Kim theory” refers to a framework developed by Minhyong Kim for making effective use of the fundamental group to bound, or conjecturally compute, integral solutions to hyperbolic equations. “Motivic” refers to the fact that while Kim’s construction, in its original formulation, is p -adic étale, our methods are motivic. As things currently stand, this limits us to working in the mixed Tate, or Artin–Tate settings, that is, essentially to the projective line with (possibly interesting) punctures. So the adjective “motivic” implies a fairly

This work was supported by Priority Program 1489 of the Deutsche Forschungsgemeinschaft: *Experimental and algorithmic methods in algebra, geometry, and number theory*.

MSC2010: primary 11G55; secondary 11D45, 14F30, 14F35, 14F42, 14G05.

Keywords: mixed Tate motives, unipotent fundamental group, p -adic periods, polylogarithms, unit equation, integral points.

¹*Explicit Chabauty–Kim theory for the thrice punctured line in depth two = Mixed Tate motives and the unit equation 0.*

specific context. While this context may seem narrow from a geometric point of view, it is quite broad from an arithmetic point of view, leading and relating to various interesting questions and conjectures.

“Explicit” refers to the fact that here our emphasis is on algorithms. *Explicit* Chabauty–Kim theory, as I see it, is somewhat orthogonal to Chabauty–Kim theory proper. If *Chabauty–Kim theory* is about attempting to prove Kim’s conjecture [Balakrishnan et al. 2018], or at least about formulating and studying a range of related conjectures, *Explicit* Chabauty–Kim theory is about making the theory *explicit*. In particular, in the explicit theory, we allow ourselves to assume conjectures left and right, so long as those affect the halting, and not the construction, of the hoped-for algorithms.

In this installment, we continue our study of $\mathbb{P}^1 \setminus \{0, 1, \infty\}$. We obtain an algorithm for computing the *polylogarithmic Chabauty–Kim loci* (see below) over number fields which obey a certain technical condition. In turn, this technical condition is known for the rationals and follows for general number fields from a conjecture due to Jannsen. We also obtain an algorithmic solution to the unit equation over totally real fields obeying the same condition. Specializing to the case of the rationals, we obtain the algorithm envisioned by Dan-Cohen and Wewers [2016].

1.2. We now state our main application in more detail. Let $X = \mathbb{P}^1 \setminus \{0, 1, \infty\}$. Below, we construct an algorithm which takes as input an open integer scheme Z (by which we mean an open subscheme of $\text{Spec } \mathcal{O}_K$ for K a number field), and outputs a subset of $X(Z)$.

Theorem 1.2.1. *Let Z be a totally real open integer scheme. If our algorithm halts for the input Z , then its output is equal to the set $X(Z)$ of integral points of X over Z .*

We also state four conjectures: *Zagier’s conjecture*, *Goncharov exhaustion (with weak control over ramification)*, the *p -adic period conjecture*, and *convergence of Chabauty–Kim loci for the polylogarithmic quotient*. Finally, we state our technical condition, which we call *Hasse principle for finite cohomology*. We say that K obeys *Kim vs. Hasse* if convergence occurs *before* the Hasse principle fails (see below for details). The following proposition motivates the theorem above.

Proposition 1.2.2. *Let Z be a totally real open integer scheme with fraction field K :*

- (1) *Assume Zagier’s conjecture, Goncharov exhaustion, the p -adic period conjecture, and convergence of Chabauty–Kim loci for the polylogarithmic quotient hold for Z . Assume K obeys Kim vs. Hasse. Then our algorithm halts for Z .*
- (2) *Suppose Z is contained in $\text{Spec } \mathbb{Z}$. Assume Goncharov exhaustion, the p -adic period conjecture, and convergence of Chabauty–Kim loci for the polylogarithmic quotient hold for Z . Then our algorithm halts for Z .*

We refer to Theorem 1.2.1 and Proposition 1.2.2, taken together, as the “equation-solving theorem”; see Theorem 7.2.1 for a more precise statement.

Practical (and unconditional) methods for solving the S -unit equation predate this work, and can be found, for instance, in de Weger [1989] who uses the theory of logarithmic forms of Baker and Wüstholz [2007] (see also [Evertse and Györy 2015] for a general discussion). A more recent approach, due to von

Känel and Matschke [2016] is based on the Shimura–Taniyama conjecture. Our primary purpose here is not to compete with these other methods, but rather, to develop Kim’s theory in a special case, to explore its interaction with the theory of mixed Tate motives and motivic iterated integrals, and, in subsequent works, to provide new numerical evidence for Kim’s conjecture. Also, while our focus here is *explicit*, it is not yet *practical*; see segment 1.15.1 below.

1.3. We now give a brief indication of our main result, from which the equation-solving theorem follows as a corollary; precise statements, as well as more background, appear in Section 2 below. For this purpose, fix a prime $\mathfrak{p} \in Z$ which we assume to be totally split and recall that there is a commutative diagram like so:

$$\begin{array}{ccc} X(Z) & \longrightarrow & X(Z_{\mathfrak{p}}) \\ \kappa \downarrow & & \downarrow \kappa_{\mathfrak{p}} \\ \mathbb{Q}_p \otimes H^1(U_{\geq -n}^{\text{PL}}) & \xrightarrow{\mathfrak{A}_{\mathfrak{p}}} & H^1(U_{\geq -n}^{\text{PL}, F\phi}) \end{array}$$

Here $Z_{\mathfrak{p}}$ denotes the complete local scheme of Z at \mathfrak{p} , isomorphic to $\text{Spec } \mathbb{Z}_{\mathfrak{p}}$, and $U_{\geq -n}^{\text{PL}}$ denotes the level- n quotient of the polylogarithmic quotient of the unipotent fundamental group of X at the tangential base point $\vec{1}_0$, a certain quotient of a unipotent, motivic version of the fundamental group. The cohomology variety $H^1(U_{\geq -n}^{\text{PL}})$ appearing below left is a certain \mathbb{Q} -variety parametrizing torsors for $U_{\geq -n}^{\text{PL}}$. The vertical map κ sends an integral point x to the torsor of homotopy classes of paths

$$1_0 \rightarrow x.$$

The cohomology variety appearing in the lower-right is a certain p -adic variant of the one to its left, based, as the notation suggests, on the theory of filtered ϕ modules. In terms of this diagram, we define

$$X(Z_{\mathfrak{p}})_n := \kappa_{\mathfrak{p}}^{-1}(\text{Im } \mathfrak{A}_{\mathfrak{p}}).$$

We construct an algorithm for computing the locus $X(Z_{\mathfrak{p}})_n$ to given p -adic precision.

Theorem 1.3.1 (see Theorem 2.4.1 below). *Let Z be a totally real open integer scheme, \mathfrak{p} a totally split prime, n a natural number, and $\epsilon > 0$. If our algorithm halts for these inputs, then the functions $\tilde{F}_i^{\mathfrak{p}}$ which the algorithm returns as output take values less than ϵ on $X(Z_{\mathfrak{p}})_n$.*

1.4. The main problem of explicit Chabauty–Kim theory is to render the map $\mathfrak{A}_{\mathfrak{p}}$ computationally accessible; in the case at hand, we proceed as follows. Let $U(Z)$ denote the unipotent part of the fundamental group of the category of mixed Tate motives over Z . If $Z^o \subset Z$ is an open subscheme, there’s an associated surjection

$$U(Z^o) \twoheadrightarrow U(Z).$$

As part of the algorithm, we search for a Z^o such that $U(Z^o)$ admits a *nice* set of coordinates. More will be said about the role played by Z^o below; for now, let us fix Z^o arbitrarily. A theory of p -adic iterated

integration due to Coleman and Besser gives rise to a point

$$I_{BC} : \text{Spec } \mathbb{Q}_p \rightarrow U(Z^o).$$

Our construction revolves around the following diagram:

$$\begin{array}{ccc}
 \text{Spec } \mathbb{Q}_p \times H^1(U_{\geq -n}^{\text{PL}}) & \xrightarrow{\mathfrak{R}_p} & H^1(U_{\geq -n}^{\text{PL}, F\phi}) \\
 \parallel & & \parallel \\
 \text{Spec } \mathbb{Q}_p \times Z^1(U(Z), U_{\geq -n}^{\text{PL}})^{\mathbb{G}_m} & \xrightarrow{\text{ev}_{I_{BC}}} & \text{Spec } \mathbb{Q}_p \times U_{\geq -n}^{\text{PL}} \\
 I_{BC} \times Id \downarrow & & \downarrow I_{BC} \times Id \\
 U(Z^o) \times Z^1(U(Z), U_{\geq -n}^{\text{PL}})^{\mathbb{G}_m} & \xrightarrow{\text{ev}_{\text{Everywhere}}} & U(Z^o) \times U_{\geq -n}^{\text{PL}}
 \end{array}$$

Here $Z^1(U(Z), U_{\geq -n}^{\text{PL}})^{\mathbb{G}_m}$ denotes a certain space of \mathbb{G}_m -equivariant cocycles

$$U(Z) \rightarrow U_{\geq -n}^{\text{PL}},$$

and the maps $\text{ev}_{I_{BC}}$, $\text{ev}_{\text{Everywhere}}$ are evaluation maps. Instead of attempting to compute the scheme-theoretic image $\text{Im } \mathfrak{R}_p$ directly, we compute the pullback

$$(I_{BC} \times Id)^{-1}(\text{Im } \text{ev}_{\text{Everywhere}}). \tag{*}$$

1.5. The group $U(Z^o)$ possesses certain special functions, known as *motivic iterated integrals*, whose pullbacks along I_{BC} are p -adic iterated integrals. The latter may be computed to arbitrary precision thanks to the algorithm of Dan-Cohen and Chatzistamatiou [2014], which we review in Section 6 below. In order to compute $\text{Im } \text{ev}_{\text{Everywhere}}$ as well as its pullback (*) algorithmically, we need coordinates on $U(Z^o)$. Moreover, as the algorithm proceeds, we need to impose different, in fact contradictory, conditions on our coordinate system: to compute the pullback along I_{BC} , we need our coordinate functions to be given explicitly in terms of motivic iterated integrals. To compute the image

$$\text{Im } \text{ev}_{\text{Everywhere}}$$

however, we need coordinates compatible with the product on $U(Z^o)$. In the construction that follows, we attempt to bridge this gap; we fail in many ways, but are nevertheless able to make the error incurred arbitrarily small.

This work does not have significant logical dependence on its predecessors [Dan-Cohen and Wewers 2015; 2016]. The reason for this, in part, is that I found it preferable to modify portions of the work done in [Dan-Cohen and Wewers 2016] in preparation for the construction of the algorithm. For instance, our use of the map “ $\text{ev}_{\text{Everywhere}}$ ” here (along with our acceptance of the p -adic period conjecture as yet another condition for halting) allows us to carry out the geometric part of the computation in a single step over the rationals and in a manner entirely divorced from arithmetic. In fact, the relationship between the

present work and the latter is rather reversed: [loc. cit.] may be seen as working out a particular example of the algorithm constructed here.

1.6. After making precise the conjectures and theorems indicated above in Section 2, we begin in segments 3.1 and 3.2 by studying formal properties of coordinate systems on $U(Z^\circ)$ which promise to shrink the apparent gap between computable properties of motivic iterated integrals and the desired compatibility with product. The result, which is summarized in Propositions 3.2.2 and 3.2.3, consists of conditions on a basis \mathcal{A} for the Hopf algebra $A(Z^\circ)$ of functions on $U(Z^\circ)$, given as a disjoint union of three subsets

$$\mathcal{A} = \mathcal{E} \cup \mathcal{P} \cup \mathcal{D},$$

under which

$$\mathcal{E} \cup \mathcal{P}$$

forms an algebra basis of the polynomial algebra $A(Z^\circ)$, and the set \mathcal{E}^\vee of dual elements forms a set of free generators for the Lie algebra

$$\mathfrak{n}(Z^\circ) := \text{Lie } U(Z^\circ).$$

Our terminology gives a rough idea of the roles played by these subsets: \mathcal{E} consists of *extensions*, \mathcal{P} of *primitive nonextensions*, and \mathcal{D} of *decomposables*.

1.7. Let $U(Z_p)$ (or $U(\mathcal{O}_p)$) denote the unipotent part of the fundamental group of the Tannakian category of mixed Tate filtered ϕ modules of Chatzistamatiou and Ünver [2013].² Let $A(Z_p)$ denote the *mixed Tate filtered ϕ Hopf algebra*, that is, the Hopf algebra of functions on $U(Z_p)$. Unlike the motivic Galois group $U(Z^\circ)$, the filtered ϕ Galois group $U(Z_p)$ possesses a canonical set of free generators which give rise, dually, to a set of *standard* basis elements in $A(Z_p)$. There is a *realization map*

$$\text{Re}_p : A(Z^\circ) \rightarrow \prod_{p|P} A(Z_p).$$

Given a motivic iterated integral in $A(Z^\circ)$, we may wish to expand its realization in the standard basis. In segment 3.7 we upgrade the algorithm of [Dan-Cohen and Chatzistamatiou 2014] to an algorithm which computes p -adic approximations of this expansion; we refer to this algorithm as the *realization algorithm*. Examples of this algorithm are worked out in [Dan-Cohen and Wewers 2016, Section 7.5] for $Z = \text{Spec } \mathbb{Z}[\frac{1}{2}]$:³

- (1) In segment 7.5.1 we compute, in the notation of that paper, the p -adic number $(\log^{F\phi} 2)(v_{-1})$.
- (2) In segment 7.5.2 we compute, for instance, $(\log^{F\phi} 2)^2(v_{-2})$.

²The same symbols might be used to denote the unipotent part of the fundamental group of the category of mixed Tate motives over Z_p if such a category exists; but this hypothetical group will not intervene in this paper.

³Actually, when Z is an open subscheme of $\text{Spec } \mathbb{Z}$ (and the higher motivic extension groups are hence of dimension ≤ 1), this algorithm may be replaced by a single direct period-computation; see [Corwin and Dan-Cohen 2018a; 2018b].

(3) In segment 7.5.3 we compute $\text{Li}_3^{F\phi}(b)(w)$ for

$$w \in \{v_{-1}^3, v_{-1}v_{-2}, v_{-2}v_{-1}, v_{-3}\}.$$

1.8. Next comes our “basis algorithm” and our “change of basis algorithm”. In comparison with the sketch of our algorithm in [Dan-Cohen and Wewers 2016, Section 5.7], the basis algorithm corresponds to step 1 (segment 5.7.1) while the change of basis algorithm is a part of step 2 (segment 5.7.2).⁴ This material was inspired by Brown [2012].

In segment 3.8 below we attempt to construct a basis \mathcal{A} of iterated integrals for $A(Z^o)$ (varying $Z^o \subset Z$ as we search) which fulfills the conditions of Proposition 3.2.2. The result is our basis algorithm. Examples can be found in [Dan-Cohen and Wewers 2016, Section 7.5] when we find a basis of $A(Z^o)_n$ for $n = 1, 2, 3, 4$ consisting of unipotent motivic polylogarithms. For instance, in Proposition 7.5.4.1 of [loc. cit.], we find that a basis for $A(\mathbb{Z}[\frac{1}{2}])_4$ is given by

$$\mathcal{B} = \{(\log^U 2)^4, (\log^U 2)\zeta^U(3), \text{Li}_4^U(\frac{1}{2})\}.$$

When constructing the basis algorithm, one problem we face is that we are unable to verify algorithmically if a given iterated integral in $A(Z^o)_r$ belongs to the subspace

$$E(Z^o)_r := \text{Ext}_{\mathcal{MT}(Z)}^1(\mathbb{Q}(0), \mathbb{Q}(r)) \subset A(Z^o)_r$$

of extensions. Using the realization algorithm, however, we can bound the distance between a given iterated integral and the extension space, and so bound the error thus incurred. We are thus forced to work with two potentially distinct bases. One basis, denoted by $\tilde{\mathcal{A}}$, is given concretely and explicitly by motivic iterated integrals, but is imperfect in that its set

$$\tilde{\mathcal{E}} \subset \tilde{\mathcal{A}}$$

of alleged extensions may actually fail to be extensions. By projecting $\tilde{\mathcal{E}}$ onto the space of extensions we obtain a second basis, \mathcal{A} , which is perfect in its fulfillment of the conditions of Proposition 3.2.2 on the one hand, but is merely *abstract* on the other hand, as its definition is not constructive.

1.9. Let us briefly visit segment 3.8.11, where the construction becomes somewhat intricate. The construction is recursive in $n \geq 2$. As soon as we have a basis $\tilde{\mathcal{A}}_{\leq n}$ of motivic iterated integrals in half-weights $\leq n$, we want to also be able to expand an arbitrary iterated integral in half-weight n in the given basis, or, more generally, to compute the inner product of two arbitrary iterated integrals in half-weight n (for the standard inner product $\langle v_i, v_j \rangle = \delta_{i,j}$ induced by this basis). We don’t hope to be able to do this precisely; instead we aim for an ϵ -approximation

$$\langle J, I \rangle_\epsilon.$$

⁴Indeed, segment 5.7.2 of [loc. cit.] is a mixture of our *change of basis* algorithm with our “cocycle-image-evaluation algorithm”.

Segment 3.8.8 of our algorithm is key in setting the stage for this computation. Under our “Hasse principle”, the realization map is injective near the extension groups (see segment 3.8.14). We may therefore require that the realization of our subset

$$\tilde{\mathcal{E}}_n \subset \tilde{\mathcal{A}}_n$$

of near-extensions be linearly independent inside $\prod A(Z_p)$; the precise statement is complicated by the fact that our realization map is itself merely an approximation. Computation of the inner products $\langle J, I \rangle_\epsilon$ for $J \in \mathcal{P}_n \cup \tilde{\mathcal{D}}_n$ reduces to computations in lower weights via the *Goncharov coproduct*, an explicit formula for the coproduct of two motivic iterated integrals due to Goncharov [2005]. For the remaining inner products, $\langle J, I \rangle_\epsilon$ with $J \in \tilde{\mathcal{E}}_n$, we use the realization algorithm to map the remaining part I' of I and J into $\prod A(Z_p)$ and compute there. Our requirement that $\text{Re}_p \tilde{\mathcal{E}}_n$ be linearly independent ensures that the resulting system of linear equations will have a unique solution.

1.10. Given our abstract basis

$$\mathcal{A} = \mathcal{E} \cup \mathcal{P} \cup \mathcal{D}$$

of $A(Z^o)$, we obtain a set

$$\Sigma^o := \mathcal{E}^\vee$$

of free generators for the Lie algebra $\mathfrak{n}(Z^o)$. The set Φ of words in Σ^o forms a basis for the universal enveloping algebra $\mathcal{U}(Z^o)$; its dual

$$\mathcal{F} \subset A(Z^o)$$

gives us a new basis, which plays nicely with the Hopf-algebra structure; we call such a basis a *shuffle basis*. We also have an exponential map

$$\exp^\sharp : U(Z^o) \xrightarrow{\sim} S^\bullet \mathfrak{n}(Z^o)^\vee$$

and we may compute the images

$$\exp^\sharp(f_w)$$

of the elements f_w of \mathcal{F} as Lie-words in Σ^o . We do not endeavor to carry this out explicitly here, contenting ourselves with the observation that the procedure is in an elementary sense algorithmic.

More interesting is the need to compare the two bases \mathcal{A} and \mathcal{F} of $A(Z^o)$. In segment 3.9, we approximate such a comparison by using our imperfect, concrete basis $\tilde{\mathcal{A}}$ to construct a near-shuffle basis $\tilde{\mathcal{F}}$, and by computing the associated change-of-basis matrix to given p -adic precision. This is our change of basis algorithm. An example is worked out in segment 7.6.3 of [Dan-Cohen and Wewers 2016].

1.11. In terms of a set of generators Σ^o for the unipotent motivic Galois group $U(Z^o)$, the problem of computing the image of $\text{ev}_{\text{Everywhere}}$ becomes purely classical (if not quite formal); we make this precise in segment 4.1 below. We let \mathfrak{n}^{PL} denote the Lie algebra of the polylogarithmic quotient U^{PL} of the

unipotent fundamental group of X , and we let $\mathfrak{n}(\Sigma^o)$ denote the free pronilpotent Lie algebra on Σ^o . The result is given as a finite family

$$\{F_i^{\text{abs}}\}_i$$

of elements of

$$S^\bullet(\mathfrak{n}_{\geq -n}^{\text{PL}} \times \mathfrak{n}(\Sigma^o)_{\geq -n})^\vee.$$

1.12. The unipotent fundamental group $U(X)$ at the tangent vector 1_0 is canonically free prounipotent on two generators e_0, e_1 corresponding to monodromy about the punctures 0 and 1, respectively. As such, its coordinate ring $\mathcal{O}(U(X))$ possesses a canonical vector space basis $\{\text{Li}_\omega\}_\omega$ where ω ranges over words in the two generators. We abbreviate words in e_0, e_1 by words in 0, 1. The polylogarithmic quotient

$$U(X) \twoheadrightarrow U^{\text{PL}}$$

corresponds to the subalgebra generated by elements

$$\log := \text{Li}_0, \quad \text{Li}_1 := \text{Li}_1, \quad \text{Li}_2 := \text{Li}_{10}, \quad \text{Li}_3 := \text{Li}_{100}, \quad \dots$$

In segment 4.2 we use the change-of-basis matrix of segment 3.9 to convert the elements F_i^{abs} into functions on

$$U(Z^o) \times U_{\geq -n}^{\text{PL}}$$

given as elements \tilde{F}_i of the polynomial ring

$$\mathbb{Q}[\tilde{\mathcal{E}} \cup \mathcal{P}, \log, \text{Li}_1, \dots, \text{Li}_n].$$

There is a natural map

$$\mathbb{Q}[\tilde{\mathcal{E}} \cup \mathcal{P}, \log, \text{Li}_1, \dots, \text{Li}_n] \rightarrow \text{Col}(X(Z_p))$$

to the ring of Coleman functions, which we use to obtain the hoped-for family

$$\{\tilde{F}_i^p\}_i$$

of Coleman functions. Having completed the construction of the ‘‘Chabauty–Kim-loci’’ algorithm, $\mathcal{A}_{\text{Loc}i}$, we prove our main theorem in segment 4.2.6.

1.13. In Section 5 we use Newton polygons to bound the number of roots in small neighborhoods, and in Section 6 we review unpublished joint work with Andre Chatzistamatiou devoted to the computation of p -adic iterated integrals, on which we’ve already relied at several points.

We’re now ready to construct the equation-solving algorithm of Theorem 1.2.1. Joint work with David Corwin [Corwin and Dan-Cohen 2018a] demonstrates the need for symmetrization with respect to the S_3 action on X . We set

$$X(Z_p)_n^{S_3} := \bigcap_{\sigma \in S_3} \sigma(X(Z_p)_n)$$

(see segment 2.1.3 for the precise definition). We search for points to obtain a gradually increasing list

$$X(Z)_n \subset X(Z).$$

At the same time we construct Coleman functions \tilde{F}_i^p vanishing on $X(Z_p)_n^{S_3}$ and use those to obtain a gradually decreasing union of neighborhoods. Thus, roughly speaking, $X(Z)$ is sandwiched

$$X(Z)_n \subset X(Z) \subset X(Z_p)_n^{S_3}$$

with $X(Z)_n$ gradually increasing while $X(Z_p)_n^{S_3}$ gradually decreases. We stop when the two sides meet. This concludes the construction of our equation-solving algorithm \mathcal{A}_{ES} , and allows us to state and prove the equation-solving theorem (segment 7.2).

1.14. In Section 8 we generalize Theorem 1.3.1 to allow arbitrary open integer schemes. Essentially the only difference is that one is forced to replace $X(Z_p)$ with the product $\prod_{p|p} X(Z_p)$. We are unable at this point, however, to obtain an equation-solving algorithm in this generality: to do so we would have to study solutions to systems of locally analytic functions on higher-dimensional spaces.

