THE POLYLOG QUOTIENT AND THE GONCHAROV QUOTIENT IN COMPUTATIONAL CHABAUTY-KIM THEORY II

ISHAI DAN-COHEN AND DAVID CORWIN

ABSTRACT. This is the second installment in a multi-part series starting with [CDC]. Building on Dan-Cohen–Wewers [DCW2], Dan-Cohen [DC], and Brown [Bro1], we push the computational boundary of our explicit motivic version of Kim's method in the case of the thrice punctured line over an open subscheme of Spec $\mathbb{Z}$. To do so, we develop a refined version of the algorithm of [DCW2] tailored specifically to this case. We also commit ourselves fully to working with the polylogarithmic quotient. This allows us to restrict our calculus with motivic iterated integrals to the so-called depth-one part of the mixed Tate Galois group studied extensively by Goncharov. An application was given in [CDC] where we verified Kim's conjecture in an interesting new case.

1. INTRODUCTION

Work by Dan-Cohen–Wewers [DCW1, DCW2] and by Dan-Cohen [DC] produced an algorithm, based on the Chabauty–Kim method, for computing the integral points of $\mathbb{P}^1\backslash\{0,1,\infty\}$ over open integer schemes whose halting was, and remains, conditional on deep conjectures by Kim and by Goncharov, among others.[1] This algorithm restricted attention to the polylogarithmic quotient of the unipotent fundamental

[1] Practical (and unconditional) methods for solving the S-unit equation predate this work, and can be found, for instance, in de Weger [dW] who uses the theory of logarithmic forms of Baker–Wüstholz [BW] (see also Everste–Győry [EG] for a general discussion). A more recent approach, due to Känel–Matchke [vKM] 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 to provide new numerical evidence for Kim's conjecture.

group $\pi_1^{\mathrm{un}}(X)$, but minimized its reliance on the polylogarithmic quotient with a view towards eventually constructing an algorithm for the full unipotent fundamental group. The resulting algorithm (to quote an anonymous referee) provides proof of concept. In terms of practical applications, however, it is quite unwieldy.

Francis Brown [Bro1] introduced various new techniques which he was able to use to construct functions for open subschemes of $\operatorname{Spec}\mathbb{Z}$ in several examples. His techniques capitalize on the relative simplicity of $\operatorname{Spec}\mathbb{Z}$ and of the polylogarithmic quotient, and inspired us to attempt to construct a simpler algorithm, and to continue to push the computational boundary, for open subschemes of $\operatorname{Spec}\mathbb{Z}$. Brown also suggested (in private communication) that we might be able to replace the full mixed Tate Galois group with a quotient tailored specifically to the polylogarithmic quotient of the unipotent fundamental group.

In part one of this series [CDC] (currently expected to have three parts), we worked out an example which goes beyond the examples of [DCW1, DCW2, DC]. This example displayed several new and interesting phenomena. It also helped us refine our methods, and led the way to the work presented here.

In this second installment, we present an algorithm based on the example considered in part I on the one hand, and based on Goncharov's investigations of the *depth-1* quotient [Gon1] on the other.[2] Let K be a number field and let Z be either $\operatorname{Spec}K$ (a "number scheme") or open in $\operatorname{Spec}\mathcal{O}_K$ (an "open integer scheme"). Associated to the *Goncharov quotient*, as we will call it (segment 2.3.2), is a Hopf subalgebra $A^G(Z)$ of the mixed Tate Hopf algebra $A(Z)$ of framed mixed Tate motives over Z. This subalgebra already contains the extension spaces

$$K_{2n-1}^{(n)}(Z) = \operatorname{Ext}_Z^1(\mathbb{Q}(0), \mathbb{Q}(n)) \subset A_n(Z),$$

and was studied extensively by Goncharov in connection with Zagier's conjecture relating special values of zeta functions of number fields to polylogarithms. This eventually led to his *depth filtration conjecture* [Gon2]; its depth-1 part says that $A^G(\operatorname{Spec}K)$ is generated by Goncharov's (unipotent) motivic polylogarithms $\operatorname{Li}_i^{\mathrm{u}}(x)$ (for $i \geqslant 1$ and x