1.15. *Near-term goals.*

1.15.1. *Algorithmic precision.* The algorithmic constructions we make in this installment are precise by mathematical standards, but not by algorithmic standards, which are far more stringent. For instance, we do not attempt to make our ϵ 's precise: any function of ϵ which is algorithmically computable, and which goes to zero with ϵ , is again denoted by ϵ — we refer to this as an *admissible change in ϵ* . Such imprecision is common in pure math, but useless for applications. Before going to Sage, we will of course have to compute exact levels of accumulated error as we make our approximations.

We also make no attempt to make our algorithm efficient: whenever we have a countable set, we don't hesitate to search through it arbitrarily. In fact, the problem of making our algorithm efficient interacts with significant, interesting problems of pure math; these include formulating explicit forms of Zagier's conjecture (available so far in only very special cases), and more precise versions of Goncharov's conjecture, at least with respect to ramification. Avoiding redundancy in our search through the set of iterated integrals is another interesting problem. Indeed, as Francis Brown has pointed out, as long as we limit ourselves to working with the polylogarithmic quotient, constructing a basis for all of $A(Z)_{\leq n}$ is huge overkill: any \mathbb{G}_m -equivariant map

$$U(Z) \rightarrow U(X)_{\geq -n}^{\text{PL}}$$

must factor through a small quotient of $U(Z)$ (easily computed in terms of abstract coordinates). A careful study of this quotient should yield a conjecture which is both much weaker than Goncharov's conjecture, and much more efficient for us.⁵

⁵We alert the reader to the forthcoming works *The Goncharov quotient in computational Chabauty–Kim theory I and II* by the author and David Corwin in which this is carried out for open subschemes of $\text{Spec } \mathbb{Z}$ and new numerical results are obtained.

With regard to the endeavor to produce actual code, we would expect to push the computational boundary gradually, starting with very special cases in which the conjectures of Zagier and Goncharov are relatively well understood.

1.15.2. Comparison with Brown’s method. In the spring of 2014 I visited Francis Brown at the IHES in order to discuss the previous installment in this series [Dan-Cohen and Wewers 2016]. Our meeting was inspiring and reassuring and helped me in developing the algorithm presented below.

Since then, Brown [2017] has made his own contribution to the subject in which he develops a method (or a kind of blueprint) for constructing *many* polylogarithmic functions on the p -adic points of $\mathbb{P}^1 \setminus \{0, 1, \infty\}$ over an open subscheme of $\text{Spec } \mathbb{Z}$ which vanish on integral points, at least when there are *enough* integral points. His idea is that if Goncharov’s conjecture is false, there should actually be *more* such functions available, increasing the chances of isolating the set of integral points. His assumption that X has many points replaces our reliance on Goncharov’s conjecture for halting, and one of his goals, which he achieves in several examples, is to circumvent our construction of a basis of the mixed Tate–Hopf algebra $A(Z)$. A particularly satisfying outcome is a more economic and aesthetic construction of the polylogarithmic function constructed in [Dan-Cohen and Wewers 2016].⁶

Work remains to be done in comparing Brown’s construction with ours, and hopefully, in harnessing the power of both approaches to construct more efficient, and more enlightening, algorithms.

1.15.3. Beyond totally real fields. Most of the work completed here applies to arbitrary open integer schemes which obey *Kim vs. Hasse*. For the final application, however, we are limited to the totally real case. As mentioned above, in order to go further, we would have to develop methods for computing solutions to systems of polylogarithmic functions in higher dimensions.

1.15.4. Beyond the polylogarithmic quotient. Beyond the polylogarithmic quotient, the motivic Selmer variety

$$H^1(G(Z), U(X)_{\geq -n})$$

is still canonically isomorphic to the space

$$Z^1(U(Z), U(X)_{\geq -n})^{\mathbb{G}_m}$$

of \mathbb{G}_m -equivariant cocycles. Explicit computation of this space is complicated however by the fact that the action of $U(Z)$ on $U(X)$ is highly nontrivial. This task is urgent for at least two reasons. Obviously, replacing the polylogarithmic quotient with the full unipotent fundamental group in our current algorithm would enable us to weaken our version of Kim’s conjecture. More interesting, perhaps, would be the

⁶I should point out, however, that the purpose of the present work is somewhat different from Brown’s work. Our goal here is to construct an actual algorithm, complete with precise criteria for halting. Moreover, its output should consist of functions that vanish not only on integral points, but also on the (a priori larger) loci defined by Kim’s general theory. This ensures that the result may be used to produce numerical evidence for Kim’s conjecture on the one hand, and provides an example of how Kim’s framework for studying integral points may be made fully explicit and algorithmic on the other hand.

possibility of going beyond our three punctures $\{0, 1, \infty\}$ to more general punctures, including possibly punctures that are not rational over the base-field in the context of mixed Artin–Tate motives.

2. Conjectures and theorems

We begin with a brief review of background material (unipotent fundamental group, Kim’s conjecture, motivic iterated integrals, filtered ϕ iterated integrals, p -adic periods). For a more detailed exposition, tailored specifically to our applications, we refer the reader to Dan-Cohen and Wewers [2016].

2.1. A motivic variant of Kim’s construction.

2.1.1. The prounipotent completion of the fundamental group of X has a motivic precursor, known as the *unipotent fundamental group*, a unipotent group object of the category of mixed Tate motives constructed by Deligne and Goncharov [2005] whose various realizations had previously been studied by Deligne [1989]. We use the tangent vector 1_0 as base-point, and denote the resulting group simply by $U(X)$; see Section 15 of [loc. cit.] for the use of tangential base-points in the various realizations. The unipotent fundamental group of \mathbb{G}_m is equal to (the covariant total space of) $\mathbb{Q}(1)$. The natural inclusion

$$\mathbb{P}^1 \setminus \{0, 1, \infty\} \hookrightarrow \mathbb{G}_m$$

induces a surjection of unipotent fundamental groups

$$U(X) \twoheadrightarrow \mathbb{Q}(1).$$

Let N denote its kernel. Then according to Deligne [loc. cit., Section 16], the Lie algebra of

$$U(X)^{\text{PL}} := U(X)/[N, N]$$

is canonically a semidirect product

$$\mathfrak{n}(X)^{\text{PL}} = \mathbb{Q}(1) \ltimes \prod_{i=1}^{\infty} \mathbb{Q}(i).$$

We write $\mathfrak{n}(X)_{\geq -n}^{\text{PL}}$ for the quotient

$$\mathbb{Q}(1) \ltimes \prod_{i=1}^n \mathbb{Q}(i),$$

of $\mathfrak{n}(X)^{\text{PL}}$, and $U_{\geq -n}^{\text{PL}}$ for the corresponding quotient of $U(X)$. There are also associated quotients $({}_b P_{1_0})_{\geq -n}^{\text{PL}}$ of the path torsors ${}_b P_{1_0}$ obtained by pushing out along the quotient map of

$$U \twoheadrightarrow U_{\geq -n}^{\text{PL}}.$$

All this holds over $\text{Spec } \mathbb{Z}$.

2.1.2. Let $Z \subset \text{Spec } \mathcal{O}_K$ be an open integer scheme. Sending a point $b \in X(Z)$ to the torsor of *polylogarithmic paths* $({}_b P_{1_0})_{\geq -n}^{\text{PL}}$ defines a map

$$\kappa : X(Z) \rightarrow H^1(U_{\geq -n}^{\text{PL}})(\mathbb{Q})$$

to the set of rational points of a finite-type affine \mathbb{Q} -scheme $H^1(U_{\geq -n}^{\text{PL}})$ which parametrizes such torsors, the *polylogarithmic Selmer variety*; see Section 2.3.2 below for a precise definition.

There is also a local p -adic version. We fix a closed point \mathfrak{p} of Z which we assume to be totally split for simplicity. We write $\mathcal{O}_{\mathfrak{p}}$ instead of \mathbb{Z}_p when we wish to emphasize the \mathcal{O}_Z -algebra structure, and similarly for $K_{\mathfrak{p}} = \mathbb{Q}_p$. We denote $\text{Spec } \mathcal{O}_{\mathfrak{p}}$ by $Z_{\mathfrak{p}}$. We obtain a map

$$\kappa_{\mathfrak{p}} : X(\mathcal{O}_{\mathfrak{p}}) \rightarrow H^1(U_n^{\text{PL}, F\phi})(\mathbb{Q}_p)$$

to the set of \mathbb{Q}_p -points of the *filtered- ϕ polylogarithmic Selmer variety* $H^1(U_n^{\text{PL}, F\phi})$. The set $X(\mathcal{O}_{\mathfrak{p}})$ may be viewed as the set of \mathbb{Q}_p -points of the rigid analytic space (for instance) obtained from $\mathbb{P}_{\mathbb{Q}_p}^1$ by removing the residue disks about 0, 1, and ∞ . Viewed this way, the map $\kappa_{\mathfrak{p}}$ is locally analytic but not rigid analytic; rather, it is given in coordinates by Coleman functions.

Connecting the filtered- ϕ and motivic versions is a map of \mathbb{Q}_p -schemes

$$\mathfrak{R}_{\mathfrak{p}} : \mathbb{Q}_p \otimes H^1(U_{\geq -n}^{\text{PL}}) \rightarrow H^1(U_{\geq -n}^{\text{PL}, F\phi})$$

induced by p -adic de Rham realization, which forms a commuting square

$$\begin{array}{ccc} X(Z) & \longrightarrow & X(\mathcal{O}_{\mathfrak{p}}) \\ \downarrow & & \downarrow \kappa_{\mathfrak{p}} \\ H^1(U_{\geq -n}^{\text{PL}})(\mathbb{Q}_p) & \xrightarrow{\mathfrak{R}_{\mathfrak{p}}} & H^1(U_{\geq -n}^{\text{PL}, F\phi})(\mathbb{Q}_p). \end{array}$$

2.1.3. The following conjecture was formulated jointly with David Corwin in [Corwin and Dan-Cohen 2018a]. Let $\text{Col}(X(\mathcal{O}_{\mathfrak{p}}))$ denote the ring of Coleman functions and consider the induced maps of \mathbb{Q}_p -algebras:

$$\begin{array}{ccc} & & \text{Col}(X(\mathcal{O}_{\mathfrak{p}})) \\ & & \uparrow \kappa_{\mathfrak{p}}^{\sharp} \\ \mathbb{Q}_p \otimes \mathcal{O}(H^1(U_{\geq -n}^{\text{PL}})) & \xleftarrow{\mathfrak{R}_{\mathfrak{p}}^{\sharp}} & \mathcal{O}(H^1(U_{\geq -n}^{\text{PL}, F\phi})) \end{array}$$

There is a natural action of the symmetric group S_3 on $\mathbb{P}^1 \setminus \{0, 1, \infty\}$, hence also on $\text{Col}(X(\mathcal{O}_{\mathfrak{p}}))$. We let $\kappa_{\mathfrak{p}}^{\sharp}(\ker \mathfrak{R}_{\mathfrak{p}}^{\sharp})$ denote the ideal of $\text{Col}(X(\mathcal{O}_{\mathfrak{p}}))$ generated by the image of $\ker \mathfrak{R}_{\mathfrak{p}}^{\sharp}$ and we let

$$\kappa_{\mathfrak{p}}^{\sharp}(\ker \mathfrak{R}_{\mathfrak{p}}^{\sharp})S_3$$

denote the ideal generated by its orbit. In down to earth terms, this means that we close the set of generators $\{F_i(z)\}_i$ of the smaller ideal under the two operations

$$F_i \mapsto F_i(1-z), \quad \text{and} \quad F_i \mapsto F_i\left(\frac{1}{z}\right). \quad (*)$$

We first define the *polylogarithmic Chabauty–Kim locus at level n*

$$X(\mathcal{O}_p)_n \subset X(\mathcal{O}_p)$$

to be the vanishing locus (not a priori reduced) of the smaller ideal $\kappa_p^\sharp(\ker \mathfrak{R}_p^\sharp)$. The polylogarithmic Chabauty–Kim loci form a nested sequence

$$X(\mathcal{O}_p) \supset X(\mathcal{O}_p)_1 \supset X(\mathcal{O}_p)_2 \supset \cdots \supset X(Z).$$

We note the following theorem, which is a direct consequence of the results of Kim [2012] via Soulé’s étale regulator isomorphism [1981].

Theorem (Kim). *Suppose Z is a totally real open integer scheme and let $\mathfrak{p} \in Z$ be any prime. Then for n sufficiently large, $\text{Im } \mathfrak{R}_p$ is contained in a subscheme of $H^1(U_{\geq -n}^{\text{PL}, F\phi})$ of strictly lower dimension.*

Recall from Kim [2009] that the map κ_p has dense image. So as soon as we have a nonzero function on $H^1(U_{\geq -n}^{\text{PL}, F\phi})$ vanishing on $\text{Im } \mathfrak{R}_p$, the associated locus will be finite.

Corollary (Kim). *Suppose Z is a totally real open integer scheme, and assume $\mathfrak{p} \in Z$ is totally split. Then for n sufficiently large, the associated polylogarithmic Chabauty–Kim locus $X(\mathcal{O}_p)$ is finite.*

We define the *symmetrized polylogarithmic Chabauty–Kim locus at level n*

$$X(\mathcal{O}_p)_n^{S_3} \subset X(\mathcal{O}_p)$$

to be the vanishing locus (not a priori reduced) of the ideal $\kappa_p^\sharp(\ker \mathfrak{R}_p^\sharp)S_3$. Stretching Kim’s conjecture from [Balakrishnan et al. 2018] somewhat, we propose the following.

Conjecture 2.1.4 (Convergence of polylogarithmic loci, joint with David Corwin). *Let Z be a totally real open integer scheme, and $\mathfrak{p} \in Z$ a totally split prime. View $X(Z)$ as a locally analytic space over \mathbb{Q}_p with reduced structure. Then for n sufficiently large, the associated polylogarithmic Chabauty–Kim locus satisfies*

$$X(\mathcal{O}_p)_n^{S_3} = X(Z).$$

Remark 2.1.5. The generalization from the rational to the totally real case should be harmless. By restricting attention to the polylogarithmic quotient, however, we are relying on a proper strengthening of Kim’s conjecture. Nevertheless, since the codimension of $\text{Im } \mathfrak{R}_p$ goes to infinity already for the polylogarithmic quotient, much of the motivation for Kim’s conjecture does hold for the polylogarithmic quotient; see [Corwin and Dan-Cohen 2018a] for a discussion of the role played by the S_3 -orbit. Finally, our interpretation of $X(\mathcal{O}_p)_n$ as a potentially nonreduced space, implying that there should be no double roots for n sufficiently large, is not discussed explicitly in [Balakrishnan et al. 2018].

2.2. Iterated integrals, p -adic periods, statement of arithmetic conjectures.

2.2.1. We begin by reviewing those properties of mixed Tate motives that we use. This material may be found, for instance, in [Deligne and Goncharov 2005]. We continue to work with an open integer scheme Z . Let $\mathbf{MT}(Z)$ denote the category of (unramified) mixed Tate motives over Z with \mathbb{Q} -coefficients. The category $\mathbf{MT}(Z)$ is \mathbb{Q} -Tannakian. It has a special object $\mathbb{Q}(1)$ of rank 1. Every simple object is isomorphic to a unique $\mathbb{Q}(n) := \mathbb{Q}(1)^{\otimes n}$. Each object is equipped with an increasing filtration W , the *Weight filtration*. (Since all the weights that occur are even, we also work with *half-weights*, which are half the usual weights. These will be denoted by subscripts.) The functor

$$\mathbf{MT}(Z) \rightarrow \text{Vect}(\mathbb{Q})$$

sending

$$E \mapsto \bigoplus \text{Hom}(\mathbb{Q}(i), \text{gr}_{-2i}^W E)$$

is a \mathbb{Q} -valued fiber functor, with associated group of the form

$$G(Z) = U(Z) \rtimes \mathbb{G}_m$$

with $U(Z)$ free pronipotent. From generalities of mixed Tate categories, we have canonical isomorphisms

$$U(Z)^{\text{ab}} = \bigoplus_{i \geq 1} \text{Ext}_Z^1(\mathbb{Q}(0), \mathbb{Q}(n))^{\vee}.$$

We have (highly nontrivial) canonical isomorphisms

$$K_{2n-1}^{(n)}(Z) \xrightarrow{\sim} \text{Ext}_Z^1(\mathbb{Q}(0), \mathbb{Q}(n)),$$

and a computation of the dimensions of these K -groups via real-analytic methods due to Borel [1953; 1977]:

$$\dim K_{2n-1}^{(n)}(Z) = \begin{cases} r_1 + r_2 & \text{for } n \text{ odd } \geq 3, \\ r_2 & \text{for } n \text{ even } \geq 2, \end{cases}$$

where r_1 (resp. r_2) denotes the number of real (resp. complex) places.

We let $\mathfrak{n}(Z)$ denote the Lie algebra of $U(Z)$, $\mathcal{U}(Z)$ its completed universal enveloping algebra, and $A(Z)$ the coordinate ring of $U(Z)$. Recall that the natural map

$$\mathcal{U}(Z)^{\vee} \rightarrow A(Z)$$

is an isomorphism of \mathbb{Q} -vector spaces.

2.2.2. Our discussion of iterated integrals applies to the complement in \mathbb{P}_Z^1 of any divisor \mathbf{D} which is a union of sections of

$$\mathbb{P}_Z^1 \rightarrow Z$$

and is étale over Z ; we continue to use the letter X which now denotes $\mathbb{P}_Z^1 \setminus \mathbf{D}$ and we refer to the components of \mathbf{D} as *punctures*. We assume $\infty \in \mathbf{D}$. We say that a section of a vector bundle is *nowhere*

vanishing if its image in every closed fiber is nonzero. We define a *base-point* to be either an integral point or a nowhere vanishing section of the normal bundle to one of the punctures. If a is a base-point, we denote the unipotent fundamental group of X at a by $U_a(X)$. The unipotent fundamental group may be thought of as a prounipotent group object of $\mathbf{MT}(Z)$, or, after applying the canonical fiber functor, as a prounipotent \mathbb{Q} -group equipped with an action of $G(Z)$, and we do not distinguish between these two points of view when we see no cause for confusion.

If b is a second base-point, we denote the unipotent path torsor by ${}_bP_a$; the latter may be thought of internally as a torsor-object of $\mathbf{MT}(Z)$ or externally as a $G(Z)$ -equivariant torsor.

2.2.3. After forgetting the $G(Z)$ -action, each unipotent path torsor ${}_bP_a$ is trivialized by a special \mathbb{Q} -rational path

$${}_bP_a^{\text{dR}} \in {}_bP_a(\mathbb{Q}),$$

and the fundamental group $U_a(X)$ is free on the set of logarithmic vector fields dual to the 1-forms

$$\omega_c = \frac{dt}{t - c}$$

for c a component of $\mathbf{D}_f := \mathbf{D} \setminus \infty$; this is proved by Deligne [1989] when $K = \mathbb{Q}$ and by Goncharov [2005] in general.⁷⁸ If $\omega = (\omega^1, \dots, \omega^r)$ is a sequence of such differential forms, we let f_ω denote the associated function (see Section 2 of [Dan-Cohen and Wewers 2016] for generalities on free prounipotent groups).

We say that the datum $(a; \omega; b)$ is *combinatorially unramified* if the associated reduced divisors are étale over Z .⁹ Being combinatorially unramified has the effect that the entire path bimodule \mathcal{U}_bP_a (i.e., the bimodule over the completed universal enveloping algebras at a and b) is unramified over Z .

2.2.4. Following Goncharov [2005], we define $I_a^b(\omega)$ to be the composite

$$U(Z) \xrightarrow{o({}_bP_a^{\text{dR}})} {}_bP_a(X) \xrightarrow{\sim} U_a(X) \xrightarrow{f_\omega} \mathbb{A}_{\mathbb{Q}}^1.$$

Here $o({}_bP_a^{\text{dR}})$ denotes the orbit map associated to the rational point ${}_bP_a^{\text{dR}}$. If $A(Z)$ denotes the graded hopf algebra $\mathcal{O}(U(Z))$ then $I_a^b(\omega)$ belongs to $A(Z)_r$. We refer to these elements as (*combinatorially unramified*) *unipotent iterated integrals*. Among the unipotent iterated integrals are the *classical unipotent polylogarithms*

$$\text{Li}_{n+1}^U(t) := I_{1_0}^t(0^n, 1)$$

⁷It is quite crucial that we work rationally here, since we will be using motivic iterated integrals to construct generators of the Hopf algebra $A(Z) = \mathcal{U}(Z)^\vee$ as a \mathbb{Q} -algebra.

⁸After tensorization with K , the canonical fiber functor on $\mathbf{MT}(Z)$ becomes canonically isomorphic to the de Rham fiber functor. A fact, which is perhaps underemphasized in the literature, however, is that the usual Tannakian interpretation of $U_a(X)$ in terms of unipotent connections is unavailable over the rationals unless $K = \mathbb{Q}$. Thus, our ${}_bP_a^{\text{dR}}$ is a *rational form* of Deligne’s canonical de Rham path.

⁹If a is a base-point, we let a_0 denote the *location* of a : $a_0 = a$ if a is an integral point, otherwise a is a tangent vector at a_0 . We assume that the datum $(a; \omega; b)$ behaves nicely over Z in an obvious sense, which requires several cases to state precisely: in all cases we assume the reduced divisor associated to ω , a_0 , b_0 , and ∞ is étale over Z ; if a is a tangent vector and $a_0 \neq b_0$, we assume the reduced divisor which supports $a + 0 + \infty$ on \mathbb{P}^1 is étale over Z ; if a, b are both tangent vectors at the same point $a_0 = b_0$, we assume similarly that the support of $a + b + 0 + \infty$ is étale over Z .

(where the comma is used as a typographical pun to denote the concatenation product) and their single valued cousins $\text{Li}_n^{U,sv}(t)$, for which we refer the reader to Brown [2013]. In terms of these objects, we may state the conjectures of Zagier and Goncharov as follows.

Conjecture 2.2.5 (Zagier’s conjecture). *For each $n \geq 2$, the motivic Ext group*

$$E_n := \text{Ext}_K^1(\mathbb{Q}(0), \mathbb{Q}(n))$$

is spanned by single valued unipotent n -logarithms $\text{Li}_n^{U,sv}(t)$ with $t \in K$.

Remark 2.2.6. We recall that Zagier’s conjecture is known for $n = 2$ by Zagier [1991] and independently by work of Suslin [1987] and Bloch [2000], and for $n = 3$ by Goncharov [1994]. The case of K cyclotomic was treated by Beilinson [1989] in an unpublished manuscript. The main algorithm we construct below could be greatly simplified in the cyclotomic case $K = \mathbb{Q}(\zeta_N)$, where a basis for E_n is given explicitly by the elements $\text{Li}_n^{U,sv}(\zeta_N^i)$ for $0 < i < N/2$. Conversely, away from the cyclotomic case, our algorithm is made complicated partly because of the lack of explicit constructions, even conjectural, of elements of E_n ; away from the roots of unity, most $\text{Li}_n^{U,sv}(t)$ are *not* contained in E_n .

Conjecture 2.2.7 (Goncharov-exhaustion). *For any open integer scheme Z and any $n \in \mathbb{N}$, there is an open subscheme $Z^o \subset Z$ such that $A(Z^o)_{\leq n}$ is spanned by combinatorially unramified unipotent iterated integrals over Z^o .*

Remark 2.2.8. Goncharov’s conjecture [1995] implies that for every Z and n there is an open subscheme $Z^o \subset Z$ such that $A(Z)_{\leq n}$ (in place of $A(Z^o)_{\leq n}$) is spanned by *linear combinations of* combinatorially unramified unipotent iterated integrals over Z^o . This distinction between actual iterated integrals and linear combinations of iterated integrals is important, and our strengthening of the conjecture is, as far as I can tell, nontrivial and necessary for our purposes. The reason is that we are unable to check algorithmically if a given linear combination of combinatorially unramified iterated integrals in $A(Z^o)$ belongs to the subalgebra

$$A(Z) \subset A(Z^o).$$

Actually, our work here does provide an algorithm for checking if a given linear combination is p -adically close to $A(Z)$, but this algorithm is rather indirect. In outline, we first apply our *basis algorithm* to obtain an open subscheme $Z^o \subset Z$ and a *concrete* basis of $A(Z^o)$ (within the specified weight range) consisting of (actual!) combinatorially unramified unipotent iterated integrals compatible to within ϵ with the extension spaces. This gives rise to a set of generators of the Lie algebra, which in turn generate an *abstract* shuffle basis of $A(Z^o)$. We then compare the two bases to within ϵ using our *change of basis algorithm* and use the shuffle basis to identify $A(Z)$ inside $A(Z^o)$.

Thus, our conjecture represents a version of Goncharov’s conjecture strengthened somewhat to include weak control over ramification. Better control over ramification would yield a faster algorithm. The case $Z = \text{Spec } \mathbb{Z} \setminus \{2\}$, $n = \infty$ established by Deligne [2010], and the discussion of the case $n = 2$

in [Dan-Cohen and Wewers 2016] both support the belief that unipotent iterated integrals should be compatible with ramification, at least to the extent predicted by our wording of the conjecture.

2.2.9. Unipotent iterated integrals have a filtered ϕ variant at each prime $\mathfrak{p} \in Z$. We mention only a few key similarities and differences, referring the reader to [Dan-Cohen and Wewers 2016, Section 4] for details. As for mixed Tate motives, there is a Tannakian (in fact, mixed Tate) category of mixed Tate filtered ϕ modules, and an associated proalgebraic group of the form

$$G(\mathcal{O}_{\mathfrak{p}}) = \mathbb{G}_m \times U(\mathcal{O}_{\mathfrak{p}})$$

with $U(\mathcal{O}_{\mathfrak{p}})$ free pronipotent, but now over \mathbb{Q}_p ; we adopt our notation $(\mathfrak{n}(\mathcal{O}_{\mathfrak{p}}), \mathcal{U}(\mathcal{O}_{\mathfrak{p}}), A(\mathcal{O}_{\mathfrak{p}}))$ from the motivic case.¹⁰ Unlike the motivic case, $U(\mathcal{O}_{\mathfrak{p}})$ possesses canonical generators $v_{\mathfrak{p},-1}, v_{\mathfrak{p},-2}, v_{\mathfrak{p},-3}, \dots$, and an associated special $K_{\mathfrak{p}}$ -valued point

$$u_{\mathfrak{p}} = \exp \sum_i v_{\mathfrak{p},i}$$

of $U(\mathcal{O}_{\mathfrak{p}})$. Note that the “generators” are not points of the group, but rather elements of the Lie algebra, regarded as Lie-like elements of the completed universal enveloping algebra — see the discussion of free pronipotent groups in Section 2 of [Dan-Cohen and Wewers 2016].

2.2.10. There is a morphism of unipotent groups

$$U(Z) \leftarrow U(Z_{\mathfrak{p}})$$

(linear over $\text{Spec } \mathbb{Q} \leftarrow \text{Spec } \mathbb{Q}_p$) induced by filtered ϕ realization. The composite

$$U(Z) \leftarrow U(Z_{\mathfrak{p}}) \xleftarrow{u_{\mathfrak{p}}} \text{Spec } K_{\mathfrak{p}}$$

is the map denoted I_{BC} above; we refer to it as “Besser–Coleman integration”. The associated map of rings

$$\text{per}_{\mathfrak{p}} := I_{\text{BC}}^{\sharp} : A(\mathcal{O}_{\mathfrak{p}}) \rightarrow K_{\mathfrak{p}}$$

is called the *p-adic period map*. If π denotes the embedding of K in $K_{\mathfrak{p}}$, then we have

$$I_a^b(\omega)(I_{\text{BC}}) = \text{per}_{\mathfrak{p}}(I_a^b(\omega)) = \int_{a^{\pi}}^{b^{\pi}} \omega^{\pi},$$

a *p-adic iterated integral* in the sense of Coleman–Besser. (From this point of view, it’s better to think of $I_a^b(\omega)$ as a “motivic iterated *integrand*”: when we combine a *motivic iterated integrand* with *p-adic integration*, we obtain a *p-adic iterated integral*.) An algorithm for computing such integrals to arbitrary *p-adic* precision is constructed in [Dan-Cohen and Chatzistamatiou 2014]; as mentioned above, we review this unpublished work in Section 6 below. The following conjecture is stated for instance in Yamashita [2010].

¹⁰Our use of $\mathcal{O}_{\mathfrak{p}}$ (in place of $K_{\mathfrak{p}}$) in the notation expresses the fact that we’re working with filtered ϕ -modules as opposed to filtered ϕ, N -modules.

Conjecture 2.2.11 (*p*-Adic period conjecture). *Let Z be an open integer scheme with fraction field K , and let \mathfrak{p} be a closed point of Z . Then the p -adic period map*

$$\text{per}_{\mathfrak{p}} : A(Z) \rightarrow K_{\mathfrak{p}}$$

is injective.

2.2.12. Hasse principle for finite cohomology. In addition to the semilinear injectivity of the period conjecture, we will also need a linear injectivity property which concerns the product of realization maps

$$\mathfrak{R}_p : \mathbb{Q}_p \otimes \text{Ext}_{\mathcal{O}_K}^1(\mathbb{Q}(0), \mathbb{Q}(n)) \rightarrow \prod_{\mathfrak{p} | p} \text{Ext}_{\mathcal{O}_{\mathfrak{p}}}^1(\mathbb{Q}_p(0), \mathbb{Q}_p(n))$$

for $n \geq 2$. We recast this in the language of finite Galois cohomology as follows. Let S be the set of places of K above p and ∞ . Let G_S denote the Galois group of the maximal extension of K which is unramified outside of S , and for v a place of K , let G_v denote the total Galois group of the local field K_v . Following Bloch and Kato [1990], we write H_f^i for the space of cohomology classes that are crystalline at all primes above p . By the p -adic regulator isomorphisms of Soulé [1981]

$$\mathbb{Q}_p \otimes \text{Ext}_{\mathcal{O}_K[1/p]}^1(\mathbb{Q}(0), \mathbb{Q}(n)) \xrightarrow{\sim} H^1(G_S, \mathbb{Q}_p(n)),$$

the injectivity of \mathfrak{R}_p is equivalent to the following condition on a number field K , a prime p of \mathbb{Z} and an integer $n \geq 2$.

Condition 2.2.13. The map

$$\text{loc}_p : H_f^1(G_S, \mathbb{Q}_p(n)) \rightarrow \prod_{\mathfrak{p} | p} H_f^1(G_{\mathfrak{p}}, \mathbb{Q}_p(n))$$

is injective.

Let Z be a totally real open integer scheme with function field K and assume the corresponding polylogarithmic Chabauty–Kim loci converge at n . We say that Z *obeys Kim vs. Hasse* if the above injectivity holds at levels $n' \leq n$.

In fact, an anonymous referee has pointed out that Condition 2.2.13 follows from a conjecture due to Jannsen. Conjecture 1 of [Jannsen 1989] (applied, in the notation of that article, to $X = \text{Spec } \mathcal{O}_K[1/p]$) says that

$$H^2(G_S, \mathbb{Q}_p(n)) = 0$$

for $n < 0$. By the Poitou–Tate exact sequence

$$\cdots \rightarrow H^2(G_S, M^\vee(1))^\vee \rightarrow H^1(G_S, M) \rightarrow \bigoplus_{v \in S} H^1(G_v, M) \rightarrow \cdots$$

applied to $M = \mathbb{Q}_p(n)$, we find that the map

$$H^1(G_S, \mathbb{Q}_p(n)) \rightarrow \bigoplus_{v \in S} H^1(G_v, \mathbb{Q}_p(n))$$

is injective whenever $n \geq 2$.

For v real and p odd, we have

$$H^1(G_v, \mathbb{Q}_p(n)) = 0.$$

Indeed, if C is a finite cyclic group with generator σ , and if we consider the elements $1 - \sigma$, $N := \sum_{\tau \in C} \tau$ of the group algebra $\mathbb{Z}[C]$, then for any $\mathbb{Z}[C]$ -module A , the sequence

$$0 \rightarrow A \xrightarrow{\sigma-1} A \xrightarrow{N} A \xrightarrow{\sigma-1} A \xrightarrow{N} \dots,$$

in which the first A is in degree zero, forms a complex A^\bullet and

$$H^i(C, A) = H^i A^\bullet.$$

When C has order 2, we have $N = \sigma + 1$. Applying this to our situation, we have

$$H^1(G_v, \mu_{p^r}^{\otimes n}) = H^1(\mathbb{Z}/(2), (\mathbb{Z}/(p^r))^{\otimes n})$$

computed by the complex

$$0 \rightarrow \mathbb{Z}/(p^r) \xrightarrow{(-1)^n-1} \mathbb{Z}/(p^r) \xrightarrow{(-1)^n+1} \mathbb{Z}/(p^r) \rightarrow \dots$$

in which isomorphisms alternate with multiplication by ± 2 depending on the parity of n . Either way, all cohomologies above degree 0 vanish.

Consequently, the map

$$H^1(G_S, \mathbb{Q}_p(n)) \rightarrow \bigoplus_{p|p} H^1(G_p, \mathbb{Q}_p(n))$$

is injective. Condition 2.2.13 follows by restricting this map to finite cohomology spaces.

As a final remark, let us note that this injectivity is related to the nonvanishing of certain p -adic L -values; see Theorem 4.2.1 of Perrin–Riou [1994].

2.3. Outline of algorithm.

2.3.1. Our main construction is an algorithm, which we denote by $\mathcal{A}_{\text{LocI}}$, which takes as input an open integer scheme Z , a prime p of \mathbb{Z} over which Z is totally split, a natural number n , and an ϵ , and returns an open subscheme Z^o of Z , an algebra basis $\tilde{\mathcal{B}}$ of the polynomial ring $A(Z^o)_{\leq n}$, and a family $\{\tilde{F}_i\}_i$ of elements of the polynomial ring

$$\mathbb{Q}[\tilde{\mathcal{B}}, \log, \text{Li}_1, \dots, \text{Li}_n].$$

2.3.2. In terms of the category of mixed Tate motives $MT(Z)$ and its Tannakian fundamental group $G(Z)$ discussed in Section 2.2.1, the polylogarithmic Selmer variety of Section 2.1.2 is characterized by the functor of \mathbb{Q} -algebras

$$R \mapsto H^1(G(Z)_R, U_{\geq -n, R}^{\text{PL}}).$$

The proof of Proposition 2 of Kim [2005] applies mutatis mutandis to show that this functor is representable by a finite-type affine \mathbb{Q} -scheme, which in this case is in fact isomorphic to affine space.

2.3.3. According to [Dan-Cohen and Wewers 2016, Section 5.2], we have

$$H^1(G(Z), U(X)_{\geq -n}^{\text{PL}}) = Z^1(U(Z), U(X)_{\geq -n}^{\text{PL}})^{\mathbb{G}_m} = \text{Hom}(U(Z), U(X)_{\geq -n}^{\text{PL}})^{\mathbb{G}_m},$$

the space of \mathbb{G}_m -equivariant homomorphisms, and similarly for the filtered ϕ version over Z_p . Moreover, in the latter case, evaluation at u_p induces an isomorphism

$$\text{ev}_{u_p} : \text{Hom}(U(Z_p), U(X_p)_{\geq -n}^{\text{PL}})^{\mathbb{G}_m} \xrightarrow{\sim} U(X_p)_{\geq -n}^{\text{PL}} = \mathbb{Q}_p \otimes U(X)_{\geq -n}^{\text{PL}}.$$

The composite map

$$\mathbb{Q}_p \otimes \text{Hom}(U(Z), U(X)_{\geq -n}^{\text{PL}})^{\mathbb{G}_m} \rightarrow \text{Hom}(U(Z_p), U(X_p)_{\geq -n}^{\text{PL}})^{\mathbb{G}_m} \xrightarrow{\sim} \mathbb{Q}_p \otimes U(X)_{\geq -n}^{\text{PL}}$$

is given by evaluation at the pullback I_{BC} of u_p to $U(Z)$. As explained in the introduction, in order to compute its scheme-theoretic image, we first put this evaluation map inside the universal family of evaluation maps $\text{ev} = \text{ev}_{\text{Everywhere}}$:

$$\text{Hom}^{\mathbb{G}_m}(U(Z), U(X)_{\geq -n}^{\text{PL}}) \times U(Z^o) \rightarrow U(X)_{\geq -n}^{\text{PL}} \times U(Z^o)$$

pulled back along

$$U(Z^o) \rightarrow U(Z).$$

If we fix arbitrary generators of $U(Z^o)$, these give rise to coordinates on $A(Z^o)$, which we refer to as *abstract shuffle-coordinates*. In terms of these, the computation is purely classical. We must then however switch to coordinates whose image under the period map can be computed, that is, to *concrete coordinates* given by unipotent iterated integrals. As explained in the introduction, the heart of our algorithm constructs such coordinates, as well as an approximate change-of-basis matrix which relates a judicious choice of abstract shuffle-coordinates to our concrete coordinates. This key step is inspired by the work of Francis Brown [2012].

2.4. Statement of main theorem. For each prime p lying above p , the p -adic period map extends in an obvious way to a map

$$\mathbb{Q}[\tilde{\mathcal{B}}, \log, \text{Li}_1, \dots, \text{Li}_n] \rightarrow \text{Col}(X(\mathcal{O}_p))$$

to the ring of Coleman functions; denote the image of the element \tilde{F}_i from segment 2.3.1 by \tilde{F}_i^p .

Theorem 2.4.1. *Let Z be an open integer scheme, $p \in Z$ a totally split prime, p the image of p in $\text{Spec } \mathbb{Z}$, n a natural number, and $\epsilon \in p^{\mathbb{Z}}$. Let*

$$\mathcal{K}_p(\mathfrak{n}_{\geq -n}^{\text{PL}}) \triangleleft \text{Col}(X(Z_p))$$

denote the ideal which defines the Chabauty–Kim locus $X(Z_p)_n$; we refer to $\mathcal{K}_p(\mathfrak{n}_{\geq -n}^{\text{PL}})$ as the p -adic Chabauty–Kim ideal associated to $\mathfrak{n}_{\geq -n}^{\text{PL}}$:

- (1) Suppose $\mathcal{A}_{\text{Loci}}(Z, p, n, \epsilon)$ halts. Then there are functions $\{F_i^{\mathfrak{p}}\}$ generating the \mathfrak{p} -adic Chabauty–Kim ideal $\mathcal{K}_{\mathfrak{p}}(\mathfrak{n}_{\geq -n}^{\text{PL}})$ associated to $\mathfrak{n}_{\geq -n}^{\text{PL}}$, such that

$$|\tilde{F}_i^{\mathfrak{p}} - F_i^{\mathfrak{p}}| < \epsilon$$

for all i .

- (2) Suppose Zagier’s conjecture (Conjecture 2.2.5) holds for K and $n' \leq n$. Suppose Goncharov exhaustion (Conjecture 2.2.7) holds for Z and $n' \leq n$. Suppose the period conjecture holds for the open subscheme $Z^o \subset Z$ constructed in segment 3.8 in half-weights $n' \leq n$. Suppose K obeys the Hasse principle for finite cohomology (Condition 2.2.13) in half-weights $2 \leq n' \leq n$. Then the computation $\mathcal{A}_{\text{Loci}}(Z, p, n, \epsilon)$ halts.

We remark that part (1) of the theorem is independent of the choice of norm on the space of polylogarithmic functions up to an admissible change in ϵ . We complete the construction of the Loci algorithm and prove Theorem 2.4.1 in Section 4.

3. Construction of arithmetic algorithms

3.1. Generators for graded free algebras.

Proposition 3.1.1. *Let $S = \bigcup_{i=1}^{\infty} S_i$ be a disjoint union of finite sets, and similarly*

$$S' = \bigcup_{i=1}^{\infty} S'_i.$$

Let k be a field and $k[S], k[S']$ associated graded free algebras and I, I' the augmentation ideals. Let

$$\phi : k[S'] \rightarrow k[S]$$

be a homomorphism which preserves the grading. Suppose the induced map

$$I'/I'^2 \rightarrow I/I^2$$

is iso. Then ϕ is iso.

Proof. For $n \geq 1$, we have $I_n = k[S]_n$. Surjectivity follows by induction using the short exact sequences

$$0 \rightarrow (I^2)_n \rightarrow k[S]_n \rightarrow (I/I^2)_n \rightarrow 0.$$

Since S_i maps to a basis of $(I/I^2)_i$, the bijection

$$(I'/I'^2)_i \rightarrow (I/I^2)_i$$

gives us a bijection between S'_i and S_i . For any n , ϕ maps $S'_{\leq n}$ into $k[S]_{\leq n}$, so ϕ restricts to a map

$$k[S'_{\leq n}] \rightarrow k[S_{\leq n}]$$

of subalgebras generated in degrees $\leq n$. These are surjective maps of polynomial algebras of same finite Krull dimension. This means that

$$\text{Spec } k[S_{\leq n}] \rightarrow \text{Spec } k[S'_{\leq n}]$$

is a closed immersion between affine spaces of same dimension, hence an isomorphism by the Hauptideal-satz. □

3.2. Generators for mixed Tate groups.

3.2.1. For a review of free pronipotent groups, we refer the reader to Section 2 of [Dan-Cohen and Wewers 2016]. By a *mixed Tate group* over a field k of characteristic zero, we mean a free pronipotent group U equipped with a grading of the Lie algebra

$$\mathfrak{n} = \text{Lie } U$$

such that $\mathfrak{n}_i = 0$ for $i \geq 0$. The Lie algebra \mathfrak{n} admits a set of homogeneous free generators, and we define a *set of homogeneous free generators of U* to be a set of homogeneous free generators of \mathfrak{n} . The grading on \mathfrak{n} induces also a grading of the completed universal enveloping algebra $\mathcal{U} = \mathcal{U}\mathfrak{n}$ such that $\mathcal{U}_0 = k$ and $\mathcal{U}_i = 0$ for $i > 0$, as well as a grading on the coordinate ring $A = \mathcal{O}(U) = \mathcal{U}^\vee$ such that $A_0 = k$ and $A_i = 0$ for $i < 0$. We refer to the graded degree of an element (of $\mathfrak{n}, \mathcal{U}, A$) as its *half-weight*.

The kernel of the comultiplication

$$E_n < A_n$$

is the space of *extensions*. Indeed, by the general theory of mixed Tate categories we have exact sequences

$$0 \rightarrow \text{Ext}_{\text{Rep}(\mathbb{G}_m \ltimes U)}^1(k(0), k(n)) \rightarrow A_n \rightarrow \bigoplus_{\substack{i+j=n \\ i,j \geq 1}} A_i \otimes A_j$$

where $k(i)$ denotes the trivial U -representation in half-weight $-i$. Similarly, the multiplication gives rise to a subspace

$$A_n > D_n,$$

namely the image of the map

$$A_n \leftarrow \bigoplus_{\substack{i+j=n \\ i,j \geq 1}} A_i \otimes A_j;$$

we refer to D_n as the *space of decomposable elements*.

Proposition 3.2.2. *Let U be a mixed Tate group, and let A denote its coordinate ring. For each i let E_i denote the space of extensions in A_i , D_i the space of decomposable elements. Let \mathcal{P}_i be a linearly independent subset of A_i which spans a subspace \mathcal{P}_i complementary to $E_i + D_i$. Let \mathcal{E}_i be a basis for E_i and let $\mathcal{E} = \bigcup \mathcal{E}_i, \mathcal{P} = \bigcup \mathcal{P}_i$. Then as a ring,*

$$A = k[\mathcal{E} \cup \mathcal{P}].$$

Proof. The subspaces E_i and D_i are disjoint. To see this, fix an arbitrary set

$$\epsilon' = \bigcup_{i=1}^{\infty} \epsilon'_{-i}$$

of homogeneous free generators for U , and for w a word in ϵ' , let $f_w \in A$ denote the associated function. Then E_i has basis

$$\{f_a \mid a \in \epsilon'_{-i}\}$$

dual to the set of one-letter words of half-weight $-i$, while D_i is spanned by shuffle products of functions f_w with w a word in $\epsilon'_{>-i}$, so is contained in the space with basis

$$\{f_w \mid w \in \mathbf{Words}_{-i}(\epsilon'_{>-i})\}.$$

It follows that A_i decomposes as a direct sum

$$A_i = E_i \oplus P_i \oplus D_i \tag{3.2.2*}$$

and that $\mathcal{E}_i \cup \mathcal{P}_i$ maps to a basis of $(I/I^2)_i$. Hence, by Proposition 3.1.1, $\mathcal{E} \cup \mathcal{P}$ forms a set of free k -algebra generators for A . \square

Proposition 3.2.3. *In the situation and the notation of Proposition 3.2.2, let*

$$\epsilon_{-i} \subset \mathcal{U}_{-i}$$

be the set of elements dual to the elements of \mathcal{E}_i relative to the decomposition (3.2.2). Then*

$$\epsilon := \bigcup_{i=1}^{\infty} \epsilon_{-i}$$

forms a set of free generators for U .

Proof. We claim that every element

$$\epsilon_{-i,j} \in \epsilon_{-i}$$

is of Lie type; if

$$v : \mathcal{U} \rightarrow \mathcal{U} \otimes \mathcal{U}$$

denotes the comultiplication, then

$$v(\epsilon_{-i,j}) = 1 \otimes \epsilon_{-i,j} + \epsilon_{-i,j} \otimes 1. \tag{*}$$

Let

$$\mathcal{P}'_i = \mathcal{E}_i \cup \mathcal{P}_i.$$

According to Proposition 3.2.2, the set \mathcal{D}_i of monomials in $\mathcal{P}'_{<i}$ forms a basis of D_i . Let

$$\mathcal{A}_i = \mathcal{E}_i \cup \mathcal{P}_i \cup \mathcal{D}_i.$$

It suffices to check the equality (*) after pairing with an arbitrary basis element

$$\mathcal{A}_{i',j'} \otimes \mathcal{A}_{i'',j''}$$

of $\mathcal{A}_{i'} \otimes \mathcal{A}_{i''}$ with $i' + i'' = i$. We have

$$\begin{aligned} \langle v(\epsilon_{-i,j}), \mathcal{A}_{i',j'} \otimes \mathcal{A}_{i'',j''} \rangle &= \langle \epsilon_{-i,j}, \mathcal{A}_{i',j'} \cdot \mathcal{A}_{i'',j''} \rangle \\ &= \begin{cases} 1 & \text{if } \mathcal{A}_{i',j'} = 1 \text{ and } \mathcal{A}_{i'',j''} = \mathcal{E}_{i,j} \text{ is dual to } \epsilon_{-i,j}, \\ 1 & \text{if } \mathcal{A}_{i',j'} = \mathcal{E}_{i,j} \text{ and } \mathcal{A}_{i'',j''} = 1, \\ 0 & \text{otherwise.} \end{cases} \\ &= \langle 1 \otimes \epsilon_{-i,j}, \mathcal{A}_{i',j'} \otimes \mathcal{A}_{i'',j''} \rangle + \langle \epsilon_{-i,j} \otimes 1, \mathcal{A}_{i',j'} \otimes \mathcal{A}_{i'',j''} \rangle \\ &= \langle 1 \otimes \epsilon_{-i,j} + \epsilon_{-i,j} \otimes 1, \mathcal{A}_{i',j'} \otimes \mathcal{A}_{i'',j''} \rangle \end{aligned}$$

which shows that $\epsilon_{-i,j}$ is of Lie type as claimed.

It follows that ϵ_{-i} is a subset of the graded piece \mathfrak{n}_{-i} of the Lie algebra $\mathfrak{n} \subset \mathcal{U}$, which maps to a basis of $\mathfrak{n}_{-i}^{\text{ab}}$. It follows that ϵ forms a set of free generators as stated. □

3.3. Recall that by an *open integer scheme* we mean an open subscheme

$$Z \subset \text{Spec } \mathcal{O}_K,$$

K a number field. By a *number scheme* we mean $\text{Spec } K$, K a number field. Given Z an open integer or number scheme, we let

$$A(Z) = \mathcal{O}(U(Z))$$

denote the graded Hopf algebra of unramified mixed Tate motives over Z .