---

[2] The remainder of the introduction presupposes some familiarity with the surrounding literature (on mixed Tate motives, the unipotent fundamental group, motivic iterated integrals, p-adic polylogarithms, Kim's method, and Kim's conjecture) as well as passing familiarity with the previously constructed algorithm of [DCW2, DC], and focuses on comparing old with new. The reader who is unfamiliar with this material may wish to skip forward to section 2 (where some of this background material is reviewed), or to go back to [DCW2] for a general introduction.

a K-point of $\mathbb{P}^1\backslash\{0, 1, \infty\}$). Although Zagier's conjecture, if stated in terms of values of zeta functions, is tautological for $\mathbb{Q}$, the *depth-1 conjecture* is still open even in this case. For our purposes we must refine this conjecture somewhat with respect to ramification. The resulting *integral depth-1 conjecture* (§2.3.6) for open subschemes of $\operatorname{Spec}\mathbb{Z}$ is based on a study of the *half-weight-2* part from [DCW1], and is of interest, we hope, in its own right. Indeed, we believe that an investigation of this conjecture and an attempt to generalize it to higher number fields (even in half-weight 2, where the case $Z = \operatorname{Spec} K$ is known and where the difference between $A(Z)$ and $A^G(Z)$ is not yet visible) may lead to near-term progress towards Goncharov's conjecture.

Focusing attention on the *Goncharov quotient* presents several simultaneous advantages. Most obviously, the dimensions of the graded pieces $A_n^G(Z)$ are far smaller than those of $A(Z)$. Correspondingly, if our integral depth-1 conjecture holds, our search through the vast collection of motivic iterated integrals for candidate basis elements may be limited to the comparatively small set of n-logarithms. In turn, working with n-logarithms allows us to avoid the complex combinatorics of the Goncharov coproduct formula [Gon2, Theorem 1.2]. Less obvious but perhaps equally important is that working with the Goncharov and polylogarithmic quotients allows us to make the geometry of the "geometric algorithm" (which computes the scheme theoretic image of the universal cocycle-evaluation map) fully explicit: we obtain a homomorphism of polynomial $\mathbb{Q}$-algebras given by an explicit family of polynomials about which we learned from Brown. As a result, our new algorithm is far simpler and more efficient than the algorithm of [DCW2]. It is therefore reasonable and worth-while to give a more explicit construction, with the promise of actual Sage code and ensuing numerical results (beyond those of [CDC]) in the near future.

While the Goncharov quotient holds much promise, it also presented us with a challenge. Unlike the full mixed Tate Galois group, the Goncharov quotient is not free, and so its coordinate ring $A^G(Z)$ is not a shuffle algebra. This threatened to send us looking through Goncharov's intricate analysis for information (actual or conjectural) about higher extension groups in the corresponding category of "Goncharov motives". Fortunately, as we discovered, by remembering the inclusion

$$A^G(Z) \subset A(Z)$$

and working sometimes in $A^G(Z)$ and sometimes in $A(Z)$, we can avoid direct confrontation with the structure of $A^G(Z)$.

A key observation for our work is that replacing the full mixed Tate Galois group of Z by its Goncharov quotient does not shrink the p-adic

analytic loci $X(\mathbb{Z}_p)_n \subset X(\mathbb{Z}_p)$ that our algorithm computes. Actually, our loci are potentially *larger* than those that intervene in Kim's conjecture [BDCKW]. One difference comes, of course, from considering only the polylogarithmic quotient of the unipotent fundamental group in place of the full unipotent fundamental group. The belief that we should nevertheless have equality