3.4. Given an open integer scheme Z with function field K and a unipotent iterated integral $I_a^b(c_1, \dots, c_r) \in A(K)_n$, we say that I is *combinatorially unramified over Z* if the associated reduced divisor

$$D = \{a, b, c_1, \dots, c_r\}$$

is étale over Z . We denote the \mathbb{Q} -vector space of formal linear combinations of such tuples $(a; c_1, \dots, c_r; b)$ by $\text{CUI}(Z)_r$, the space of *formal integrands in half-weight r* .

3.5. If k is a field equipped with an absolute value $|\cdot|$, we say that a subset of k^n is ϵ -linearly independent if each of the associated determinants has absolute value greater than ϵ .

3.6. Let Z be an open integer scheme and $p \in \mathbb{Z}$ a prime such that Z is totally split above p . Recall that $A(\mathcal{O}_p)$ denotes the graded Hopf algebra of mixed Tate filtered ϕ modules over K_p , and recall that $A(\mathcal{O}_p)$ possesses a *standard basis*. We say that a subset

$$\mathcal{P} \subset A(Z)_n$$

is ϵ -linearly independent relative to \mathfrak{R}_p if its image in $\prod_{p|p} A(\mathcal{O}_p)_n$ is ϵ -linearly independent with respect to the standard basis.

3.7. Realization algorithm.

3.7.1. We recall from segment 2.2.9 that $U(\mathbb{Z}_p)$ denotes the unipotent fundamental group of the category of mixed Tate filtered ϕ modules, that it contains a special \mathbb{Q}_p -point u , and that the family

$$v_i = (\log u)_i \in \mathfrak{n}(\mathbb{Q}_p)$$

for $i \in \mathbb{Z}_{\leq -1}$ forms a set of free generators. The associated shuffle basis of $A(\mathbb{Z}_p)$ (which is dual to the basis of the universal enveloping algebra consisting of words in the generators) is what we call the *standard basis*. We now construct an algorithm for evaluating an iterated integral $I_a^b(\omega)$, whose associated divisor D is a union of \mathbb{Z}_p -points, on a word

$$w = v_{-i_r} \cdots v_{-i_2} v_{-i_1}$$

in the generators v_i to given precision ϵ .

3.7.2. Let $Z \subset \text{Spec } \mathcal{O}_K$ be an open integer scheme, and $\mathfrak{p} \in Z$ a prime which is totally split. Recall from segment 3.4 that $\text{CUI}(Z)_r$ denotes the \mathbb{Q} -vector space of combinatorially unramified integrands in half-weight r . The *realization algorithm*, alluded to above and constructed in segment 3.7.16 below, may be interpreted as an algorithm which takes a natural number r and an $\epsilon \in p^{\mathbb{Z}}$ as input, and returns a linear map

$$\widetilde{U_I^{F\phi}}_{\text{Std}} : \text{CUI}(Z)_r \rightarrow \prod_{\mathfrak{p} | p} A(\mathcal{O}_{\mathfrak{p}})_r$$

given explicitly by a matrix with rational entries. If

$$\text{Re} : A(Z)_r \rightarrow \prod_{\mathfrak{p} | p} A(\mathcal{O}_{\mathfrak{p}})_r$$

denotes the realization map, and

$$U_I : \text{CUI}(Z)_r \rightarrow A(Z)_r$$

denotes the map taking an integrand to the associated unipotent iterated integral, then the triangle

$$\begin{array}{ccc} \text{CUI}(Z)_r & \xrightarrow{\widetilde{U_I^{F\phi}}_{\text{Std}}} & \prod_{\mathfrak{p} | p} A(\mathcal{O}_{\mathfrak{p}})_r \\ U_I \downarrow & \searrow & \uparrow \\ A(Z)_r & \xrightarrow{\text{Re}} & \prod_{\mathfrak{p} | p} A(\mathcal{O}_{\mathfrak{p}})_r \end{array}$$

fails to commute by at most ϵ . Said differently, $\widetilde{U_I^{F\phi}}_{\text{Std}}$ is an approximation of the matrix representing the composite

$$U_I^{F\phi} := \text{Re} \circ (U_I)$$

with respect to the “standard” bases on source and target. An example is worked out in segment 7.5.3 of [Dan-Cohen and Wewers 2016]. Note, however, that the triviality of the motivic Galois action on the poly-logarithmic quotient makes that example deceptively simple compared to the general algorithm that follows.

We begin in segments 3.7.3–3.7.8 by deriving a formula (Lemma 3.7.4) for the action of the special \mathbb{Q}_p -point u of the unipotent mixed Tate filtered ϕ Galois group $U(\mathbb{Z}_p)$ on any generator of the unipotent fundamental group of $X := \mathbb{A}_{\mathbb{Q}_p}^1 \setminus D$. We then note in segment 3.7.9 that the formula of Lemma 3.7.4 gives rise to an algorithm for computing the action of u on any word in the generators. In segment 3.7.11 we extend this algorithm to include not only fundamental groups but also path torsors. After a few elementary observations regarding the matrix entries of a graded representation of a graded Lie algebra on a graded vector space equipped with a graded basis on which we do not wish to impose an ordering (segments 3.7.13–3.7.14), and after constructing a certain family of polynomials with rational coefficients based on these observations (segment 3.7.15), we construct the realization algorithm in segment 3.7.16 and we state and verify the correctness of its output in segments 3.7.17–3.7.18.

3.7.3. Although our application is global, this algorithm may equally be constructed in a purely p -adic situation.¹¹ In order to minimize the number of decorations, we introduce notation specific to the present situation; these will remain in effect through the proof of Proposition 3.7.18.

We let $\mathbf{F}\phi$ denote the category of mixed Tate filtered ϕ modules over \mathbb{Q}_p . We let

$$\Omega : \mathbf{F}\phi \rightarrow \text{Vect}(\mathbb{Q}_p)$$

denote the forgetful functor. As in segment 2.2.9, we let $U(\mathbb{Z}_p)$ denote the unipotent part of the Tannakian fundamental group $\text{Aut}^{\otimes}(\Omega)$. Given $E \in \mathbf{F}\phi$, $v \in \rho(E)$ and $f \in \rho(E)^\vee$, we let

$$[E, v, f]$$

denote the function

$$U(\mathbb{Z}_p) \rightarrow \mathbb{A}_{\mathbb{Q}_p}^1$$

given on a point γ with values in an arbitrary \mathbb{Q}_p -algebra by

$$\gamma \mapsto f(\gamma v).$$

Recall that u denotes the \mathbb{Q}_p -point of $U(\mathbb{Z}_p)$ associated to the p -adic period map.

Let D be a finite set of elements of \mathbb{Z}_p no two of which are congruent modulo p . Let $X := \mathbb{A}_{\mathbb{Z}_p}^1 \setminus D$. We consider two \mathbb{Z}_p -integral base points a, b of X . We let ${}_a P_a$ denote the filtered ϕ realization of the unipotent fundamental group of $X_{\mathbb{Q}_p}$ at a , a unipotent group object of $\mathbf{F}\phi$. We let ${}_b P_a$ denote the filtered

¹¹There’s a slight caveat: where the algorithm and its subalgorithms take p -adic numbers an input, those must be specified by a finite amount of data. This means that the domain of the algorithm must be restricted to those p -adic numbers which can be specified by a finite amount of data. However, since we’ve agreed not to keep track of ϵ , this restriction on the domain need not concern us any further.

ϕ realization of the unipotent path torsor. We let ${}_a\mathcal{U}_a$ denote the completed universal enveloping algebra of ${}_aP_a$ and let

$${}_b\mathcal{U}_a := {}_a\mathcal{U}_a \times_{{}_aP_a} {}_bP_a$$

be the associated rank one free module.

Lemma 3.7.4. *We put ourselves in the situation and the notation of segment 3.7.3. Consider an element c of the set D of punctures and a \mathbb{Z}_p -integral base point a of $X(\mathbb{Z}_p)$. Let e^c denote the element of ${}_a\mathcal{U}_a$ associated to monodromy about c . Then we have the equality*

$$ue^c = p \left(\sum_{\eta} \left(\int_c^a \eta \right) \eta \right) \cdot e^c \cdot \left(\sum_{\omega} \left(\int_a^c \omega \right) \omega \right)$$

in the noncommutative formal power series ring ${}_a\mathcal{U}_a$. Both sums run over the set of words in the family of differential forms

$$\left\{ \frac{dt}{t-d} \right\}_{d \in D}$$

and the integrals are regularized with respect to the unit tangent vector at c . The integral of the empty word is defined to be 1.

The proof (which is purely formal) spans segments 3.7.5–3.7.8.

3.7.5. We recall that each path torsor ${}_bP_a$ possesses a unique \mathbb{Q}_p -valued point contained in step 0 of the Hodge filtration

$$p^{\text{dR}} = {}_bP_a^{\text{dR}}$$

and a unique \mathbb{Q}_p -valued point

$$p^{\text{cris}} = {}_bP_a^{\text{cris}}$$

fixed by Frobenius. We have

$$up^{\text{dR}} = p^{\text{cris}}.$$

We use the de Rham path ${}_bP_a^{\text{dR}}$ to identify ${}_b\mathcal{U}_a$ with ${}_a\mathcal{U}_a$. Let us write ${}_b\omega_a$ for a word ω regarded as an element of ${}_b\mathcal{U}_a$. Thus,

$${}_b\omega_a = {}_bP_a^{\text{dR}} \cdot {}_a\omega_a.$$

In this notation,

$${}_bP_a^{\text{dR}} = {}_b1_a.$$

We denote ${}_c e_c^c$ simply by ϵ^c .

By Besser’s definition of the p -adic iterated integrals

$$\int_a^b \omega,$$

we have

$${}_b p_a^{\text{cris}} = \sum_{\omega} \left(\int_a^b \omega \right) {}_b \omega_a$$

where the integral of the empty word is defined to be 1.

3.7.6. We have

$${}_b p_a^{\text{dR}} \cdot {}_a \omega_a = {}_b \omega_b \cdot {}_b p_a^{\text{dR}}. \quad (*)$$

Indeed, this equality reduces to the case of a one-letter word

$$\omega = e^c.$$

We have

$${}_b e_b^c = {}_b p_c^{\text{dR}} \cdot \epsilon^c \cdot {}_c p_b^{\text{dR}}.$$

Since the composition of de Rham paths is again a de Rham path, it follows that both sides of equation (*) (when $\omega = e^c$) are equal to

$${}_b p_c^{\text{dR}} \cdot \epsilon^c \cdot {}_c p_a^{\text{dR}}.$$

3.7.7. By segment 3.7.6, we have for any word ω in the set D of punctures and any points a, b, c

$${}_c \eta_b \cdot {}_b \omega_a = {}_c (\eta \omega)_a.$$

3.7.8. We thus have

$$\begin{aligned} u({}_a e_a^c) &= u({}_a p_c^{\text{dR}} \cdot \epsilon^c \cdot {}_c p_a^{\text{dR}}) \\ &= u({}_a p_c^{\text{dR}}) \cdot u(\epsilon^c) \cdot u({}_c p_a^{\text{dR}}) \\ &= \left(\sum_{\eta} \left(\int_c^a \eta \right) {}_a \eta_c \right) \cdot p \epsilon^c \cdot \left(\sum_{\omega} \left(\int_a^c \omega \right) {}_c \omega_a \right) \\ &= {}_a \left(p \left(\sum_{\eta} \left(\int_c^a \eta \right) \eta \right) \cdot e^c \cdot \left(\sum_{\omega} \left(\int_a^c \omega \right) \omega \right) \right)_a. \end{aligned}$$

This completes the proof of Lemma 3.7.4.

3.7.9. *Action of u on an arbitrary loop-word.* Let ω be a word in the set D of punctures regarded as an element of the completed universal enveloping algebra ${}_a \mathcal{U}_a$ at a base-point a of X . Since the action of u on ${}_a \mathcal{U}_a$ respects multiplication, Lemma 3.7.4 coupled with the algorithm of [Dan-Cohen and Chatzistamatiou 2014] for computing p -adic iterated integrals provides an algorithm for computing any coefficient of the noncommutative formal power series $u\omega$ to precision ϵ .

3.7.10. *Remark on the unipotent nature of the action on loop algebras.* We recall that the generators e^c ($c \in D$) of the completed universal enveloping algebra ${}_a \mathcal{U}_a$ (or “loop algebra”) have half-weight -1 and that the action of $U(\mathbb{Z}_p)$ (and hence of u) on ${}_a \mathcal{U}_a$ is unipotent with respect to the weight filtration. More specifically, the formula of Lemma 3.7.4 shows that $u\omega$ has coefficient 1 in front of the word ω itself,

and that every word which occurs with nonzero coefficient has ω as a subword (by which we mean a subsequence of not necessarily consecutive letters).

3.7.11. *Action of u on arbitrary path-words.* Let ω be a word in the set D of punctures regarded as an element of the completed universal enveloping bimodule ${}_b\mathcal{U}_a$ associated to a pair of base-points a and b of X . The algorithm of segment 3.7.9 may be upgraded to an algorithm which computes any coefficient of the noncommutative formal power series $u\omega$ to precision ϵ , or, which is the same, an algorithm which computes the p -adic period

$$[{}_b\mathcal{U}_a, \omega, f_{\omega'}](u)$$

of any matrix entry $[{}_b\mathcal{U}_a, \omega, f_{\omega'}]$. Indeed, $[{}_b\mathcal{U}_a, \omega, f_{\omega'}](u)$ is the ω' -coefficient of the noncommutative formal power series

$$u({}_b\omega_a) = u({}_b p_a^{\text{dR}} \cdot {}_a\omega_a) = {}_b p_a^{\text{cris}} \cdot u({}_a\omega_a). \tag{*}$$

Using the algorithm of segment 3.7.9, we expand $u({}_a\omega_a)$ as a linear combination of words

$$u({}_a\omega_a) = \sum_{\eta} c_{\eta} \cdot {}_a\eta_a$$

with coefficients $c_{\eta} \in \mathbb{Q}_p$ computed to p -adic precision ϵ . We then have

$$\begin{aligned} [{}_b\mathcal{U}_a, \omega, f_{\omega'}](u) &= f_{\omega'}(u({}_b\omega_a)) \\ &= f_{\omega'}({}_b p_a^{\text{cris}} \cdot u({}_a\omega_a)) \\ &= f_{\omega'}({}_b p_a^{\text{cris}} \cdot \sum_{\eta} c_{\eta} \cdot {}_a\eta_a) \\ &= \sum_{\eta} c_{\eta} f_{\omega'}({}_b p_a^{\text{cris}} \cdot {}_a\eta_a) \\ &= \sum_{\eta} c_{\eta} \int_a^b \omega' / \eta \end{aligned}$$

where the right-division ω' / η is defined to be zero whenever ω' is not right-divisible by η . Using [Dan-Cohen and Chatzistamatiou 2014] again we compute these last p -adic iterated integrals to precision ϵ .

3.7.12. *Remark on the unipotent nature of the action on path modules.* We recall that the generators e^c ($c \in D$) of the completed universal enveloping bimodule ${}_b\mathcal{U}_a$ (or “path module”) have half-weight -1 and that the action of $U(\mathbb{Z}_p)$ (and hence of u) on ${}_b\mathcal{U}_a$ is unipotent with respect to the weight filtration. This squares with the computation of segment 3.7.11. To see this more clearly, we repeat the computation in slightly different notation: we have

$$u({}_b\omega_a) = {}_b p_a^{\text{cris}} \cdot u({}_a\omega_a) = \sum_{\theta} \left(\int_a^b \theta \right) {}_b\theta_a \cdot \sum_{\eta} c_{\eta} {}_a\eta_a = \sum_{\theta, \eta} \left(c_{\eta} \int_a^b \theta \right) {}_b\theta\eta_a.$$

We find that the coefficient in front of the word $\omega = \eta$ ($\theta = 1$) is 1, and that all words occurring in the sum are left-multiples of words which contain ω as a subword.

3.7.13. *Elementary remarks on matrices with respect to unordered bases.* Let k be a field, V, W finite dimensional vector spaces,

$$\phi : V \rightarrow W$$

a linear map, \mathcal{V} a basis of V and \mathcal{W} a basis of W . Then the associated matrix is indexed by the set $\mathcal{V} \times \mathcal{W}$. The entry associated to the pair (v, w) is given by

$${}_w\phi_v = w^\vee(\phi v)$$

where w^\vee is the linear functional on W dual to w with respect to the basis \mathcal{W} .

If $V = \bigoplus_i V_i$, $W = \bigoplus_j W_j$ are finite direct sums of finite dimensional vector spaces with bases \mathcal{V}_i , \mathcal{W}_j and $\phi = \bigoplus_{i,j} \phi_{i,j}$ is a direct sum of linear maps

$$\phi_{i,j} : V_i \rightarrow W_j,$$

then the matrix associated to ϕ is given in terms of the matrices of the $\phi_{i,j}$ as follows: if $v \in \mathcal{V}_i$ and $w \in \mathcal{W}_j$ then

$${}_w\phi_v = w(\phi_{i,j})_v.$$

3.7.14. *Elementary remarks on graded pieces of graded representations.* Let $\mathfrak{g} = \bigoplus_n \mathfrak{g}_n$ be a graded Lie algebra over a field k , $E = \bigoplus E_i$ a finite dimensional graded vector space,

$$\rho : \mathfrak{g} \rightarrow \mathfrak{gl} E$$

a graded representation. Let \mathcal{U} denote the universal enveloping algebra of \mathfrak{g} . Then the induced ring homomorphism

$$\rho : \mathcal{U} \rightarrow \text{End } E$$

preserves gradings. We spell out what this means. We let

$$\text{End}^n E \subset \text{End } E$$

denote the subspace of homomorphisms which are graded of graded degree n :

$$\text{End}^n E = \bigoplus_i \text{Hom}(E_i, E_{i+n}).$$

Then ϕ sends the n -th graded piece \mathcal{U}_n of \mathcal{U} into $\text{End}^n E$. This also means that ρ is compatible with projections, in the sense that the squares

$$\begin{array}{ccc} \mathcal{U} & \longrightarrow & \text{End } E \\ \downarrow & & \downarrow \\ \mathcal{U}_n & \longrightarrow & \text{End}^n E \end{array}$$

commute.

In terms of matrices, the projection has the effect of setting entries in all other graded degrees equal to zero. More precisely, if $\phi \in \text{End } E$ has n -th graded piece $\phi^n \in \text{End}^n E$, if $\mathcal{E} = \bigcup_i \mathcal{E}_i$ is a graded basis of E and if $v \in \mathcal{E}_i, w \in \mathcal{E}_j$ are basis vectors of graded degrees i and j , respectively, then

$${}_w\phi_v^n = \begin{cases} {}_w\phi_v & \text{if } j - i = n, \\ 0 & \text{otherwise.} \end{cases}$$

To see this, let P_i denote the idempotent

$$E \rightarrow E_i \hookrightarrow E$$

associated to the i -th graded piece. Then

$$\phi^n(v) = P_{i+n}\phi(v),$$

so

$${}_w\phi_v^n = w^\vee P_{i+n}\phi(v).$$

We complete the verification by noting that

$$w^\vee \circ P_{i+n} = \begin{cases} w^\vee & \text{if } j = i + n, \\ 0 & \text{otherwise.} \end{cases}$$

3.7.15. *Universal polynomials for entries of products of graded pieces of the logarithm of a matrix.* Let $\text{Word}(D)$ denote the set of words in the set D of punctures. Let R be the polynomial \mathbb{Q} -algebra

$$R = \mathbb{Q}[\text{Word } D \times \text{Word } D]$$

graded by setting the degree of a word equal to minus its length as usual. We denote the generator associated to a pair of words ω, η by $x_{\omega,\eta}$. Let M be the $\text{Word } D \times \text{Word } D$ -matrix whose (ω, η) -th entry ${}_\eta M_\omega$ is 1 if $\omega = \eta, x_{\omega,\eta}$ if η contains ω as a subword, and 0 otherwise. Then the logarithm of M converges (in the sense that each entry is a polynomial). We let

$$N = \log M.$$

For any integer l , we define a new matrix ${}^l N$ with entries

$${}^l N_\omega = \begin{cases} {}_\eta N_\omega & \text{if } |\eta| - |\omega| = l, \\ 0 & \text{otherwise.} \end{cases}$$

Let w be a word of length n in D and let

$$w = l_1 \cdots l_r$$

be a word in the set $\mathbb{Z}_{<0}$ of negative integers such that

$$l_1 + \cdots + l_s = -n.$$

We define a polynomial $P(\omega, w) \in R$ by taking the (\emptyset, ω) -th entry

$$P(\omega, w) = {}_{\omega} [{}^{l_1} N \cdots {}^{l_s} N]_1$$

of the product of graded pieces of N indicated by ω .

3.7.16. Main algorithm. We now arrive at the construction of the realization algorithm. As input, the algorithm takes a positive real number ϵ , a prime number p , a finite set D of elements of \mathbb{Z}_p and two further elements a, b (given up to p -adic precision ϵ), a natural number n , a word ω of length n in the set D , and a word w of degree n in the set of symbols

$$\{v_{-1}, v_{-2}, v_{-3}, \dots\}$$

indexed and weighted by the negative integers. Distinct points in the set $D \cup \{a, b\}$ must not be congruent modulo p , but the elements a, b may belong to the set D (in the latter case, they will be treated as unit tangent vectors). The output consists of a single element

$$\mathcal{A}_{\text{Real}}(\epsilon, p, D, a, b, \omega, w)$$

of \mathbb{Q}_p given up to p -adic precision ϵ . To construct it, we first check which variables $x_{\theta, \eta}$ intervene in the polynomial $P(\omega, w)$ constructed in segment 3.7.15. For each such variable, we apply the subalgorithm of segment 3.7.11 to compute the element

$$[{}_b \mathcal{U}_a, \eta, f_{\theta}](u)$$

of \mathbb{Q}_p to precision ϵ . We then output the value

$$\mathcal{A}_{\text{Real}}(\epsilon, p, D, a, b, \omega, w) = P(\omega, w)(\{[{}_b \mathcal{U}_a, \eta, f_{\theta}](u)\}_{\eta, \theta}).$$

3.7.17. We now announce the meaning of the output. In terms of the input, we let $X = \mathbb{A}_{\mathbb{Q}_p}^1 \setminus D$, and we work with the filtered ϕ unipotent path bimodule ${}_b \mathcal{U}_a$ on X . Let n be the length of the word ω . As in segment 4.9 of [Dan-Cohen and Wewers 2016], we define the *unipotent filtered ϕ iterated integral* $I_a^b(\omega) \in A(\mathbb{Z}_p)_n$ to be the Tannakian matrix entry

$$I_a^b(\omega) = [{}_b \mathcal{U}_a, {}_b 1_a, f_{\omega}].$$

Via the isomorphism

$$A(\mathbb{Z}_p)_n = \mathcal{U}(\mathbb{Z}_p)_{-n}^{\vee},$$

the unipotent filtered ϕ iterated integral $I_a^b(\omega)$ may be *evaluated* at the element $w \in \mathcal{U}(\mathbb{Z}_p)_{-n}$.

Proposition 3.7.18. *The realization algorithm $\mathcal{A}_{\text{Real}}$ halts. Moreover, in the notation of segment 3.7.17, its output is within ϵ of the p -adic number $I_a^b(\omega)(w)$.*

Proof. The halting presents no issue. Turning to the verification of the correctness of the output, we fix an arbitrary input datum

$$(\epsilon, p, D, a, b, \omega, w)$$

and we set ourselves the task of computing $I_a^b(\omega)(w)$ in terms of the periods

$$[{}_b\mathcal{U}_a, \eta, f_\theta](u);$$

this is mostly a matter of rearranging definitions. Let

$${}_b\mathcal{U}_a^{\geq -n} = {}_b\mathcal{U}_a / {}_b\mathcal{U}_a I^{n+1}$$

where I denotes the augmentation ideal of ${}_a\mathcal{U}_a$. The quotient module ${}_b\mathcal{U}_a^{\geq -n}$ has vector space basis consisting of words of length $\leq n$. We note that

$$[{}_b\mathcal{U}_a^{\leq -n}, \eta, f_\theta](u) = [{}_b\mathcal{U}_a, \eta, f_\theta](u)$$

so long as η and θ are both of length $\leq n$.