(*) $X(Z) = X(\mathbb{Z}_p)_n$ for n sufficiently large

has travelled down a somewhat bumpy road. Kim showed in [Kim1] that the loci $X(\mathbb{Z}_p)_n$ associated to the polylogarithmic quotient are finite for sufficiently large n and in [Kim2] that the same holds for open integer schemes associated to totally real number fields. Experts expressed the hope (if only tentatively and quietly) that the polylogarithmic quotient should be *big enough* for Kim's conjecture. However, upon completing our realization of the case $\mathbb{Z}[1/3]$ in [CDC], we discovered by computing numerically that $-1 \in X(\mathbb{Z}_p)_4$ in that case, and subsequently showed more generally that for $Z = \operatorname{Spec} \mathbb{Z}[1/q]$ (for any prime $q \neq p$), we have

$$-1 \in X(\mathbb{Z}_p)_n \qquad\qquad \text{for all } n.$$

This meant that (*) was in fact false as stated, since for $q \neq 2$, $X(\mathbb{Z}[1/q]) = \varnothing$ (so, in particular, does *not* contain -1). Nevertheless, we view this bump in the road as reflecting a particular interaction of the polylogarithmic quotient with roots of unity, or, at the very least, as a result of its symmetry-breaking nature. We may thus symmetrize our loci with respect to the S_3 action and, thus modified, expect property (*) to hold after all.

There is also a second, less obvious difference between Kim's loci and ours. This too intervened already in [DC]. While Kim's version may be defined in terms of the scheme-theoretic image of a p-adic realization map between nonabelian cohomology varieties over $\mathbb{Q}_p$, our algorithm computes the scheme theoretic image of the rationally-defined universal cocycle evaluation map, and only then pulls back the result to $\mathbb{Q}_p$. The result is again a possible enlargement of the resulting loci. However, as discussed in loc. cit., if the p-adic period conjecture holds, then there is no such enlargement after all. Period conjecture or no period conjecture, the final result is that our algorithm may be used to *verify* Kim's conjecture, but can have little bearing on any attempt to falsify the conjecture.

Because of its relative simplicity, we find it appropriate to describe the new algorithm in a somewhat more informal style than that of loc. cit., which we hope will make the present article more approachable.

A concrete case ("$\mathbb{Z}[1/3]$ in depth 4"), which provides new numerical evidence for Kim's conjecture, is worked out in [CDC]. Let us point out, however, that *that* work should not be viewed as merely executing the algorithm constructed in *this* work since the history is rather reversed: as the numbering suggests, the example worked out in [CDC] came first, and many of the ideas that went into constructing the present algorithm first developed in working out the example.

Acknowledgements. We would like to thank Bjorn Poonen and Herbert Gangl for their interest and encouragement. We would like to thank the referee for a careful reading and many helpful comments.

2. Conjectures and theorems

In this section, which doubles as a long introduction, we give precise statements of the conjectures on which our algorithm depends for halting. We also announce the success of our algorithm in computing the set of integral points and the conditional halting in a complementary pair of theorems (2.4.6) similar to the main theorems of [DC]. As promised, we begin by summarizing background material; details may be found in [DCW2, DC, CDC] and the references given there.

2.1. **Mixed Tate motives and mixed Tate Galois group.** Fix an open subscheme $Z \subset \operatorname{Spec} \mathbb{Z}$ and a prime $p \in Z$. Write

$$S := \operatorname{Spec} \mathbb{Z} \backslash Z = \{q_1, \ldots, q_s\}.$$

We let $K_m^{(n)}(Z)$ denote the n-eigenspace for the Adams operations on the rational Quillen K-group $K_m(Z) \otimes \mathbb{Q}$. Historically (due in large part to the work of Borel [Bor1, Bor2]), it was known that

$$K_{2n-1}^{(n)}(Z) = \begin{cases} \mathbb{Q}\langle \log^{\mathrm{u}}(q_1), \ldots, \log^{\mathrm{u}}(q_s)\rangle & n = 1, \\ \mathbb{Q}\zeta^{\mathrm{u}}(n) & n \text{ odd } \geqslant 3, \end{cases}$$

and that all other Adams pieces vanish. Here, $\log^{\mathrm{u}}(q_i)$ and $\zeta^{\mathrm{u}}(n)$ are certain special elements. Moreover, there were certain naturally defined p-adic regulator maps

$$\operatorname{reg} : K_{2n-1}^{(n)} \to \mathbb{Q}_p$$

and

$$\operatorname{reg}(\log^{\mathrm{u}}(q_i)) = \log^p(q_i)$$
$$\operatorname{reg}(\zeta^{\mathrm{u}}(n)) = \zeta^p(n),$$

the p-adic logarithm and zeta value respectively.

The p-adic zeta values $\zeta^p(n)$ (n odd $\geqslant 3$) are known to be nonzero for p regular. A small piece of the p-adic period conjecture asserts that

the same holds for all primes p. See Examples 2.19 and Remark 2.20 of Furusho [Fur] for a discussion of this and related conjectures.

2.1.1.   The theory of mixed Tate motives puts the K-groups above inside a big Hopf algebra. To define it, let $\mathbf{MT}(Z)$ denote the category of mixed Tate motives unramified over Z. The category $\mathbf{MT}(Z)$ is $\mathbb{Q}$-Tannakian; its simple objects up to isomorphism are precisely the tensor powers of $\mathbb{Q}(1)$. De Rham cohomology gives rise to a fiber functor

$$\mathrm{dR}^* : \mathbf{MT}(Z) \to \mathbf{Vect}\,\mathbb{Q}.$$

We have

$$\mathrm{Hom}(\mathbb{Q}(0), \mathbb{Q}(0)) = \mathbb{Q},$$
$$\mathrm{Ext}^1(\mathbb{Q}(0), \mathbb{Q}(n)) = K_{2n-1}^{(n)}(Z)$$

and all other Ext groups $\mathrm{Ext}^i(\mathbb{Q}(0), \mathbb{Q}(n))$ vanish. This means that $\mathbf{MT}(Z)$ is a *mixed Tate category*, and the results that follow are formal consequences of the axioms; see, for instance, Appendix A of Goncharov [Gon2].

There is a semi-direct product decomposition

$$\pi_1^{\mathrm{MT}}(Z) := \mathrm{Aut}^{\otimes}(\mathrm{dR}^*) = \pi_1^{\mathrm{un}}(Z) \rtimes \mathbb{G}_m$$

in which $\pi_1^{\mathrm{un}}(Z)$ is free prounipotent with abelianization

$$(*) \qquad \pi_1^{\mathrm{un}}(Z)^{\mathrm{ab}} = \bigoplus_{n \geqslant 1} \mathrm{Ext}^1(\mathbb{Q}(0), \mathbb{Q}(n))^{\vee},$$

and $A(Z) := \mathcal{O}(\pi_1^{\mathrm{un}}(Z))$ is a *shuffle algebra*: in terms of homogeneous generators

$$\tau_1, \ldots, \tau_s \qquad \text{and} \qquad \sigma_3, \sigma_5, \sigma_7, \ldots$$

(with τ_i in degree -1 and σ_i in degree $-i$) $A(Z)$ has vector space basis

$$\left\{ f_w \mid w \text{ a word in } \tau_1, \ldots, \tau_s, \sigma_3, \sigma_5, \ldots \right\}$$

called a "shuffle basis" on which the "shuffle" product is given by

$$f_{w'} f_{w''} = \sum_{\text{shuffles } w \text{ of } w', w''} f_w,$$

and the "deconcatenation" coproduct is given by

$$\Delta f_w = \sum_{w = w'w''} f_{w'} \otimes f_{w''}.$$

Equation (*) may be written dually as a family of exact sequences

$$(*^{\vee}) \qquad 0 \to \mathrm{Ext}^1(\mathbb{Q}(0), \mathbb{Q}(n)) \to A_n \xrightarrow{\Delta'} \bigoplus_{i+j=n\ i,j \geqslant 1} A_i \otimes A_j$$

where Δ' is the *reduced coproduct*:

$$\Delta'(a) = \Delta(a) - (1 \otimes a + a \otimes 1).$$

2.2. Unipotent fundamental group and motivic polylogarithms.

Let $X = \mathbb{P}^1_Z \backslash \{0, 1, \infty\}$. We use the tangent vector $\vec{1}_0$ as base point. We define $\pi_1^{\mathrm{un}}(X)$ to be the fundamental group $\mathrm{Aut}^{\otimes}(\omega_0)$ of the Tannakian category of unipotent connections on $X_\mathbb{Q}$ at the fiber functor associated to $\vec{1}_0$. Similarly, we define the path torsor associated to a point $x \in X(Z)$ by

$$\pi_1^{\mathrm{un}}(X, 0, x) := \mathrm{Isom}^{\otimes}(\omega_0, \omega_x).$$

According to Deligne [Del], $\pi_1^{\mathrm{un}}(X, 0, x)$ is canonically trivialized by a path ${}_x p_0^{\mathrm{dR}} \in \pi_1^{\mathrm{un}}(X, 0, x)(\mathbb{Q})$ (see [DCW2, §3.1.7] and the references given there). Moreover, $\pi_1^{\mathrm{un}}(X)$ is free prounipotent on two generators e_0, e_1 representing monodromy about 0 and 1, respectively. Consequently,

$$A(X) := \mathcal{O}(\pi_1^{\mathrm{un}}(X))$$

is a shuffle algebra on the shuffle basis e_0, e_1. Deligne–Goncharov [DG] (with subsequent different approaches, for instance, by Levine [Lev] and Dan-Cohen–Schlank [DCS]) construct a natural action of $\pi_1^{\mathrm{MT}}(Z)$ on $\pi_1^{\mathrm{un}}(X, 0, x)$.

Special elements $\mathrm{Li}_n^{\mathrm{u}}(x) \in A_n(Z)$ were constructed by Goncharov [DG]; these were called *motivic polylogarithms* in loc. cit. but are called *unipotent motivic polylogarithms* by Francis Brown [Bro2] to distinguish them from his somewhat different notion. (In fact the n-logarithms (or *polylogarithms*) $\mathrm{Li}_n^{\mathrm{u}}(x)$ form a special class among the more general *multiple polylogarithms*, which, in turn, are a special class of (unipotent motivic) iterated integrals defined and studied in [Gon2]). In the case of $Z \subset \mathrm{Spec}\,\mathbb{Z}$ (rather than more general integer schemes) these elements may be defined quite simply in terms of the action of $\pi_1^{\mathrm{MT}}(Z)$ on $\pi_1^{\mathrm{un}}(X, 0, x)$ and in terms of the special de Rham paths ${}_x p_0^{\mathrm{dR}}$, as we now recall.[3]

We abbreviate words in e_0, e_1 by writing words in 0 and 1, especially when these appear as subscripts. We let o denote the orbit map associated to the de Rham path ${}_x p_0^{\mathrm{dR}}$ and we let τ denote the trivialization of the path torsor $\pi_1^{\mathrm{un}}(X, 0, x)$ associated to the same path. Then $\mathrm{Li}_n^{\mathrm{u}}(x)$

---

[3] When $Z \subset \mathrm{Spec}\,\mathcal{O}_K$, K a number field bigger than $\mathbb{Q}$, the de Rham fiber functor is no longer $\mathbb{Q}$-rational. Instead, one must work with the *canonical* realization of the unipotent fundamental group, which thus loses its Tannakian interpretation in terms of connections. The ensuing construction of motivic polylogarithms, which is due to Goncharov, is more complicated.