Let ${}_b\rho_a$ denote homomorphism of graded \mathbb{Q}_p -algebras

$$\mathcal{U}(\mathbb{Z}_p) \rightarrow \text{End } {}_b\mathcal{U}_a^{\leq -n}$$

induced by the action of the filtered ϕ Galois group $U(\mathbb{Z}_p)$ on the path bimodule ${}_b\mathcal{U}_a$. Then

$$I_a^b(\omega)(w) = {}_\omega [{}_b\rho_a(w)]_1$$

is the $(1, \omega)$ -th entry of the matrix associated to the endomorphism ${}_b\rho_a(w)$ of ${}_b\mathcal{U}_a^{\leq -n}$. To compute it, write w as a product of letters

$$w = l_1 \cdots l_s$$

which we identify with the negative integers which parametrize them (while taking care *not* to confuse the above juxtaposition of letters with the product of integers). Meanwhile, recall that for i a negative integer,

$$v_i = {}^i(\log u)$$

is the i -th graded piece of $\log u$. Thus, if we set M equal to the matrix associated to ${}_b\rho_a(u)$, and $N = \log M$, we have

$${}_b\rho_a(v_i) = {}^i N.$$

Consequently,

$${}_b\rho_a(w) = {}_b\rho_a(l_1) \cdots {}_b\rho_a(l_s) = {}^{l_1} N \cdots {}^{l_s} N.$$

Putting the pieces back together, we have

$$I_a^b(\omega)(w) = {}_\omega [{}_b\rho_a(w)]_1 = P(\omega, w)(\{\theta M_\eta\}_{\eta, \theta}) \sim_\epsilon P(\omega, w)(\{\theta \widetilde{M}_\eta\}_{\eta, \theta}) = \mathcal{A}_{\text{Real}}(\epsilon, p, D, a, b, \omega, w)$$

where \widetilde{M}_η denotes the ϵ -approximation produced by the algorithm of segment 3.7.11 and \sim_ϵ signals an error bounded by ϵ (up to an admissible change in ϵ). \square

3.8. Basis algorithm.

3.8.1. We now construct an algorithm which takes as input an open integer scheme

$$Z \subset \text{Spec } \mathcal{O}_K,$$

a prime p of \mathbb{Z} , a natural number n , and an

$$\epsilon \in p^{\mathbb{Z}},$$

and returns the following data:

- (1) An open subscheme $Z^o \subset Z$. We write

$$\bar{S} = \{q_1, \dots, q_s\}$$

for its complement.

- (2) Sets

$$\mathcal{E}_1^s = \{\log^U \alpha_{1,1}, \dots, \log^U \alpha_{1,r_1+r_2-1}\}, \quad \mathcal{E}_1^r = \{\log^U \beta_1, \dots, \log^U \beta_s\}$$

of unipotent logarithms of elements of $\mathcal{O}_{Z^o}^*$.

- (3) For each integer $n' \in [2, n]$,

- (a) a set of single-valued unipotent polylogarithms

$$\tilde{\mathcal{E}}_{n'} = \{\text{Li}_{n'}^{U,sv}(a_{n',1}), \dots, \text{Li}_{n'}^{U,sv}(a_{n',e_{n'}})\},$$

where e_m denotes the dimension of the motivic extension space

$$\text{Ext}_{Z^o}^1(\mathbb{Q}(0), \mathbb{Q}(m)),$$

- (b) a set $\mathcal{P}_{n'}$ of unipotent iterated integrals of half-weight n' ,

- (c) an $\epsilon' \in p^{\mathbb{Z}}$,

- (d) an algorithm which takes a pair I, J of unipotent iterated integrals of half-weight n' as input and returns a rational number

$$\langle I, J \rangle_{\epsilon'} \in \mathbb{Q}.$$

We denote this algorithm by A_{Basis} . We first announce the meaning of its output in Proposition 3.8.2; we then construct the algorithm in segments 3.8.3–3.8.11, and prove the proposition in segments 3.8.12–3.8.14.

Proposition 3.8.2. (1) *Suppose $A_{\text{Basis}}(Z, p, n, \epsilon)$ halts. Then we have:*

- (a) \mathcal{E}_1^s forms a basis of $A(\text{Spec } \mathcal{O}_K)_1$.

- (b) $\mathcal{E}_1^s \cup \mathcal{E}_1^r$ forms a basis of $A(Z^o)_1$.

- (c) Each $\tilde{\mathcal{B}}_{n'} := \tilde{\mathcal{E}}_{n'} \cup \mathcal{P}_{n'}$ ($n' = 2, 3, \dots, n$) forms a basis for a subspace $\tilde{\mathcal{B}}_{n'}$ of $A(Z^o)_{n'}$ complementary to the space $D_{n'}$ of decomposables. Moreover, the space $P_{n'}$ spanned by $\mathcal{P}_{n'}$ is disjoint from the space $E_{n'}$ of extensions.

- (d) Relative to this basis, the projection $\mathcal{E}_{n'}$ of $\tilde{\mathcal{E}}_{n'}$ onto $E_{n'}$ forms a basis of $E_{n'}$.
- (e) We let $\mathcal{B}_{n'} = \mathcal{E}_{n'} \cup \mathcal{P}_{n'}$, we let $\mathcal{D}_{n'}$ denote the set of monomials in $\mathcal{B}_{<n'}$, we let

$$\mathcal{A}_{n'} = \mathcal{B}_{n'} \cup \mathcal{D}_{n'},$$

and we denote by $|\cdot|_{\mathcal{A}}$ the norm induced on $A(Z^o)_{n'}$ by the basis $\mathcal{A}_{n'}$. If $\text{Li}_{n'}^{E,sv}(a_{n',i})$ denotes the projection of $\text{Li}_{n'}^{U,sv}(a_{n',i})$ onto $E_{n'}$ then we have

$$|\text{Li}_{n'}^{U,sv}(a_{n',i}) - \text{Li}_{n'}^{E,sv}(a_{n',i})|_{\mathcal{A}} < \epsilon'.$$

- (f) We have $\epsilon' \leq \epsilon$.
- (g) If I, J are unipotent iterated integrals of half-weight n' , and

$$\langle I, J \rangle_{\mathcal{A}}$$

denotes the inner product in which the basis $\mathcal{A}_{n'}$ is orthonormal, then

$$|\langle I, J \rangle_{\epsilon'} - \langle I, J \rangle_{\mathcal{A}}|_p < \epsilon'.$$

In other words, the algorithm produced as part (d) of the output of A_{Basis} computes this inner product up to precision ϵ' .

- (2) If Zagier's conjecture (Conjecture 2.2.5), Goncharov exhaustion (Conjecture 2.2.7) and the Hasse principle for finite cohomology (Condition 2.2.13) hold for n, Z , and K , then the computation $A_{\text{Basis}}(Z, p, n, \epsilon)$ halts.

3.8.3. We write d_G for the reduced Goncharov coproduct, regarded as a map

$$\text{CUI}(Z)_r \rightarrow (\text{CUI}(Z)_{>0})_r^{\otimes 2}.$$

3.8.4. The algorithm A_{Basis} searches arbitrarily through the countably infinite set of data $(Z^o, \tilde{\mathcal{E}}_{\leq n}, \mathcal{P}_{\leq n}, \epsilon')$. For the rest of the construction, we fix such a datum, and construct an algorithm which returns a boolean argument, as well as a function $\langle \cdot, \cdot \rangle_{\epsilon'}$. If the boolean result is *False*, we start over with a new datum. If the boolean result is *True*, we output

$$(Z^o, \tilde{\mathcal{E}}_{\leq n}, \mathcal{P}_{\leq n}, \epsilon', \langle \cdot, \cdot \rangle_{\epsilon'}).$$

For the base case with $n' = 1$ we require our basis to be of the form given in the proposition, with

$$\{a_{1,1}, \dots, a_{1,r_1+r_2-1}\}$$

a basis for \mathcal{O}_K^* , and each b_i a generator for a power of q_i .

3.8.5. We assume for a recursive construction that conditions (a)–(f) have been verified in half-weights $< n'$, and that the algorithm computing the inner products $\langle I, J \rangle_{\epsilon'}$ has been constructed in half-weights $< n'$. The inner products give us maps

$$\widetilde{U}_{I_{\mathcal{A}}} : \text{CUI}(Z^o)_r \rightarrow A(Z^o)_r \quad \text{and} \quad \widetilde{U}_{I_{\mathcal{A}}}^{\otimes 2} : \text{CUI}(Z^o)_r^{\otimes 2} \rightarrow A(Z^o)_r^{\otimes 2}$$

in the form of explicit matrices with rational coefficients with respect to the bases $\mathcal{A}_{<n'}$ of iterated integrals already constructed in lower half-weights.

3.8.6. We check if the divisors associated to the iterated integrals in $\mathcal{B}_{n'}$ are étale over Z^o ; if not, we return *false*.

3.8.7. We check each element I of $\tilde{\mathcal{E}}_{n'}$ for proximity to $E_{n'}$. To do so, we lift I to an integrand $w \in \text{CUI}(Z^o)_{n'}$, compute $\widetilde{U}_{I_{\tilde{\mathcal{A}}}}(d_G(w))$, and check that the p -adic norm of the resulting vector is $< \epsilon'$. If not, we return *False*.

3.8.8. We check

$$\widetilde{U}_{I_{\text{Std}}}^{F\phi}(\tilde{\mathcal{E}}_{n'})$$

for ϵ' -linear independence in the sense of segments 3.5 and 3.6 using the *realization algorithm* of segment 3.7. If this fails, we return *False*.

3.8.9. We check $d(\mathcal{P}_{n'} \cup \tilde{\mathcal{D}}_{n'})$ for ϵ' -linear independence by lifting $\mathcal{P}_{n'}$, $\tilde{\mathcal{D}}_{n'}$ to $\text{CUI}(Z^o)$ and applying $\widetilde{U}_{I_{\tilde{\mathcal{A}}}}^{\otimes 2} \circ d_G$. If this fails, we return *False*.

3.8.10. We check that ϵ' is sufficiently small compared to the spread of the basis $\tilde{\mathcal{A}}_{n'}$ that the projection onto the space $E_{n'}$ of extensions will preserve the linear independence of $\tilde{\mathcal{A}}_{n'}$. If this fails, we return *False*. Otherwise we return *True*.

3.8.11. For the inner product in half-weight n' , it suffices to construct

$$\langle w, x \rangle_{\epsilon'}$$

for $x \in \text{CUI}(Z^o)_{n'}$ arbitrary and $w \in \tilde{\mathcal{A}}_{n'}$ a basis element. We first construct the inner products

$$\{\langle w, x \rangle \mid w \in \mathcal{P}_{n'} \cup \tilde{\mathcal{D}}_{n'}\}.$$

It may happen that $\widetilde{U}_{I_{\tilde{\mathcal{A}}}}^{\otimes 2}(d_G(w))$ is not in the span V of the set

$$\mathcal{V} := \widetilde{U}_{I_{\tilde{\mathcal{A}}}}^{\otimes 2}(d_G(\mathcal{P}_{n'} \cup \tilde{\mathcal{D}}_{n'})). \quad (*)$$

Nevertheless, we may compute the projection w' of w onto V with respect to the basis $(\tilde{\mathcal{A}}^{\otimes 2})_{n'}$. Subsequently, expanding w' in the set \mathcal{V} is a matter of solving a system of linear equations with rational coefficients; the linear independence of $(*)$ established in step 3.8.9 above, implies the uniqueness of the solution.

To compute the remaining inner products

$$\{\langle w, x \rangle_{\epsilon'} \mid w \in \tilde{\mathcal{E}}_{n'}\},$$

we replace x by

$$x' = x - \sum_{w \in \mathcal{P}_{n'} \cup \tilde{\mathcal{D}}_{n'}} \langle x, w \rangle_{\epsilon'} w.$$

We then compute the projection of $\widetilde{U_{I_{\text{Stdd}}}^{F\phi}}(x')$ onto the span of $\widetilde{U_{I_{\text{Stdd}}}^{F\phi}}(\tilde{\mathcal{E}}_{n'})$ inside $\prod_{p|p} A(\mathcal{O}_p)$. The linear independence of the latter, established in segment 3.8.8 above, ensures that the resulting system of linear equations will have a unique solution.

This completes the construction of the algorithm.

3.8.12. We now prove Proposition 3.8.2. Suppose as in part (1) of the proposition that $A_{\text{Basis}}(Z, p, n, \epsilon)$ halts. Parts (a) and (b) are clear. For parts (c) and (d) we note that if ϵ -approximations are ϵ -linearly independent, then the actual vectors are linearly independent. Part (e) is clear, except for perhaps the admissibility of the change in ϵ' ; see segment 3.8.13 below. For part (f) we of course limit ourselves to searching through data satisfying $\epsilon' \leq \epsilon$ in the first place.

For part (g), we note that the square below, left, commutes.

$$\begin{array}{ccc} A(Z^o)_r & \xrightarrow{d} & (A(Z^o)^{\otimes 2})_r \\ \uparrow u_I & & \uparrow u_{I^{\otimes 2}} \\ \text{CUI}(Z^o)_r & \xrightarrow{d_G} & (\text{CUI}(Z^o)^{\otimes 2})_r \end{array} \quad \begin{array}{ccc} A(Z^o)_r & \xrightarrow{d} & (A(Z^o)^{\otimes 2})_r \\ \uparrow \widetilde{u}_{I_{\tilde{\mathcal{A}}}} & & \uparrow \widetilde{u}_{I_{\tilde{\mathcal{A}}}^{\otimes 2}} \\ \text{CUI}(Z^o)_r & \xrightarrow{d_G} & (\text{CUI}(Z^o)^{\otimes 2})_r \end{array}$$

Since the corresponding vertical arrows in the left and right squares differ by ϵ' , it follows that the square on the right fails to commute by at most ϵ' . This gives us the inequality of Proposition 3.8.2(g) up to a possible change in ϵ' stemming from the failure of $\widetilde{U_{I_{\text{Stdd}}}^{F\phi}}$ to respect two splittings: the splitting of

$$\tilde{E}_r \subset A(Z^o)_r$$

given by the complementary space $P_r \oplus D_r$ inside the source on the one hand and the splitting of

$$\widetilde{U_{I_{\text{Stdd}}}^{F\phi}}(\tilde{E}_r) \subset \prod_{p|p} A(\mathcal{O}_p)$$

induced by the standard basis inside the target on the other hand.¹² This is clearly admissible; we omit the details.

3.8.13. Returning to part (e), we must show that our modifications of ϵ form an algorithmically computable function which goes to zero with ϵ . This is elementary, and fits into the general setting of a valued field $(k, |\cdot|)$ and linear map

$$\phi : k^m \rightarrow k^n$$

with kernel E . We claim that if

$$|\phi x| < \epsilon$$

then

$$|x - E| < C\epsilon$$

¹²In fact, to decrease the change in ϵ , we could replace the standard basis of $A(\mathcal{O}_p)$ with a basis compatible with the decomposition of the latter into extensions, primitive nonextensions, and decomposables, as we do for $A(Z^o)$. The map $\widetilde{U_{I_{\tilde{\mathcal{A}}}}^{F\phi}}$ would then be nearly compatible with the splittings, yielding a function which is quadratic in ϵ .

for some algorithmically computable constant C . We let W denote the image of ϕ and V the coimage, both with induced norms. For $x \in k^m$ we let \bar{x} denote its image in V , and we let $\bar{\phi}$ denote the isomorphism

$$V \xrightarrow{\sim} W$$

induced by ϕ . We fix a metric isomorphism $V = W$ arbitrarily (in practice this would be accomplished by constructing orthonormal bases of both spaces), and we let C^{-1} be the absolute value of the smallest eigenvalue. Then for $x \in k^m$ we have

$$|\phi x| = |\bar{\phi} \bar{x}| \geq C^{-1} |\bar{x}| = C^{-1} |x - E|,$$

independently of the choice of metric isomorphism, which establishes the claim.

3.8.14. We turn to part (2) of the proposition: the conditional halting. If the conjectures of Zagier and Goncharov hold for the given input, then our search-space includes an open subscheme $Z^o \subset Z$, a basis $\mathcal{E}_{\leq n}$ of $E_{\leq n}$ consisting of single valued unipotent ($\leq n$)-logarithms which are combinatorially unramified over Z^o , and a linearly independent set $\mathcal{P}_{\leq n}$ of unipotent iterated integrals which are combinatorially unramified over Z^o completing $\mathcal{E}_{\leq n} \cup \mathcal{D}_{\leq n}$ to a basis of $A(Z^o)_{\leq n}$. Our claim is that if the Hasse principle holds, then for ϵ' sufficiently small, the boolean subalgorithm evaluated on the associated datum

$$(Z^o, \mathcal{E}_{\leq n}, \mathcal{P}_{\leq n}, \epsilon')$$

returns *True*. The map

$$\mathfrak{R}_p : \mathbb{Q}_p \otimes \text{Ext}_K^1(\mathbb{Q}(0), \mathbb{Q}(n)) \rightarrow \prod_{p|p} \text{Ext}_{\mathcal{O}_p}^1(\mathbb{Q}_p(0), \mathbb{Q}_p(n))$$

from the global motivic Ext group to the product of filtered ϕ Ext groups corresponds to the localization map of the Hasse principle through the p -adic regulator isomorphism of Soulé [1981] on the source and through the Bloch–Kato exponential map [Bloch and Kato 1990] on the target. So under the Hasse principle, the map

$$\text{Re}_p : A(Z^o)_n \rightarrow \prod_{p|p} A(\mathcal{O}_p)_n$$

(for $n \geq 2$) is injective near the extension space E_n . For any set of linearly independent vectors in a (finite dimensional) normed vector space, there exists an ϵ such that any set of ϵ -approximations is ϵ -linearly independent. So the claim follows. This concludes the proof Proposition 3.8.2.

Remark 3.8.15. Recall that the iterated integrals through which we search to form the set $\mathcal{P}_{\leq n}$ are parametrized by families of sections of \mathbb{P}^1 over Z^o (and have no particular relationship to $\mathbb{P}^1 \setminus \{0, 1, \infty\}$). Moreover, the Goncharov exhaustion conjecture places no bound on the height of points needed to form a basis. Thus, the search, as formulated here, is huge and unwieldy. Nevertheless, as a second attempt to convince the reader of the termination, we note that no matter how we order this countably huge set through which we search, if, as predicted by the conjectures, a successful candidate exists, it will, in due course, be met. In practice, we would probably place a height bound B on points and a bound C on the

size of $Z \setminus Z^o$ and then, in turns, increase B , decrease ϵ' , increase C . Beyond that, as mentioned in the introduction, pairing down the data and ordering it for an efficient search presents an interesting problem in its own right.

3.9. Change of basis algorithm.

3.9.1. We now construct an algorithm which changes the basis constructed by the basis algorithm to one which is compatible with the coproduct up to possible errors of size ϵ . This algorithm takes as input a datum $(Z^o, \tilde{\mathcal{E}}_{\leq n}, \mathcal{P}_{\leq n}, \epsilon, \langle \cdot, \cdot \rangle_\epsilon)$ as in the output of the basis algorithm A_{Basis} , and outputs for each $n' \leq n$, a square matrix of size $a_{n'} \times a_{n'}$ over \mathbb{Q} . We denote this algorithm by A_{Change} and the resulting n' -th matrix by

$$A_{\text{Change}}(Z^o, \tilde{\mathcal{E}}_{\leq n}, \mathcal{P}_{\leq n}, \epsilon, \langle \cdot, \cdot \rangle_\epsilon, n').$$

3.9.2. For each $n' \leq n$ we fix a set

$$\Sigma_{n'}^o = \{\sigma_{-n',1}, \dots, \sigma_{-n',e_{n'}}\}$$

of symbols, and define the half-weight of $\sigma_{-n',i}$ to be $-n'$. We may then speak about words in $\Sigma_{\geq -n}^o$ and about the half-weight of a word. Entries in our matrix will be indexed by pairs (I, w) , with

$$I \in \tilde{\mathcal{A}}_{n'} = \tilde{\mathcal{E}}_{n'} \cup \mathcal{P}_{n'} \cup \tilde{\mathcal{D}}_{n'}$$

($\tilde{\mathcal{D}}_{n'}$ denoting the set of monomials in $\tilde{\mathcal{B}}_{<n} = \tilde{\mathcal{E}}_{<n} \cup \mathcal{P}_{<n}$ of half-weight n as usual), and w a word in Σ^o of half weight $-n'$. We construct the associated matrix entry $a_{I,w}$ by recursion on the length of w . We write $\tilde{\mathcal{E}}_{n'}$ as a vector

$$\tilde{\mathcal{E}}_{n'} = (\tilde{\mathcal{E}}_{n',1}, \dots, \tilde{\mathcal{E}}_{n',e_{n'}})$$

(so $\tilde{\mathcal{E}}_{n',i} = \text{Li}_n^{U,sv}(a_{n',i})$ is a single-valued unipotent n' -logarithm). When $w = \sigma_{-n',i}$ is a one-letter word, we set

$$a_{I,w} = \begin{cases} 1 & \text{if } I = \tilde{\mathcal{E}}_{n',i}, \\ 0 & \text{otherwise.} \end{cases}$$

Now suppose $n' = l + m$ with $l, m > 0$, and let w be a word of half-weight $-m$. Using the Goncharov coproduct and the inner product, we expand

$$d_{l,m} I = \sum c_{j,k} \tilde{\mathcal{A}}_{l,j} \otimes \tilde{\mathcal{A}}_{m,k}$$

in the basis

$$\tilde{\mathcal{A}}_l \otimes \tilde{\mathcal{A}}_m = \{\tilde{\mathcal{A}}_{l,j} \otimes \tilde{\mathcal{A}}_{m,k}\}_{j,k}$$

of $A_l \otimes A_m$ to precision ϵ . In terms of the $c_{j,k}$, we define

$$a_{I, \sigma_{-l,i} \cdot w} = \sum_{j,k} c_{j,k} \cdot a_{\tilde{\mathcal{A}}_{l,j}, \sigma_{-l,i}} \cdot a_{\tilde{\mathcal{A}}_{m,k}, w}$$

which equals

$$\sum_k c_{i,k} a_{\tilde{\mathcal{A}}_{m,k},w}$$

if we number the basis $\tilde{\mathcal{A}}_m$ in such a way that

$$\tilde{\mathcal{A}}_{m,j} = \tilde{\mathcal{E}}_{m,j}$$

for $j \in [1, e_m]$.

3.9.3. We now make the meaning of the output precise. Let $\mathcal{E}_{n,i}$ denote the projection of $\tilde{\mathcal{E}}_{n,i}$ onto the space E_n of extensions (so in the context of the basis algorithm, we have $\mathcal{E}_{n,i} = \text{Li}_n^{E,sv}(a_{n,i})$). For each n , we let $\mathcal{B}_n = \mathcal{E}_n \cup \mathcal{P}_n$, and we let \mathcal{D}_n denote the set of monomials in $\mathcal{B}_{<n}$. According to Proposition 3.2.2,

$$\mathcal{A}_n := \mathcal{B}_n \cup \mathcal{D}_n$$

forms a basis of $A(Z^o)_n$. Let $\sigma_{-n,i} \in \mathcal{U}(Z^o)_{-n}$ denote the element dual to $\mathcal{E}_{n,i}$ relative to this basis. With this interpretation of the set Σ^o of symbols $\sigma_{-n,i}$, according to Proposition 3.2.3, Σ^o becomes a set of free generators of the free pronipotent group $U(Z^o)$. For $w \in \mathcal{U}(Z^o)_{-n}$ a word in Σ^o of half-weight $-n$, let $f_w \in A(Z^o)_n$ denote the corresponding function.