is defined to be the composite map

$$(*) \qquad \pi_1^{\mathrm{un}}(Z) \xrightarrow{o} \pi_1^{\mathrm{un}}(X, 0, x) \xrightarrow[\tau]{\sim} \pi_1^{\mathrm{un}}(X) \xrightarrow{f_{10\cdots0}} \mathbb{A}^1$$

with $n - 1$ zeroes below the 'f'. (The intermediate map

$$\kappa(x) := \tau \circ o$$

is a $\mathbb{G}_m$-equivariant 1-cocycle and will play an important role below.) The unipotent logarithm is defined similarly by using the one-letter word '0' and satisfies

$$\mathrm{Li}_1^{\mathrm{u}}(x) = -\log^{\mathrm{u}}(1 - x).$$

The unipotent special zeta value $\zeta^{\mathrm{u}}(n)$ is defined (using the tangential end-point $-\vec{1}_1$ in place of x) by

$$\zeta^{\mathrm{u}}(n) := \mathrm{Li}_n^{\mathrm{u}}(-\vec{1}_1).$$

p-Adic integration gives rise to a ring homomorphism

$$\mathrm{per}_p : A(Z) \to \mathbb{Q}_p$$

which extends the regulator maps and

$$\mathrm{per}_p(\mathrm{Li}_n^{\mathrm{u}}(x)) = \mathrm{Li}_n^p(x)$$

is the p-adic n-logarithm of x.

2.3. **The polylog quotient and the Goncharov quotient.** The natural inclusion

$$X \hookrightarrow \mathbb{G}_m$$

gives rise to a map

$$\pi_1^{\mathrm{un}}(X) \to \pi_1^{\mathrm{un}}(\mathbb{G}_m) = \mathbb{Q}(1).$$

Let N be the kernel. The polylog quotient is defined as

$$\pi^{\mathrm{PL}}(X) := \pi_1^{\mathrm{un}}(X)/[N, N].$$

Let $\mathfrak{n}^{\mathrm{PL}}(X) := \mathrm{Lie}\,\pi^{\mathrm{PL}}(X)$. According to Proposition 16.13 of Deligne [Del], $\mathfrak{n}^{\mathrm{PL}}(X)$ is a sum of Tate motives. Hence $\pi_1^{\mathrm{un}}(Z)$ acts trivially on $\pi^{\mathrm{PL}}(X)$. Consequently, the projection $\kappa^{\mathrm{PL}}(x)$ of the cocycle $\kappa(x)$ (associated to $x \in X(Z)$) to $\pi^{\mathrm{PL}}(X)$ is simply a $\mathbb{G}_m$-equivariant homomorphism

$$\pi_1^{\mathrm{un}}(Z) \to \pi^{\mathrm{PL}}(X).$$

Lemma 2.3.1. The functions f_0 and $f_1, f_{10}, f_{100}, \ldots$ on $\pi_1^{\mathrm{un}}(X)$ factor through $\pi^{\mathrm{PL}}(X)$ and form a set of homogeneous coordinates on the latter.

Proof. After forgetting the $\pi_1^{\mathrm{un}}(Z)$ action, $\mathfrak{n}(X)$ is just the free pronilpotent Lie algebra on generators e_0, e_1, and the ideal associated to N is generated by e_1. So this is purely formal. $\square$

We will denote the function f_0 on $\pi^{\mathrm{PL}}(X)$ by $\log^{\mathrm{u}}$ and the function $f_{10\cdots0}$ with $(n-1)$ zeroes by $\mathrm{Li}_n^{\mathrm{u}}$.

2.3.2.   Let $\mathfrak{n} = \mathfrak{n}(Z) = \mathrm{Lie}\,\pi_1^{\mathrm{un}}(Z)$. We define the *Goncharov quotient* by

$$\mathfrak{n}^G(Z) := \mathfrak{n}/[\mathfrak{n}_{\leqslant -2}, \mathfrak{n}_{\leqslant -2}].$$

We also consider the associated quotient $\pi^G(Z)$ of $\pi_1^{\mathrm{un}}(Z)$ and the associated Hopf subalgebra

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

Lemma 2.3.3. Every $\mathbb{G}_m$-equivariant homomorphism

$$\pi_1^{\mathrm{un}}(Z) \to \pi^{\mathrm{PL}}(X)$$

factors through $\pi^G(Z)$.