Let $(b_{w,I})_{w,I}$ denote the inverse of the matrix constructed in the algorithm. For w a word of half-weight $-n$, define $\tilde{f}_w \in A(Z^o)_n$ by

$$\tilde{f}_w = \sum_{I \in \tilde{\mathcal{A}}_n} b_{w,I} I.$$

Proposition 3.9.4. *In the situation and the notation above, we have*

$$|f_w - \tilde{f}_w| < \epsilon.$$

Proof. This is equivalent (up to an admissible change in ϵ) to the estimate

$$|a_{I,w} - \langle w, I \rangle| < \epsilon.$$

Our algorithm is based on the following two properties of the numbers $\langle w, I \rangle$ for w a word in our set of abstract generators Σ , and I an element of our concrete basis $\tilde{\mathcal{A}}_n$:

(1) We have

$$\left| \langle \sigma_{n,i}, I \rangle - \begin{cases} 1 & \text{if } I = \tilde{\mathcal{E}}_{n,i}, \\ 0 & \text{otherwise} \end{cases} \right| < \epsilon.$$

(2) We have

$$|\langle \sigma_{n,i} \cdot w, I \rangle - \langle \sigma_{n,i} \otimes w, dI \rangle| < \epsilon.$$

The proposition follows. □

4. Construction of geometric algorithms

4.1. Cocycle-evaluation-image algorithm. Fix finite sets $\Sigma_{-1}, \Sigma_{-2}, \Sigma_{-3}, \dots, \Sigma_{-n}$ and $\Sigma_{-1}^\circ, \Sigma_{-2}^\circ, \Sigma_{-3}^\circ, \dots, \Sigma_{-n}^\circ$ with

$$\Sigma_{-1} \subset \Sigma_{-1}^\circ$$

and $\Sigma_i^\circ = \Sigma_i$ for $i \leq -2$. Set

$$\Sigma = \bigcup \Sigma_i, \quad \Sigma^\circ = \bigcup \Sigma_i^\circ.$$

Let $\mathfrak{n}(\Sigma), \mathfrak{n}(\Sigma^\circ)$ denote the free graded pronilpotent Lie algebras on generators Σ, Σ° . As usual, we refer to the grading as the *half-weight*. Let \mathfrak{n}^{PL} denote the polylogarithmic Lie algebra over \mathbb{Q} ,

$$\mathfrak{n}^{\text{PL}} = \mathbb{Q}(1) \times \prod_{i=1}^{\infty} \mathbb{Q}(i)$$

with $\mathbb{Q}(i)$ in half-weight $-i$. We write $\text{Hom}_{\text{Lie}}^{\mathbb{G}_m}$ for homogeneous Lie-algebra homomorphisms of graded degree 0. Let ϕ denote the natural quotient map

$$\phi : \mathfrak{n}(\Sigma^\circ) \twoheadrightarrow \mathfrak{n}(\Sigma)$$

and let ev denote the map

$$\text{Hom}_{\text{Lie}}^{\mathbb{G}_m}(\mathfrak{n}(\Sigma), \mathfrak{n}^{\text{PL}}) \times \mathfrak{n}(\Sigma^\circ)_{\geq -n} \rightarrow \mathfrak{n}_{\geq -n}^{\text{PL}} \times \mathfrak{n}(\Sigma^\circ)_{\geq -n}$$

given by

$$\text{ev}(\mathcal{C}, F) = (\mathcal{C}(\phi(F)), F).$$

Then ev is in an obvious sense a map of finite dimensional affine spaces, and it is straightforward to construct an algorithm which computes its scheme-theoretic image. (At the very least, this would be a standard application of elimination theory, but in fact, it should be possible to obtain a closed formula.) We omit the details. We refer to this as the *cocycle-evaluation-image* algorithm. We denote it by $\mathcal{A}_{\text{Eval}}$, and its output, a finite list of elements of

$$\mathcal{S}^\bullet(\mathfrak{n}_{\geq -n}^{\text{PL}} \times \mathfrak{n}(\Sigma^\circ)_{\geq -n})^\vee,$$

by $\mathcal{A}_{\text{Eval}}(\Sigma, \Sigma^\circ, n)$.

4.2. Chabauty–Kim-loci algorithm.

4.2.1. We now construct the Chabauty–Kim-loci algorithm discussed in the introduction. As input it takes an open integer scheme Z , a prime p of \mathbb{Z} , a natural number n , and an $\epsilon \in p^{\mathbb{Z}}$. As output it returns a finite family

$$\tilde{\mathcal{B}} = \tilde{\mathcal{E}} \cup \mathcal{P}$$

of unipotent iterated integrals, and a finite family $\{\tilde{F}_i\}_i$ of elements of the polynomial ring

$$\mathbb{Q}[\tilde{\mathcal{B}}, \log, \text{Li}_1, \text{Li}_2, \dots, \text{Li}_n],$$

which we denote by $\mathcal{A}_{\text{LocI}}(Z, p, n, \epsilon)$.

4.2.2. We run $A_{\text{Basis}}(Z, p, n, \epsilon)$. This gives us our set $\tilde{\mathcal{B}} = \tilde{\mathcal{B}}_{\leq n}$ of unipotent iterated integrals. We run $\mathcal{A}_{\text{Change}}$ on $A_{\text{Basis}}(Z, p, n, \epsilon)$ to obtain a matrix

$$M_{\leq n} = \bigoplus_{i=0}^n M_i.$$

4.2.3. We let Σ_{-1} denote a set of size $e_1 = \dim \mathcal{O}_Z^* \otimes \mathbb{Q}$, Σ_{-1}^o a set containing Σ_{-1} of size $e_1^o = \dim \mathcal{O}_{Z^o}^* \otimes \mathbb{Q}$, and for each $i \in [2, n]$, $\Sigma_{-i} = \Sigma_{-i}^o$ a set of size

$$e_i = \dim \text{Ext}_K^1(\mathbb{Q}(0), \mathbb{Q}(i)).$$

We run $\mathcal{A}_{\text{Eval}}(\Sigma, \Sigma^o, n)$ to obtain a finite family $\{F_i^{\text{abs}}\}_i$ of elements of $S^\bullet(\mathfrak{n}_{\geq -n}^{\text{PL}} \times \mathfrak{n}(\Sigma^o)_{\geq -n})^\vee$.

4.2.4. We pull back along the quotient map

$$\mathfrak{n}(\Sigma^o) \twoheadrightarrow \mathfrak{n}(\Sigma^o)_{\geq -n}.$$

We pull back further along the logarithm

$$U(\Sigma^o) \rightarrow \mathfrak{n}(\Sigma^o).$$

Denoting the natural coordinates on \mathfrak{n}^{PL} by $\log, \text{Li}_1, \text{Li}_2, \text{Li}_3, \dots$, we obtain a finite family of elements of

$$S^\bullet \mathfrak{n}_{\geq -n}^{\text{PL}} \otimes A(\Sigma^o) = A(\Sigma^o)[\log, \text{Li}_1, \dots, \text{Li}_n]$$

which are contained in degrees $\leq n$.

4.2.5. The matrix $M_{\leq n}$ defines a linear bijection

$$A(\Sigma^o)_{\leq n} \xrightarrow{\sim} \mathbb{Q}[\tilde{\mathcal{B}}]_{\leq n}$$

which we use to obtain the hoped-for family $\{\tilde{F}_i\}_i$. This completes the construction of the algorithm.

4.2.6. *Proof of Theorem 2.4.1.* We have a sequence of maps

$$U(X)_{\geq -n, \mathbb{Q}_p}^{\text{PL}} \rightarrow \mathfrak{n}(X)_{\geq -n}^{\text{PL}} \times \text{Spec } \mathbb{Q}_p \rightarrow \mathfrak{n}(X)_{\geq -n}^{\text{PL}} \times \mathfrak{n}(Z^o) \rightarrow \mathfrak{n}(X)_{\geq -n}^{\text{PL}} \times \mathfrak{n}(Z^o)_{\geq -n}$$

and an associated sequence of Cartesian squares:

$$\begin{array}{ccc}
 \text{Hom}_{\text{Lie}}^{\mathbb{G}_m}(\mathfrak{n}(Z), \mathfrak{n}(X)_{\geq -n}^{\text{PL}} \times \mathfrak{n}(Z^o)_{\geq -n}) & \xrightarrow{\bar{e}\bar{v}_n} & \mathfrak{n}(X)_{\geq -n}^{\text{PL}} \times \mathfrak{n}(Z^o)_{\geq -n} \\
 \uparrow & & \uparrow \\
 \text{Hom}_{\text{Lie}}^{\mathbb{G}_m}(\mathfrak{n}(Z), \mathfrak{n}(X)_{\geq -n}^{\text{PL}} \times \mathfrak{n}(Z^o)) & \xrightarrow{e v_n} & \mathfrak{n}(X)_{\geq -n}^{\text{PL}} \times \mathfrak{n}(Z^o) \\
 \uparrow & & \uparrow \\
 \text{Hom}_{\text{Lie}}^{\mathbb{G}_m}(\mathfrak{n}(Z), \mathfrak{n}(X)_{\geq -n}^{\text{PL}} \times \text{Spec } \mathbb{Q}_p) & \xrightarrow{e v_n(v_p)} & \mathfrak{n}(X)_{\geq -n}^{\text{PL}} \times \text{Spec } \mathbb{Q}_p \\
 \uparrow & & \uparrow \\
 \text{Hom}_{\text{Groups}}^{\mathbb{G}_m}(U(Z), U(X)_{\geq -n}^{\text{PL}})_{\mathbb{Q}_p} & \xrightarrow{e v_n(u_p)} & U(X)_{\geq -n, \mathbb{Q}_p}^{\text{PL}}
 \end{array}$$

Γ

We write Im for scheme-theoretic image. By the mere commutativity of the outer square we have a containment of closed subschemes

$$\text{Im } e v_n(u_p) \subset \Gamma^{-1} \text{Im } \bar{e}\bar{v}_n.$$

In view of Propositions 3.8.2 and 3.9.4, this establishes part 1 of the theorem (correctness of the output upon halting).

For the conditional halting, we contend that formation of scheme-theoretic image along each horizontal map is compatible with pullback along each vertical map. We start at the top. For $v \in \mathfrak{n}(Z^o)$ mapping to $\bar{v} \in \mathfrak{n}(Z)$ and

$$\phi : \mathfrak{n}(Z) \rightarrow \mathfrak{n}(X)_{\geq -n}^{\text{PL}}$$

a \mathbb{G}_m -equivariant homomorphism, $\phi(\bar{v})$ depends only on the image of v in $\mathfrak{n}(Z^o)_{\geq -n}$. So

$$\text{Im } e v_n = (\text{Im } \bar{e}\bar{v}_n) \times \mathfrak{n}(Z^o)_{< -n}.$$

We go on to the middle square. By the period conjecture, $A(Z^o) \rightarrow \mathbb{Q}_p$ is flat. (In general, if A is integral, K a field, and $\psi : A \rightarrow K$ is injective, then ψ is flat, since it factors as a localization map followed by a field extension.) Hence formation of the scheme-image is compatible with pullback. Turning to the bottom square, the vertical maps are iso, so this is clear. This completes the proof of Theorem 2.4.1.

5. Construction of analytic algorithm

5.1. We now construct an algorithm for deciding whether the number of zeroes of a p -adic power series in a given ball is zero or one, given a sufficiently close approximation. This is quite standard, but we are unaware of a reference for this exact problem.

More precisely, we construct a boolean-valued algorithm which takes as input a boolean $b \in \{0, 1\}$, natural numbers N , r and h , and a polynomial with rational coefficients

$$\tilde{F} = \sum_{i=0}^N \tilde{a}_i T^i$$

which has at most b (\mathbb{Q}_p -rational) roots inside the disk of radius p^{-r} . We call this algorithm the *root criterion algorithm* and denote the output by $\mathcal{A}_{\text{RC}}(b, N, r, h, \tilde{F})$. We first announce the meaning of the output as a remark.

Remark 5.2. In our application below,

$$F = \sum_{i=1}^{\infty} a_i T^i$$

will be a power-series expansion of a polynomial in logarithms and polylogarithms of half-weight h over \mathbb{Q}_p , and \tilde{F} will be an approximation of F with arithmetic precision p^{-r} and geometric precision e^{-N} . Suppose $\mathcal{A}_{\text{RC}}(b, N, r, h, \tilde{F}) = \text{True}$. Then F has at most b roots within the disk of radius p^{-r} . This amounts to an elementary use of Newton polygons, together with the growth estimate

$$v(a_k) \geq -h \log_p(k)$$

which follows from Proposition 6.7 of Besser and de Jeu [2008].

Case 1: $b = 0$.

- (1) If $\tilde{a}_0 = 0$, return *False*.
- (2) Compute real solutions to

$$v(\tilde{a}_0) - rt = -h \log_p t$$

to within 0.5. If there are none, return *True*.

- (3) Otherwise, there are two solutions $t_L < t_R$. If $t_R > N$, return *False*.
- (4) Check the condition

$$v(\tilde{a}_k) > v(\tilde{a}_0) - rk$$

for $1 \leq k \leq t_R$. If the condition holds, return *True*. Otherwise return *False*.

Case 2.1: $b = 1$, $\tilde{a}_0 = 0$.

- (1) If $\tilde{a}_1 = 0$, return *False*.
- (2) Compute solutions to

$$-r(t-1) + v(\tilde{a}_1) = -h \log_p t$$

to within 0.5. If there are none, return *True*.

- (3) Otherwise, there are two solutions $t_L < t_R$. If $t_R > N$, return *False*.

(4) Check the condition

$$v(\tilde{a}_k) > -r(k - 1) + v(\tilde{a}_1)$$

for $2 \leq k \leq t_R$. If this condition holds, return *True*. Otherwise, return *False*.

Case 2.2: $b = 1, \tilde{a}_0 \neq 0$. In this case, we have

$$v(\tilde{a}_1) = v(\tilde{a}_0) - r \tag{*}$$

and

$$v(\tilde{a}_0) - rt = -h \log_p t \tag{**}$$

has two solutions $t_L < t_R$:

- (1) If $t_R > N$, return *False*.
- (2) Check the condition

$$v(\tilde{a}_i) > v(\tilde{a}_0) - ri$$

for $2 \leq i \leq t_R$. If this condition holds, return *True*, otherwise return *False*.

6. Numerical approximation

We present the results of the unpublished work [Dan-Cohen and Chatzistamatiou 2014] concerning computation of p -adic iterated integrals on the projective line. For background we refer the reader to [Furusho 2004; 2007] and to [Chatzistamatiou 2017]. The results of this section should be compared with prior and with concurrent works by Besser and de Jeu [2008], by Jarossay [2016], and by Ünver [2019].

6.1. Let K denote a finite extension of \mathbb{Q}_p . A general p -adic iterated integral on the line with arbitrary punctures with good reduction is a multiple polylogarithm up to sign: if the points a_1, \dots, a_m of \mathcal{O}_K^* lie in distinct residue disks, then we have

$$\int_{1_0}^{a_{m+1}} \left(\frac{dt}{t}\right)^{n_m-1} \frac{dt}{t - a_m} \cdots \left(\frac{dt}{t}\right)^{n_1-1} \frac{dt}{t - a_1} = (-1)^m \text{Li}_{n_1, \dots, n_m} \left(\frac{a_2}{a_1}, \frac{a_3}{a_2}, \dots, \frac{a_{m+1}}{a_m}\right)$$

(see Theorem 2.2 of [Goncharov 2001]). Here 1_0 denotes the tangent vector 1 at 0. We will restrict attention to the case $m = 1, a_1 = 1$, i.e., to iterated integrals on $\mathbb{P}^1 \setminus \{0, 1, \infty\}$; in terms of multiple polylogarithms, this means restricting attention to multiple polylogarithms of one variable. We do this merely for concreteness: the difficulty in going from this case to the general case is largely a notational one.

6.2. We work with the rigid analytic space equal to the closed unit disk minus the residue disk about 1:

$$U = \text{Spm } K\{t, u\}/(u(t - 1) - 1),$$

with log structure induced by the divisor $\{0\}$.¹³ The coordinate ring $\mathcal{O}(U)$ has a map

$$\rho_0 : \mathcal{O}(U) \rightarrow B := K\{t\}$$

as well as a map

$$\rho_1 : \mathcal{O}(U) \rightarrow A := K\{w, u\}/(wu - 1)$$

sending

$$t \mapsto w + 1$$

(recentering the unit circle). Both ρ_0 and ρ_1 are injective, and on a practical level, all computations that occur within the algorithm may in fact be carried out inside the rings A and B up to given arithmetic and geometric precision. There will be no need to verify convergence (or overconvergence) algorithmically. As usual, we do not keep track of the error incurred.

6.3. Remark. There are several possible treatments of the singular points $0, 1, \infty$. In one approach, we puncture over the residue field k (which corresponds, via Berthelot's theory of rigid analytic tubes, to removing residue disks over $\mathrm{Spm} K$). In another approach, we include the points $0, 1, \infty$, allowing log poles instead of puncturing; in Berthelot's construction of isocrystals, this does not require the use of log geometry. This approach is convenient for dealing with tangential base-points. (There is also the possibility of working with the rigid analytic thrice punctured line $\mathbb{P}_{\mathrm{Spm} K}^1 \setminus \{0, 1, \infty\}$, needed when considering points of bad reduction.) The resulting categories of unipotent isocrystals on the special fiber or of unipotent connections on any of the above rigid analytic spaces are all canonically equivalent. Our use of the rigid analytic space U means that we choose to mix the first two approaches.

6.4. We give a brief sketch of the definition of the p-adic multiple polylogarithms we wish to evaluate. We refer to Besser [2012; 2002] and to Chatzistamatiou [2017] for more thorough accounts.

We let $\mathrm{unVIC}(U)$ denote the category of unipotent vector bundles with integrable connection with log poles at 0. Its equivalence with, say, the category of unipotent isocrystals on $\mathbb{P}_k^1 \log 0 \setminus \{1, \infty\}$ endows it with a Frobenius pullback functor

$$F^* : \mathrm{unVIC}(U) \rightarrow \mathrm{unVIC}(U).$$

If ω, ω' are fiber functors *compatible with Frobenius*, then F^* acts on the Tannakian path torsor

$${}_{\omega'} P_{\omega} = \mathrm{Isom}^{\otimes}(\omega, \omega').$$

The exact notion of compatibility is a bit subtle, and we refer the reader to [Chatzistamatiou 2017] for a detailed discussion. The result of this detailed discussion however, is that in our setting, a naive approach will be sufficient.

¹³For us, this merely means that we will be working with differential forms with log poles at the origin; we will not make use of log geometry.

We consider the K -rational fiber functors

$$\text{unVIC}(U) \xrightarrow[\omega_x]{\omega_{1_0}} \text{Vect } K$$

associated to the tangent vector 1_0 and to x respectively. According to Besser [2012], there's a unique Frobenius fixed point $p^{\text{cris}} \in ({}_x P_{1_0})(K)$.

We let \tilde{E} denote the KZ-connection over U : $\tilde{E} = \mathcal{O}_U \langle\langle e_0, e_1 \rangle\rangle$, with connection given by

$$\nabla(W) = e_0 W \frac{dt}{t} + e_1 W \frac{dt}{1-t}$$

for any word W in e_0, e_1 . Thus, if

$$\mathcal{L} = \sum_W \mathcal{L}_W W$$

is an arbitrary section, we have

$$\nabla(W) = d\mathcal{L} + e_0 \mathcal{L} \omega_0 + e_1 \mathcal{L} \omega_1$$

where

$$\omega_0 := \frac{dt}{t}, \quad \omega_1 := \frac{dt}{t-1}, \quad \text{and} \quad d\mathcal{L} = \sum_W \mathcal{L}'_W W dt$$

is given by differentiating the coefficient functions.

Each K -rational fiber of \tilde{E} is canonically equal to

$$\mathcal{U} := K \langle\langle e_0, e_1 \rangle\rangle;$$

let λ_W denote the linear functional

$$\mathcal{U} \rightarrow K$$

associated to the word W . The Tannakian path p^{cris} gives rise to a linear map

$$p^{\text{cris}}_{\tilde{E}} : \tilde{E}(1_0) \rightarrow \tilde{E}(x).$$

In terms of the path p^{cris} and the linear functional λ_W , we define the p -adic multiple polylogarithms we wish to evaluate by

$$\text{Li}_W(x) = \lambda_W(p^{\text{cris}}_{\tilde{E}}(1)).$$

6.5. Our algorithm depends on a notion of *residue over residue disk*. In turn, this depends on an elementary lemma:

Lemma. *Suppose we have a congruence relation*

$$\sum_{i,j \geq 0} a_{i,j} w^i u^j \equiv \sum_{i,j \geq 0} b_{i,j} w^i u^j \pmod{(wu - 1)}$$

in the restricted formal power series ring $K\{w, u\}$. Then we have an equality of convergent sums

$$\sum_{j=0}^{\infty} a_{j+1,j} = \sum_{j=0}^{\infty} b_{j+1,j}$$

in the nonarchimedean field K .

Proof. We provide the details of this elementary verification. In a nonarchimedean field, a sum whose terms tend to zero converges, so the convergence is immediate. For the equality, suppose the congruence relation is witnessed by the equation

$$\sum_{i,j \geq 0} (a_{i,j} - b_{i,j}) = (wu - 1) \sum_{i,j \geq 0} c_{i,j} w^i u^j.$$

We then have for each $n, k \in \mathbb{N}$,

$$c_{n+k+1,k+1} = \sum_{r=1}^k a_{n+r,r} - \sum_{r=1}^k b_{n+r,r}.$$

Restricting attention to $n = 1$ and taking the limit as $k \rightarrow \infty$, we obtain the result. □

Returning to our definition of the residue, we consider the space

$$\Omega^1(U) = \mathcal{O}(U) \frac{dt}{t}$$

of rigid analytic 1-forms with log poles at the origin. The pullback of an arbitrary element

$$\omega = f(t, u) \frac{dt}{t}$$

along the map ρ_1 defined in segment 6.2 is given by

$$\rho_1^* \omega = (w + 1)^{-1} f(w + 1, w^{-1}) dw.$$

We define

$$\text{Res}_{D(1)} \omega := \text{Res}_{w < 1} (w + 1)^{-1} f(w + 1, w^{-1}),$$

where

$$\text{Res}_{w < 1} : K\{w, u\} / (wu - 1) \rightarrow K$$

is defined by

$$\text{Res}_{w < 1} \left(\sum_{i,j} a_{i,j} w^i u^j \right) := \sum_{j=0}^{\infty} a_{j+1,j}.$$

6.6. We will construct elements $\tau_1 \in \mathcal{U}$ and $L \in \tilde{E}(U)$ recursively. To do so, we set

$$\omega'_1 := \frac{pt^{p-1}dt}{t^p - 1}.$$

We denote the length of a word W by $|W|$. We also let $|W|_i$ denote the number of occurrences of the letter e_i . We set

$$\tau_1 := pe_1 + \sum_{\substack{|W| \geq 2 \\ |W|_1 \geq 1}} \tau_W W \tag{\#}$$

and

$$L = 1 + \sum_{|W| \geq 1} L_W W. \tag{\text{h}}$$

We require that L , which will be determined by a system of differential equations, satisfy the initial condition

$$L_W(0) = 0 \tag{\text{b}}$$

for all nonempty words W . We construct the functions L_W as elements of the ring A . There, we set $t := w + 1$. We may transport the 1-forms $\omega_0, \omega_1, \omega'_1$ to A in the obvious way. We may also formally differentiate as well as take residues about the open disk $|w| < 1$, which we continue to denote by $\text{Res}_{D(1)}$. A 1-form ω in the free rank-one module Adw has a primitive in A if and only if $\text{Res}_{D(1)} \omega = 0$. With these notations, and this last fact in mind, we define τ_W in terms of lower terms by

$$\tau_W = -\text{Res}_{D(1)} \left(p(L_{W/e_0} - L_{e_0 \setminus W})\omega_0 + \sum_{\substack{W=W'W'' \\ W', W'' \neq \emptyset}} L_{W'}\tau_{W''}\omega_1 - L_{e_1 \setminus W}\omega'_1 \right). \tag{*}$$

Notationally, the term with the left-division $e_1 \setminus W$ is equal to 0 if W is not left-divisible by e_1 . We define L_W in terms of lower terms by the differential equation

$$dL_W = p(L_{W/e_0} - L_{e_0 \setminus W})\omega_0 + \sum_{\substack{W=W'W'' \\ W'' \neq \emptyset}} L_{W'}\tau_{W''}\omega_1 - L_{e_1 \setminus W}\omega'_1, \tag{\star}$$

the equation being solvable over A since equation (*) above guarantees that the right-hand side has no residue. Again, terms with an impossible left or right division are to be interpreted as zero.

6.7. We now use the elements $\tau_W \in K$ to construct more elements $\tau_W^V \in K$ indexed by pairs of words V, W with

$$V \subset W$$

by which we mean that V occurs as an ordered subsequence of (not necessarily contiguous) letters. To do so, we let τ be the endomorphism of \mathcal{U} determined by

$$\tau(e_0) = pe_0 \tag{\#}$$

and

$$\tau(e_1) = \tau_1. \tag{a}$$

We then define τ_W^V by

$$\tau(V) = \sum_{W \supset V} \tau_W^V W. \tag{b}$$

6.8. We construct certain rational numbers $c_{i,j,W}$ ($i, j \in \mathbb{N}$, W a word in e_0, e_1) which arise from the KZ-connection. The k -th power of the covariant derivative applied to a word W' ,

$$\left(\frac{\nabla_{\partial/\partial t}^k W'}{k!} \right)$$

is of the form

$$\sum_{\substack{i+j=k \\ |W|_1 \leq j \\ |W|_0 \leq i}} \frac{c_{i,j,W}}{t^i(t-1)^j} W W'.$$

To compute the coefficients $c_{i,j,W}$ algorithmically, we simply apply

$$\begin{aligned} & \frac{\nabla_{\partial/\partial t}}{i+j+1} \left(\frac{1}{t^i(t-1)^j} W' \right) \\ &= \frac{1}{i+j+1} \left(\frac{-i}{t^{i+1}(t-1)^j} I + \frac{-j}{t^i(t-1)^{j+1}} I + \frac{1}{t^{i+1}(t-1)^j} e_0 + \frac{0}{t^i(t-1)^{j+1}} e_1 \right) W' \end{aligned}$$

iteratively and collect terms.

6.9. All ingredients above are independent of the endpoint. We now fix the point $x \in \mathbb{P}^1 \setminus \{0, 1, \infty\}(\mathcal{O}_K)$ at which we wish to evaluate. In terms of the rational coefficients constructed in segment 6.8, and in terms of a lift σ of Frobenius to K , we define for each word W , an element $\epsilon_W(x) \in K$ by the infinite sum

$$\epsilon_W(x) = \sum_{\{i,j \in \mathbb{N} \mid i \geq |W|_0, j \geq |W|_1\}} \frac{c_{i,j,W}(x^p - x)^{i+j}}{(x^\sigma)^i (x^\sigma - 1)^j}.$$

We will discuss its convergence below.

Theorem 6.9.1. (Joint with Andre Chatzistamatiou.) *Let T be a word in $\{e_0, e_1\}$, let p be a prime, let K be a finite extension of \mathbb{Q}_p and let $x \in \mathbb{P}^1 \setminus \{0, 1, \infty\}(\mathcal{O}_K)$. Then the p -adic multiple polylogarithm $\text{Li}_T^p(x)$ is given in terms of the values $L_W(x)$, in terms of the constants τ_W^V , in terms of the values $\epsilon_W(x)$, and in terms of multiple polylogarithms of lower weight, by*

$$\text{Li}_T^p(x) = (-1)^{|T|_0} (1 - p^{|T|})^{-1} \sum_{\substack{T=UW'W \\ W \supset V \\ V \neq T}} (-1)^{|V|_0} \epsilon_U(x) L_{W'}(x) \tau_W^V \text{Li}_V^p(x).$$

(In particular, the terms $\epsilon_U(x)$ and $L_{W'}(x)$ appearing on the right converge.)

6.10. Proof of Theorem 6.9.1.

6.10.1. Let ϕ denote the Frobenius lift

$$U \rightarrow U$$

over σ given by $\phi(t) = t^p$ and let ϕ' be a lift of Frobenius which fixes the endpoint x . For instance, when $K = \mathbb{Q}_p$ we may set $\phi'(t) = (t - x)^p + x$. (Over)convergence gives rise to a canonical isomorphism

$$\epsilon : \phi^* \tilde{E} \xrightarrow{\sim} \phi'^* \tilde{E}.$$

We recall that the pullback along the semilinear Frobenius lift ϕ is accomplished in two steps as a base-change along σ followed by a K -linear pullback, as in the familiar diagram

$$\begin{array}{ccccc} U & \xrightarrow{\phi/K} & U^\sigma & \xrightarrow{\sigma} & U \\ & \searrow & \downarrow & & \downarrow \\ & & \text{Spm } K & \xrightarrow{\sigma} & \text{Spm } K \end{array}$$

and similarly for ϕ' . In concrete terms, Frobenius-invariance of p^{cris} means that the square

$$\begin{array}{ccc} (\phi^* \tilde{E})(1_0) & \xrightarrow{p^{\text{cris}}_{\phi^* \tilde{E}}} & (\phi^* \tilde{E})(x) \\ \parallel & & \sim \downarrow \epsilon(x) \\ \sigma^* \tilde{E}(1_0) & \xrightarrow{\sigma^*(p^{\text{cris}}_{\tilde{E}})} & \sigma^* \tilde{E}(x) \end{array}$$

commutes.

6.10.2. Together with the choice of unit vector $1 \in \tilde{E}(1_0)$, the KZ-connection corepresents the fiber functor: for any unipotent connection E , we have

$$\text{Hom}(\tilde{E}, E) = E(1_0).$$

This is proved in a surprising way (using complex iterated integrals) by Kim [2009], and in a more straightforward way (via a certain iterative construction of universal extensions which has appeared in various places in the literature) for instance by Chatzistamatiou [2017]. This gives us a canonical identification between the fiber $\tilde{E}(1_0)$ and the completed universal enveloping algebra of the unipotent fundamental group. It also means that there's a unique overconvergent horizontal morphism

$$\theta : \tilde{E} \rightarrow \phi^* \tilde{E}$$

such that

$$\theta(1_0) : \tilde{E}(1_0) \rightarrow (\phi^* \tilde{E})(1_0) = \sigma^*(\tilde{E}(1_0))$$

sends $1 \mapsto \sigma^* 1$.

6.10.3. Let $\text{Li}(x)$ denote the noncommutative formal power series

$$\text{Li}(x) = \sum_W \text{Li}_W(x)W.$$

Placed side by side, θ , ϵ , and p^{cris} form a commutative diagram like so:

$$\begin{array}{ccc}
 1 & \xrightarrow{\quad} & \text{Li}(x) \\
 \downarrow \theta(1_0) & \begin{array}{c} \xrightarrow{p_{\tilde{E}}^{\text{cris}}} \\ \downarrow \theta(x) \end{array} & \downarrow \theta(x) \\
 \tilde{E}(1_0) & \xrightarrow{\quad} & \tilde{E}(x) \\
 \downarrow \theta(1_0) & \begin{array}{c} \xrightarrow{p_{\phi^*\tilde{E}}^{\text{cris}}} \\ \downarrow \epsilon(x) \end{array} & \downarrow \epsilon(x) \\
 (\phi^*\tilde{E})(1_0) & \xrightarrow{\quad} & (\phi^*\tilde{E})(x) \\
 \parallel & & \sim \\
 \sigma^*\tilde{E}(1_0) & \xrightarrow{\sigma^*(p_{\tilde{E}}^{\text{cris}})} & \sigma^*\tilde{E}(x) \\
 \downarrow & \begin{array}{c} \xrightarrow{\quad} \\ \downarrow \end{array} & \downarrow \\
 \sigma^*1 & \xrightarrow{\quad} & \sigma^*\text{Li}(x)
 \end{array}$$

We will see that $\text{Li}(x)$ is uniquely determined by the equation

$$\sigma^* \text{Li}(x) = \epsilon(x)\theta(x)(\text{Li}(x)).$$

6.10.4. It follows from the analysis of tangential fiber functors in [Chatzistamatiou 2017, Section 3.5] that there’s a canonical isomorphism from the fiber functor ω_{1_0} to the functor

$$\omega_0 : E \mapsto E(0)$$

which is compatible with the action of our chosen Frobenius lift ϕ . We claim that the fiber $\theta(0)$ of θ at 0, regarded as a map

$$\mathcal{U} \rightarrow \sigma^*\mathcal{U}$$

is equal to τ , and that the value $\theta(U)(1)$ of θ at the identity element 1 of $\tilde{E}(U)$ is equal to L . These facts follow from two key properties of θ , which in turn follow from a certain functorial characterization of θ . If

$$f : T \rightarrow U$$

is a rigid analytic space over U , and E is a quasicoherent sheaf over U , we set

$$E(T) := \Gamma(T, f^*E).$$

We let $\text{Vect } T$ denote the category of vector sheaves. We let ω_T denote the functor

$$\text{Vect } T \leftarrow \text{unVIC}(U \log 0)$$

induced by f (forget the connection and pull back). We let ω_{0T} denote the composite

$$\text{Vect } T \leftarrow \text{Vect } K \xleftarrow{\omega_0} \text{unVIC}(U).$$

We let $\phi_*\omega_T$ denote the composite

$$\text{Vect } T \xleftarrow{\omega_T} \text{unVIC}(U) \xleftarrow{\phi^*} \text{unVIC}(U),$$

and similarly for ω_{0_T} . Then we have canonical isomorphisms

$$\tilde{E}(T) = \text{Hom}(\omega_{0_T}, \omega_T), \quad \text{and} \quad (\phi^*\tilde{E})(T) = \text{Hom}(\phi_*\omega_{0_T}, \phi_*\omega_T),$$

which are natural in T . Moreover, translated through these isomorphisms, θ sends a 2-morphism

$$\omega_{0_T} \rightarrow \omega_T$$

to its composite with the 1-morphism ϕ^* . It follows, on the one hand, that the fiber $\theta(0)$ is the σ -linear ring homomorphism induced by the action of Frobenius on the unipotent fundamental group, and on the other hand, that the map of global sections $\theta(U)$ is equivariant for the right-action of $\tilde{E}(0)$ on $\tilde{E}(U)$ and for the right action of $\phi^*\tilde{E}(0)$ on $\phi^*\tilde{E}(U)$ through $\theta(0)$. This last property means that for any $g \in \mathcal{U}$, we have

$$\theta(U)(g) = \theta(U)(1) \cdot \theta(0)(g). \quad (\text{equivariance})$$

Thus, θ is completely determined by two small pieces: a *horizontal* piece $\mathcal{L} := \theta(U)(1)$, and a *vertical* piece $\mathcal{T} := \theta(0)$. Moreover, \mathcal{T} is determined by its action on the generators e_0 and e_1 . Finally,

$$\mathcal{T}(e_0) = pe_0$$

and $\mathcal{T}_1 := \mathcal{T}(e_1)$ has constant term 0 and linear term pe_1 .

6.10.5. We will now show that $L = \mathcal{L}$ and $\tau = \mathcal{T}$. We first obtain the initial condition for \mathcal{L} :

$$\mathcal{L}(0) = \theta(U)(1)(0) = \theta(0)(1(0)) = 1.$$

Here “1” denotes the empty word, regarded first as a section of \tilde{E} over U , and then as a section of $\phi^*\tilde{E}$ over U . Its *value* $1(0)$ is the unit element of the fiber $\tilde{E}(0)$, which gets sent to the unit element of $(\phi^*\tilde{E})(0)$ since $\phi(0)$ is a homomorphism.

By the horizontality of θ , we have the equation

$$\nabla'(\theta(U)(1)) = \theta(U)(\nabla 1) \quad (\#)$$

in the $\mathcal{O}(U)$ -module

$$\Gamma(U, (\phi^*\tilde{E}) \otimes \Omega_U^1) = (\phi^*\tilde{E})(U) \otimes \Omega^1(U) = (\phi^*\tilde{E})(U) \frac{dt}{t}.$$

Here, ∇' denotes the pullback of ∇ along the Frobenius lift ϕ . By the equivariance property, this equation may be rewritten in terms of \mathcal{L} and \mathcal{T} as follows. We denote the free generators ϕ^*e_i of $\phi^*\tilde{E}$ simply by e_i . We let ω'_i denote the pullback of ω_i by the Frobenius lift ϕ . With this notation, we have

$$\begin{aligned} d\mathcal{L} + \sum_{i=0,1} e_i \mathcal{L} \omega'_i &= \nabla \mathcal{L} \\ &= \theta(U)(\nabla(1)) \\ &= \theta(U) \left(\sum_{i=0,1} e_i \omega_i \right) \\ &= \sum_{i=0,1} \theta(U)(e_i) \omega_i \\ &= \sum_{i=0,1} \mathcal{L} \cdot \mathcal{T}(e_i(0)) \omega_i. \quad (\text{by equivariance}) \end{aligned} \tag{b}$$

Plugging in pe_0 for $\mathcal{T}(e_0)$ and

$$\mathcal{T}_1 = pe_1 + \sum_{|W| \geq 2} \mathcal{T}_W W$$

for $\mathcal{T}(e_1)$, we obtain

$$d\mathcal{L} + pe_0 \mathcal{L} \omega_0 + e_1 \mathcal{L} \omega'_1 = p\mathcal{L}e_0 \omega_0 + \mathcal{L} \mathcal{T}_1 \omega_1. \tag{b}$$

Modulo the augmentation ideal I , (b) becomes

$$d\mathcal{L}_\emptyset = 0.$$

Hence, from the initial condition, we find that

$$\mathcal{L}_\emptyset = 1.$$

Thus \mathcal{L} has the form

$$\mathcal{L} = 1 + \sum_{|W| \geq 1} \mathcal{L}_W W.$$

Projecting (b) onto the W -coordinate for an arbitrary word W , we find that the functions $L_W := \mathcal{L}_W$ satisfy segment 6.6(★). Applying $\text{Res}_{D(1)}$ to both sides of segment 6.6(★), we find that the constants $\tau_W := \mathcal{T}_W$ satisfy segment 6.6(*). This completes the verification that $\mathcal{L} = L$ and $\mathcal{T} = \tau$.

An overconvergent 1-form ω on U with log poles at the origin has an overconvergent primitive if and only if $\text{Res}_0 \omega = 0$ and $\text{Res}_{D(1)} \omega = 0$. It follows that L is overconvergent. In particular, the values $L_W(x)$ converge.

6.10.6. To compute ϵ , we write

$$\begin{aligned} \epsilon(\phi^* W') &= \sum_{k=0}^{\infty} (\phi^{\sharp} t - \phi'^{\sharp} t)^k \phi'^{*} \left(\frac{\nabla_{\partial/\partial t}^k W'}{k!} \right) \\ &= \sum_k (\phi^{\sharp} t - \phi'^{\sharp} t)^k \cdot \phi'^{*} \left(\sum_{\substack{i+j=k \\ |W|_0 \leq i \\ |W|_1 \leq j}} \frac{c_{i,j,W}}{t^i (t-1)^j} W W' \right) \\ &= \sum_{\substack{i,j \in \mathbb{N} \\ |W|_0 \leq i \\ |W|_1 \leq j}} \frac{c_{i,j,W} (\phi^{\sharp} t - \phi'^{\sharp} t)^k}{\phi'^{\sharp} (t^i (t-1)^j)} \phi'^{*} (W W'). \end{aligned}$$

The coefficient of $\phi'^{*} (W W')$ is independent of W' ; setting ϵ_W equal to this coefficient and valuating at $t = x$ we obtain the formula given in segment 6.9. The prounipotence of \tilde{E} implies convergence of ϵ . In particular, the values $\epsilon_W(x)$ converge.

6.10.7. Setting

$$v = \sum_T v_T T,$$

the equation

$$\epsilon(x) \theta(x)(v) = v$$

becomes

$$\begin{aligned} \sum_T v_T T &= \epsilon(x) \theta(x) \left(\sum_V v_V V \right) \\ &= \sum_V v_V \epsilon(x) \left(\sum_{\substack{W' \\ W \supset V}} L_{W'}(x) \tau_W^V W' W \right) \\ &= \sum_V v_V \sum_{\substack{W' \\ W \supset V}} L_{W'}(x) \tau_W^V \sum_U \epsilon_U(x) U W' W \\ &= \sum_{\substack{V,U,W' \\ W \supset V}} \epsilon_U(x) L_{W'}(x) \tau_W^V v_V U W' W \\ &= \sum_T \left(\sum_{\substack{T=UW'W \\ W \supset V}} \epsilon_U(x) L_{W'}(x) \tau_W^V v_V \right) T. \end{aligned}$$

Hence

$$v_T = \sum_{\substack{T=UW'W \\ W \supset V}} \epsilon_U(x) L_{W'}(x) \tau_W^V v_V = p^{|T|} v_T + \sum_{\substack{T=UW'W \\ W \supset V \\ V \neq X}} \epsilon_U(x) L_{W'}(x) \tau_W^V v_V.$$

So the equations

$$v_I = 1 \quad \text{and} \quad \epsilon(x)\theta(x)(v) = v$$

are equivalent to

$$v_I = 1$$

and

$$(1 - p^{|T|})v_T = \sum_{\substack{T=UW'W \\ V \neq X \\ W \supset V}} \epsilon_U(x)L_{W'}(x)\tau_W^V v_V$$

from which we obtain the formula for

$$\text{Li}_T(x) = v_T$$

given in the theorem.¹⁴ This completes the proof of Theorem 6.9.1.

6.11. We apply this to the computation of p -adic multiple zeta values. We have the path composition formula

$$\int_x^z \omega_n \cdots \omega_1 = \left(\sum_{i=0}^n \int_y^z \omega_n \cdots \omega_{i+1} \cdot \int_x^y \omega_i \cdots \omega_1 \right)$$

and the path reversal formula

$$\int_y^x \omega_n \cdots \omega_1 = (-1)^n \int_x^y \omega_n \cdots \omega_1.$$

If $f : Y \rightarrow X$ is an isomorphism of rigid curves, then

$$\int_{f(x)}^{f(y)} \omega_n \cdots \omega_1 = \int_x^y (f^* \omega_n) \cdots (f^* \omega_1).$$

Applying this to $\omega_i \in \left\{ \frac{dx}{x}, \frac{dx}{1-x} \right\}$, to

$$x \mapsto 1 - x$$

on \mathbb{P}^1 , and to an auxiliary point y , we obtain

$$\int_y^{-\bar{1}_1} \omega_n \cdots \omega_1 = (-1)^n \int_{-\bar{1}_1}^y \omega_n \cdots \omega_1 = \int_{\bar{1}_0}^{1-y} \omega_n^\circ \cdots \omega_1^\circ$$

where $\left(\frac{dx}{x}\right)^\circ = \left(\frac{dx}{1-x}\right)$ and $\left(\frac{dx}{1-x}\right)^\circ = \left(\frac{dx}{x}\right)$. So

$$\zeta(W) = \int_{\bar{1}_0}^{-\bar{1}_1} \omega_W = \sum_{W=W''W'} \int_y^{-\bar{1}_1} \omega_{W''} \int_{\bar{1}_0}^y \omega_{W'} = \sum_{W=W''W'} \text{Li}_{W''}(1-y)(\text{Li}_{W'} y).$$

¹⁴Actually, differing sign conventions necessitate the addition of the signs seen in the final formula to accord with the traditional definition.

7. The equation-solving algorithm

7.1. Construction of the algorithm.

7.1.1. We now construct the promised algorithm for totally real fields. Our algorithm takes as input an open integer scheme Z and outputs a finite set of elements of $X(Z)$. We denote the output by $\mathcal{A}_{\text{ES}}(Z)$. As explained in the introduction, the success of the algorithm depends on first finding $X(Z)$ by a naive search, and then proving that there are no other points by verifying that $X(Z_p)_n = X(Z)$. Recall also (from our formulation of the convergence conjecture (Conjecture 2.1.4)) that success (i.e., halting) depends also on the absence of repeated roots for n sufficiently large.

7.1.2. We find a prime p of \mathbb{Z} in the image of Z , for which Z is totally split. We fix arbitrarily a prime p of Z lying above p .

7.1.3. Our algorithm searches through the set of triples (n, N, ϵ) , $n, N \in \mathbb{N}$, ϵ in a countable subset of $\mathbb{R}_{>0}$ with accumulation point 0. After each attempt, we increase n and N and decrease ϵ . To each such triple, our algorithm assigns a set $X(Z)_n$ of points of $X(Z)$ and a boolean. If the boolean output is *True*, then we output $X(Z)_n$. If the boolean output is *False*, then we continue the search.

To produce the set $X(Z)_n$, we spend n seconds searching for points.¹⁵ To produce the boolean output, we follow the steps described in segments 7.1.4–7.1.9 below.

7.1.4. Partition $X(\mathcal{O}_p)$ into ϵ -balls, decreasing ϵ as needed to ensure that each ball contains at most one element of the set $X(Z)_n$ (our, potentially incomplete, list of integral points).

7.1.5. Run $\mathcal{A}_{\text{Loc}}(Z, p, n, \epsilon)$ to obtain a family $\{\tilde{F}_i\}_i$ of polylogarithmic functions. Symmetrize the family with respect to the S_3 -action using the formulas 2.1.3(*). Set h_i equal to the half-weight of \tilde{F}_i .

7.1.6. We focus our attention on an ϵ -ball B containing a rational representative $y \in B$. Expand each polylogarithmic function \tilde{F}_i to arithmetic precision ϵ and geometric precision e^{-N} about y ; denote the result by \tilde{F}_i^p .

7.1.7. Fixing i , write

$$\tilde{F}_i^p = \sum_{j=0}^N \tilde{a}_j T_j.$$

Check the following condition:

$$\text{For each } i \text{ and each } j \leq N, \text{ if } \tilde{a}_j \neq 0 \text{ then } |\tilde{a}_j| \geq \epsilon.$$

If this fails, return, *False*.

7.1.8. We continue to work with the single ϵ -ball B . Set b equal to the number of points (0 or 1) in $X(Z)_n \cap B$. Choose an $r \in \mathbb{N}$ such that $\epsilon \geq p^{-r}$. Run the root-criterion algorithm $\mathcal{A}_{\text{RC}}(b, N, r, h_i, \tilde{F}_i^p)$ for varying i .

¹⁵Evidently, this choice is arbitrary. In reality we would probably search up to a chosen height bound $B(n)$ which grows to ∞ as n goes to ∞ .

7.1.9. Repeat the steps of segments 7.1.6–7.1.9 for each ϵ -ball B . If for each ball B there exists an i such that

$$\mathcal{A}_{\text{RC}}(b, N, r, h_i, \widetilde{F}_i^{\text{p}}) = \text{True},$$

return *True*. Otherwise return *False*. This completes the construction of the algorithm.

7.2. Equation-solving theorem. We come to the main applications announced in the introduction.

Theorem 7.2.1. *Let Z be an open integer scheme with fraction field K :*

(1) *Suppose the algorithm $\mathcal{A}_{\text{ES}}(Z)$ halts. Then we have*

$$\mathcal{A}_{\text{ES}}(Z) = X(Z).$$

(2) *Assume K is totally real. Suppose Kim’s conjecture (Conjecture 2.1.4) holds for Z at level n . Suppose Zagier’s conjecture (Conjecture 2.2.5) holds for K and $n' \leq n$. Suppose Goncharov’s conjecture (Conjecture 2.2.7) holds for Z and $n' \leq n$. Suppose the period conjecture holds for the open subscheme $Z^o \subset Z$ constructed in segment 3.8 in half-weights $n' \leq n$. Suppose K obeys the Hasse principle for finite cohomology (segment 2.2.12) in half-weights $2 \leq n' \leq n$. Then $\mathcal{A}_{\text{ES}}(Z)$ halts.*

(3) *Assume $K = \mathbb{Q}$. Suppose Kim’s conjecture holds for Z at level n . Suppose Goncharov’s conjecture holds for Z and $n' \leq n$. Suppose the period conjecture holds for the open subscheme $Z^o \subset Z$ constructed in segment 3.8 in half-weights $n' \leq n$. Then $\mathcal{A}_{\text{ES}}(Z)$ halts.*

Proof. Parts (1) and (2) are a direct application of Theorem 2.4.1. One point may require clarification: the role of segment 7.1.7. Let $\{F_i^{\text{p}}\}_i$ denote the generators of the Chabauty–Kim ideal close to $\{\widetilde{F}_i^{\text{p}}\}_i$ whose existence is guaranteed by Theorem 2.4.1. Fixing an ϵ -ball B with representative $y \in B$ and an i , write

$$F_i^{\text{p}} = \sum_{j=1}^{\infty} a_j T^j \quad \text{and} \quad \widetilde{F}_i^{\text{p}} = \sum_{j=0}^{\infty} \widetilde{a}_j T^j$$

for the power series expansions about y . Then after an admissible change in ϵ (depending on N), we have

$$|a_j - \widetilde{a}_j| < \epsilon$$

for all $j \leq N$. By construction, we have

$$|\widetilde{a}_j - \widetilde{\widetilde{a}}_j| < \epsilon,$$

hence

$$|a_j - \widetilde{\widetilde{a}}_j| < \epsilon.$$

For part (1) of the theorem, suppose that for given B , i and j , we find that $|\widetilde{\widetilde{a}}_j| \geq \epsilon$. Then by the nonarchimedean triangle inequality, we have

$$|\widetilde{\widetilde{a}}_j| = |a_j|.$$

This means that those valuations whose precise determination is needed for the root criterion algorithm \mathcal{A}_{RC} , will indeed be precise. For part (2), we need only note that for ϵ sufficiently small depending on N , we will indeed have for each ϵ -ball B , each i , and each $j \leq N$, either $\tilde{a}_j = 0$ or $|\tilde{a}_j| \geq \epsilon$.

We turn to part (3). The period conjecture implies in particular that the p -adic zeta values $\zeta^p(n')$ for $n' \in [3, n]$ odd are nonzero. In turn, this implies that the unipotent zeta values

$$\zeta^U(n') \in \text{Ext}^1(\mathbb{Q}(0), \mathbb{Q}(n'))$$

are nonzero. Since these extension groups have dimension 1 while the remaining extension groups have dimension 0, this would imply Zagier’s conjecture in this case. (In fact, since the extension groups for $n \geq 2$ don’t depend on Z , we’re free to choose any prime p . Choosing a regular one, where the nonvanishing is known, we obtain one possible proof of Zagier’s conjecture for this case.)

We claim that the period conjecture also implies the Hasse principle. Indeed, the Hasse principle in this case merely says that a linear map from a vector space of dimension ≤ 1 is injective. For this, it’s enough to show that the map is nonzero. However, the composite map

$$\mathbb{Q}_p \otimes \text{Ext}_Z^1(\mathbb{Q}(0), \mathbb{Q}(n')) \rightarrow \text{Ext}_{\mathbb{Z}_p}^1(\mathbb{Q}_p(0), \mathbb{Q}_p(n')) \rightarrow \mathbb{Q}_p$$

sends $\zeta^U(n')$ to $\zeta^p(n')$ which, as we’ve already noted, is nonzero if the period conjecture holds. □

8. Beyond totally real fields

8.1. We first explain the inadequacy of the methods developed above for dealing with fields which are not totally real.

Proposition. *Let Z be an open integer scheme, n a natural number, $\mathfrak{p} \in Z$ a totally split prime, and $X(\mathcal{O}_{\mathfrak{p}})_n$ the associated polylogarithmic Chabauty–Kim locus. Suppose Z is not totally real, and assume the period conjecture holds. Then $X(\mathcal{O}_{\mathfrak{p}})_n = X(\mathcal{O}_{\mathfrak{p}})$.*

Proof. In this case, each motivic Ext group $\text{Ext}_Z^1(\mathbb{Q}(0), \mathbb{Q}(n))$ is nonzero, and by the period conjecture, each (abelian) syntomic realization map

$$\text{Ext}_Z^1(\mathbb{Q}(0), \mathbb{Q}(n)) \rightarrow \text{Ext}_{\mathcal{O}_{\mathfrak{p}}}^1(\mathbb{Q}_p(0), \mathbb{Q}_p(n))$$

is at least nonzero. Since the motivic Ext^2 -groups are nevertheless zero, the Selmer scheme

$$H^1(G(Z), U(X)_{\geq -n}^{\text{PL}})$$

is an $\text{Ext}_Z^1(\mathbb{Q}(0), \mathbb{Q}(n))$ -torsor over $H^1(G(Z), U(X)_{\geq -(n-1)}^{\text{PL}})$. The realization map

$$\mathfrak{R}_{\mathfrak{p}} : H^1(G(Z), U(X)_{\geq -n}^{\text{PL}}) \rightarrow H^1(G(\mathcal{O}_{\mathfrak{p}}), U(X)_{\geq -n}^{\text{PL}})$$

is compatible with torsor structures. It follows by induction that $\mathfrak{R}_{\mathfrak{p}}$ is surjective, which completes the proof of the proposition. □

8.2. Instead of considering the single realization map \mathfrak{R}_p we may consider the product, which fits into a square similar to the one considered above

$$\begin{CD} X(Z) @>>> \prod_{p|p} X(\mathcal{O}_p) \\ @VVV @VV\alpha V \\ H^1(G(Z), U(X)_{\geq -n}^{\text{PL}}) @>\mathfrak{R}_p>> \prod_{p|p} H^1(G(\mathcal{O}_p), U(X)_{\geq -n}^{\text{PL}}). \end{CD}$$

We define the *big polylogarithmic Chabauty–Kim locus* by

$$\left(\prod_{p|p} X(\mathcal{O}_p) \right)_n := \alpha^{-1}(\text{Im } \mathfrak{R}_p).$$

and we again symmetrize with respect to the S_3 action to obtain a *symmetrized big polylogarithmic Chabauty–Kim locus*

$$\left(\prod_{p|p} X(\mathcal{O}_p) \right)_n^{S_3}.$$

We also write $\mathcal{K}_p^{\text{Big}}(\mathfrak{n}_{\geq -n}^{\text{PL}})$ and $\mathcal{K}_p^{\text{Big}}(\mathfrak{n}_{\geq -n}^{\text{PL}})S_3$ for the corresponding ideals of Coleman functions, the *big p-adic Chabauty–Kim ideal* and *symmetrized big p-adic Chabauty–Kim ideal*, respectively. We restrict ourselves as usual to the totally split case for simplicity.

Conjecture 8.2.1 (convergence of polylogarithmic loci, general case. Joint with David Corwin). *Let Z be an open integer scheme and p a prime below Z , for which Z is totally split. For each $n \in \mathbb{N}$ let $\left(\prod_{p|p} X(\mathcal{O}_p)\right)_n^{S_3}$ denote the associated symmetrized big polylogarithmic Chabauty–Kim locus. Then for some n we have*

$$X(Z) = \left(\prod_{p|p} X(\mathcal{O}_p) \right)_n^{S_3}.$$

8.3. A straightforward modification of the algorithm $\mathcal{A}_{\text{LocI}}$ yields an algorithm which produces approximate generators for the ideal of polylogarithmic functions defining the big polylogarithmic loci. Its output includes an algebra basis \mathcal{B} of $A(Z^\circ)_{\leq n}$ for Z° an open subscheme of Z , as well as a family of elements \tilde{F}_i of the polynomial ring

$$\mathbb{Q}[\mathcal{B}, \{\log t_p\}_p, \{\text{Li}_i t_p\}_{i,p}].$$

We denote its output by $\mathcal{A}_{\text{Big-LocI}}(Z, p, n, \epsilon)$. The result is a theorem which is analogous to the one stated above.

Theorem 8.3.1. *Let Z be an open integer scheme, p a prime over which Z is totally split, n a natural number, and $\epsilon \in p^{\mathbb{Z}}$:*

- (1) Suppose $\mathcal{A}_{\text{Big-Local}}(Z, p, n, \epsilon)$ halts. Then there are functions $\{F_i^p\}$ generating the big p -adic Chabauty–Kim ideal $\mathcal{K}_p^{\text{Big}}(\mathfrak{n}_{\geq -n}^{\text{PL}})$ associated to $\mathfrak{n}_{\geq -n}^{\text{PL}}$ such that

$$|\tilde{F}_i^p - F_i^p| < \epsilon$$

for all i .

- (2) Suppose Zagier’s conjecture (Conjecture 2.2.5) holds for K and $n' \leq n$. Suppose Goncharov exhaustion (Conjecture 2.2.7) holds for Z and $n' \leq n$. Suppose the period conjecture holds for the open subscheme $Z^o \subset Z$ constructed in segment 3.8 in half-weights $n' \leq n$. Suppose K obeys the Hasse principle for finite cohomology (segment 2.2.12) in half-weights $2 \leq n' \leq n$. Then the computation $\mathcal{A}_{\text{Local}}(Z, p, n, \epsilon)$ halts.

Appendix: A minor erratum

A.1. The article [Goncharov 2001] contains a minor error: if Lemma 3.7 of that article were true, our algorithm could be greatly simplified. However, Clément Dupont has pointed out the following simple counterexample: $(\log^U 2)\zeta^U(3)$ is ramified at 2. To see this, note that $A(\text{Spec } \mathbb{Z})_4 = 0$, that $A(\text{Spec } \mathbb{Q})$ is an integral domain, and that both $\log^U 2$ and $\zeta^U(3)$ are nonzero. However, since both of these elements are contained in the space of extensions, in the notation of that article, we have $\Delta'_{[4]}((\log^U 2)\zeta^U(3)) = 0$.

Acknowledgements

I would like to thank Stefan Wewers for helpful conversations during the conference on multiple zeta values in Madrid in December of 2014. I would like to thank Minhyong Kim, Amnon Besser, Francis Brown, Francesc Fité, Go Yamashita for helpful conversations and email exchanges. I would like to thank Clément Dupont for long conversations during our time in Sarriens, and for pointing out a very helpful counterexample (see the appendix). I would like to thank Rodolfo Venerucci for conversations about finite cohomology. I would like to thank Jochen Heinloth and Giuseppe Ancona for help improving my presentation of the results. I would like to thank David Corwin for a careful reading and many helpful comments; moreover, in the course of our joint work [Corwin and Dan-Cohen 2018a], we discovered that Conjecture 2.1.4 was false as stated in a previous draft. Finally, I wish to thank the referees for their helpful comments and suggestions.

References

- [Baker and Wüstholz 2007] A. Baker and G. Wüstholz, *Logarithmic forms and Diophantine geometry*, New Math. Monogr. **9**, Cambridge Univ. Press, 2007. MR Zbl
- [Balakrishnan et al. 2018] J. S. Balakrishnan, I. Dan-Cohen, M. Kim, and S. Wewers, “A non-abelian conjecture of Tate–Shafarevich type for hyperbolic curves”, *Math. Ann.* **372**:1-2 (2018), 369–428. MR Zbl
- [Beilinson 1989] A. A. Beilinson, “Polylogarithm and cyclotomic elements”, preprint, 1989.
- [Besser 2002] A. Besser, “Coleman integration using the Tannakian formalism”, *Math. Ann.* **322**:1 (2002), 19–48. MR Zbl

- [Besser 2012] A. Besser, “Heidelberg lectures on Coleman integration”, pp. 3–52 in *The arithmetic of fundamental groups* (Heidelberg, 2010), edited by J. Stix, *Contrib. Math. Comput. Sci.* **2**, Springer, 2012. MR Zbl
- [Besser and de Jeu 2008] A. Besser and R. de Jeu, “ $\text{Li}^{(p)}$ -service? An algorithm for computing p -adic polylogarithms”, *Math. Comp.* **77**:262 (2008), 1105–1134. MR Zbl
- [Bloch 2000] S. J. Bloch, *Higher regulators, algebraic K-theory, and zeta functions of elliptic curves*, CRM Monogr. Series **11**, Amer. Math. Soc., Providence, RI, 2000. MR Zbl
- [Bloch and Kato 1990] S. Bloch and K. Kato, “ L -functions and Tamagawa numbers of motives”, pp. 333–400 in *The Grothendieck Festschrift, I*, edited by P. Cartier et al., *Progr. Math.* **86**, Birkhäuser, Boston, 1990. MR Zbl
- [Borel 1953] A. Borel, “Sur la cohomologie des espaces fibrés principaux et des espaces homogènes de groupes de Lie compacts”, *Ann. of Math. (2)* **57** (1953), 115–207. MR Zbl
- [Borel 1977] A. Borel, “Cohomologie de SL_n et valeurs de fonctions zeta aux points entiers”, *Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4)* **4**:4 (1977), 613–636. MR Zbl
- [Brown 2012] F. C. S. Brown, “On the decomposition of motivic multiple zeta values”, pp. 31–58 in *Galois–Teichmüller theory and arithmetic geometry*, edited by H. Nakamura et al., *Adv. Stud. Pure Math.* **63**, Math. Soc. Japan, Tokyo, 2012. MR Zbl
- [Brown 2013] F. Brown, “Single-valued periods and multiple zeta values”, preprint, 2013. arXiv
- [Brown 2017] F. Brown, “Integral points on curves, the unit equation, and motivic periods”, preprint, 2017. arXiv
- [Chatzistamatiou 2017] A. Chatzistamatiou, “On integrality of p -adic iterated integrals”, *J. Algebra* **474** (2017), 240–270. MR Zbl
- [Chatzistamatiou and Ünver 2013] A. Chatzistamatiou and S. Ünver, “On p -adic periods for mixed Tate motives over a number field”, *Math. Res. Lett.* **20**:5 (2013), 825–844. MR Zbl
- [Corwin and Dan-Cohen 2018a] D. Corwin and I. Dan-Cohen, “The polylog quotient and the Goncharov quotient in computational Chabauty–Kim theory, I”, preprint, 2018. To appear in *International Journal of Number Theory*. arXiv
- [Corwin and Dan-Cohen 2018b] D. Corwin and I. Dan-Cohen, “The polylog quotient and the Goncharov quotient in computational Chabauty–Kim theory, II”, preprint, 2018. To appear in *Transactions of the American Mathematical Society*. arXiv
- [Dan-Cohen and Chatzistamatiou 2014] I. Dan-Cohen and A. Chatzistamatiou, “Computation of p -adic iterated integrals”, unpublished, 2014.
- [Dan-Cohen and Wewers 2015] I. Dan-Cohen and S. Wewers, “Explicit Chabauty–Kim theory for the thrice punctured line in depth 2”, *Proc. Lond. Math. Soc. (3)* **110**:1 (2015), 133–171. MR Zbl
- [Dan-Cohen and Wewers 2016] I. Dan-Cohen and S. Wewers, “Mixed Tate motives and the unit equation”, *Int. Math. Res. Not.* **2016**:17 (2016), 5291–5354. MR Zbl
- [Deligne 1989] P. Deligne, “Le groupe fondamental de la droite projective moins trois points”, pp. 79–297 in *Galois groups over \mathbb{Q}* (Berkeley, 1987), edited by Y. Ihara et al., *Math. Sci. Res. Inst. Publ.* **16**, Springer, 1989. MR Zbl
- [Deligne 2010] P. Deligne, “Le groupe fondamental unipotent motivique de $\mathbb{G}_m - \mu_N$, pour $N = 2, 3, 4, 6$ ou 8 ”, *Publ. Math. Inst. Hautes Études Sci.* **112** (2010), 101–141. MR Zbl
- [Deligne and Goncharov 2005] P. Deligne and A. B. Goncharov, “Groupes fondamentaux motiviques de Tate mixte”, *Ann. Sci. École Norm. Sup. (4)* **38**:1 (2005), 1–56. MR Zbl
- [Evertse and Györy 2015] J.-H. Evertse and K. Györy, *Unit equations in Diophantine number theory*, Cambridge Stud. Adv. Math. **146**, Cambridge Univ. Press, 2015. MR Zbl
- [Furusho 2004] H. Furusho, “ p -adic multiple zeta values, I: p -adic multiple polylogarithms and the p -adic KZ equation”, *Invent. Math.* **155**:2 (2004), 253–286. MR Zbl
- [Furusho 2007] H. Furusho, “ p -adic multiple zeta values, II: Tannakian interpretations”, *Amer. J. Math.* **129**:4 (2007), 1105–1144. MR Zbl
- [Goncharov 1994] A. B. Goncharov, “Polylogarithms and motivic Galois groups”, pp. 43–96 in *Motives* (Seattle, WA, 1991), edited by U. Jannsen et al., *Proc. Sympos. Pure Math.* **55**, Amer. Math. Soc., Providence, RI, 1994. MR
- [Goncharov 1995] A. B. Goncharov, “Polylogarithms in arithmetic and geometry”, pp. 374–387 in *Proc. Int. Congress of Math., I* (Zürich, 1994), edited by S. D. Chatterji, Birkhäuser, Basel, 1995. MR Zbl

- [Goncharov 2001] A. B. Goncharov, “Multiple polylogarithms and mixed Tate motives”, preprint, 2001. arXiv
- [Goncharov 2005] A. B. Goncharov, “Galois symmetries of fundamental groupoids and noncommutative geometry”, *Duke Math. J.* **128**:2 (2005), 209–284. MR Zbl
- [Jannsen 1989] U. Jannsen, “On the l -adic cohomology of varieties over number fields and its Galois cohomology”, pp. 315–360 in *Galois groups over \mathbb{Q}* (Berkeley, 1987), edited by Y. Ihara et al., Math. Sci. Res. Inst. Publ. **16**, Springer, 1989. MR Zbl
- [Jarossay 2016] D. Jarossay, “Pro-unipotent harmonic actions and a dynamical method for the computation of p -adic cyclotomic multiple zeta values”, preprint, 2016. arXiv
- [von Känel and Matschke 2016] R. von Känel and B. Matschke, “Solving S -unit, Mordell, Thue, Thue–Mahler and generalized Ramanujan–Nagell equations via Shimura–Taniyama conjecture”, preprint, 2016. arXiv
- [Kim 2005] M. Kim, “The motivic fundamental group of $\mathbb{P}^1 \setminus \{0, 1, \infty\}$ and the theorem of Siegel”, *Invent. Math.* **161**:3 (2005), 629–656. MR Zbl
- [Kim 2009] M. Kim, “The unipotent Albanese map and Selmer varieties for curves”, *Publ. Res. Inst. Math. Sci.* **45**:1 (2009), 89–133. MR Zbl
- [Kim 2012] M. Kim, “Tangential localization for Selmer varieties”, *Duke Math. J.* **161**:2 (2012), 173–199. MR Zbl
- [Perrin-Riou 1994] B. Perrin-Riou, “La fonction L p -adique de Kubota–Leopoldt”, pp. 65–93 in *Arithmetic geometry* (Tempe, AZ, 1993), edited by N. Childress and J. W. Jones, Contemp. Math. **174**, Amer. Math. Soc., Providence, RI, 1994. MR Zbl
- [Soulé 1981] C. Soulé, “On higher p -adic regulators”, pp. 372–401 in *Algebraic K-theory* (Evanston, IL, 1980), edited by E. M. Friedlander and M. R. Stein, Lecture Notes in Math. **854**, Springer, 1981. MR Zbl
- [Suslin 1987] A. A. Suslin, “Algebraic K -theory of fields”, pp. 222–244 in *Proc. Int. Congress of Math., I* (Berkeley, 1986), edited by A. M. Gleason, Amer. Math. Soc., Providence, RI, 1987. MR Zbl
- [Ünver 2019] S. Ünver, “Cyclotomic p -adic multi-zeta values”, *J. Pure Appl. Algebra* **223**:2 (2019), 489–503. MR Zbl
- [de Weger 1989] B. M. M. de Weger, *Algorithms for Diophantine equations*, CWI Tract **65**, Stichting Math. Centrum, Amsterdam, 1989. MR Zbl
- [Yamashita 2010] G. Yamashita, “Bounds for the dimensions of p -adic multiple L -value spaces”, *Doc. Math.* extra volume (2010), 687–723. MR Zbl
- [Zagier 1991] D. Zagier, “Polylogarithms, Dedekind zeta functions and the algebraic K -theory of fields”, pp. 391–430 in *Arithmetic algebraic geometry* (Texel, Netherlands, 1989), edited by G. van der Geer et al., Progr. Math. **89**, Birkhäuser, Boston, 1991. MR Zbl

Communicated by Bjorn Poonen

Received 2018-10-10 Revised 2019-09-16 Accepted 2019-11-27

ishaidc@gmail.com

Department of Mathematics, Ben Gurion University, Be'er Sheva, Israel

Algebra & Number Theory

msp.org/ant

EDITORS

MANAGING EDITOR

Bjorn Poonen
Massachusetts Institute of Technology
Cambridge, USA

EDITORIAL BOARD CHAIR

David Eisenbud
University of California
Berkeley, USA

BOARD OF EDITORS

Bhargav Bhatt	University of Michigan, USA	Martin Olsson	University of California, Berkeley, USA
Richard E. Borcherds	University of California, Berkeley, USA	Raman Parimala	Emory University, USA
Antoine Chambert-Loir	Université Paris-Diderot, France	Jonathan Pila	University of Oxford, UK
J-L. Colliot-Thélène	CNRS, Université Paris-Sud, France	Irena Peeva	Cornell University, USA
Brian D. Conrad	Stanford University, USA	Anand Pillay	University of Notre Dame, USA
Samit Dasgupta	Duke University, USA	Michael Rapoport	Universität Bonn, Germany
Hélène Esnault	Freie Universität Berlin, Germany	Victor Reiner	University of Minnesota, USA
Gavril Farkas	Humboldt Universität zu Berlin, Germany	Peter Sarnak	Princeton University, USA
Hubert Flenner	Ruhr-Universität, Germany	Michael Singer	North Carolina State University, USA
Sergey Fomin	University of Michigan, USA	Christopher Skinner	Princeton University, USA
Edward Frenkel	University of California, Berkeley, USA	Vasudevan Srinivas	Tata Inst. of Fund. Research, India
Wee Teck Gan	National University of Singapore	J. Toby Stafford	University of Michigan, USA
Andrew Granville	Université de Montréal, Canada	Shunsuke Takagi	University of Tokyo, Japan
Ben J. Green	University of Oxford, UK	Pham Huu Tiep	University of Arizona, USA
Joseph Gubeladze	San Francisco State University, USA	Ravi Vakil	Stanford University, USA
Christopher Hacon	University of Utah, USA	Michel van den Bergh	Hasselt University, Belgium
Roger Heath-Brown	Oxford University, UK	Akshay Venkatesh	Institute for Advanced Study, USA
János Kollár	Princeton University, USA	Marie-France Vignéras	Université Paris VII, France
Philippe Michel	École Polytechnique Fédérale de Lausanne	Melanie Matchett Wood	University of California, Berkeley, USA
Susan Montgomery	University of Southern California, USA	Shou-Wu Zhang	Princeton University, USA
Shigefumi Mori	RIMS, Kyoto University, Japan		

PRODUCTION

production@msp.org
Silvio Levy, Scientific Editor


See inside back cover or msp.org/ant for submission instructions.

The subscription price for 2020 is US \$415/year for the electronic version, and \$620/year (+\$60, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscriber address should be sent to MSP.

Algebra & Number Theory (ISSN 1944-7833 electronic, 1937-0652 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

ANT peer review and production are managed by EditFLOW® from MSP.

PUBLISHED BY

 **mathematical sciences publishers**
nonprofit scientific publishing

<http://msp.org/>

© 2020 Mathematical Sciences Publishers

Algebra & Number Theory

Volume 14 No. 5 2020

The universal family of semistable p -adic Galois representations URS HARTL and EUGEN HELLMANN	1055
On the group of purely inseparable points of an abelian variety defined over a function field of positive characteristic, II DAMIAN RÖSSLER	1123
Mixed Tate motives and the unit equation II ISHAI DAN-COHEN	1175
p -adic distribution of CM points and Hecke orbits I: Convergence towards the Gauss point SEBASTIÁN HERRERO, RICARDO MENARES and JUAN RIVERA-LETELIER	1239
Roots of L -functions of characters over function fields, generic linear independence and biases CORENTIN PERRET-GENTIL	1291



1937-0652(2020)14:5;1-X