Proof. Any degree zero graded homomorphism

$$\mathfrak{n}(Z) \to \mathfrak{n}^{\mathrm{PL}}(X)$$

must send $\mathfrak{n}(Z)_{\leqslant -2}$ to $\mathfrak{n}^{\mathrm{PL}}(X)_{\leqslant -2}$. But

$$\left[\mathfrak{n}^{\mathrm{PL}}(X)_{\leqslant -2}, \mathfrak{n}^{\mathrm{PL}}(X)_{\leqslant -2}\right] = 0.\qquad\square$$

Proposition 2.3.4. The unipotent motivic polylogarithmic values $\mathrm{Li}_i^{\mathrm{u}}(x)$ $(x \in X(Z))$ belong to $A^G(Z)$.

Proof. Returning to 2.2(*), we saw in lemma 2.3.1 that the function $f_{10\cdots0}$ factors through $\pi^{\mathrm{PL}}(X)$, and we saw in lemma 2.3.3 that the cocycle $\kappa^{\mathrm{PL}}(x)$ factors through $\pi^G(Z)$. $\square$

Proposition 2.3.5. The map

$$Z^1(\pi_1^{\mathrm{un}}(Z), \pi^{\mathrm{PL}}(X))^{\mathbb{G}_m} \leftarrow Z^1(\pi^G(Z), \pi^{\mathrm{PL}}(X))^{\mathbb{G}_m}$$

induced by pulling back a $\mathbb{G}_m$-equivariant cocycle along the projection

$$\pi_1(Z) \twoheadrightarrow \pi^G(Z)$$

is bijective. In particular (given that we're working with the polylogarithmic quotient of $\pi_1^{\mathrm{un}}(X)$), replacing the full mixed Tate Galois group $\pi_1^{\mathrm{un}}(Z)$ by its Goncharov quotient will have no further effect on the resulting loci $X(\mathbb{Z}_p)_n$.

Proof. Direct consequence of lemma 2.3.3. $\square$

We consider the following strengthening of the depth-1 part of Goncharov's depth filtration conjecture [Gon2]. For any prime q, let

$$Z_{>q} = \operatorname{Spec}\mathbb{Z}\backslash\{\text{primes} \leqslant q\}.$$

For any graded algebra A, we let $A_{[\leqslant n]}$ denote the subalgebra generated by elements of degree $\leqslant n$.

Conjecture 2.3.6 (Integral depth-1 conjecture). For every prime q_s and every $n \in \mathbb{N}$, there exists a $q_M \geqslant q_s$ such that $A^G_{[\leqslant n]}(Z_{>q_M})$ is generated as a $\mathbb{Q}$-algebra by the elements $\log^{\mathrm{u}}(q')$ for q' prime $\leqslant q_M$, the elements $\zeta^{\mathrm{u}}(n)$ for n odd $\geqslant 3$ and the elements $\operatorname{Li}^{\mathrm{u}}_i(a)$ for $n \geqslant i \geqslant 2$ and $a \in X(Z_{>q_M})$.

2.3.7. As an example, $A^G(\operatorname{Spec}\mathbb{Z})$ is spanned by $\zeta^{\mathrm{u}}(n)$ for n odd $\geqslant 3$, so the integral depth-1 conjecture holds for $\operatorname{Spec}\mathbb{Z}$.

2.3.8. *Remark.* Let us put this conjecture in context with a brief preview of things to come. In section 4 below we construct an algorithm that takes a natural number n and a prime number q_s as input, and that upon halting outputs two primes $q_s \leqslant q_M < p$ and a family of points $a_{i,j} \in X(Z_{>q_M})$, such that

   (1) if the algorithm halts then $\{\operatorname{Li}^{\mathrm{u}}_i(a_{i,j})\}_{i,j}$ forms an algebra basis of $A^G(Z_{>q_M})$ in half-weights $\leqslant n$, and
   (2) if conjecture 2.3.6 holds, then the algorithm halts.

We emphasize that while the halting is conditional, the validity of the output is unconditional. In particular, our algorithm may be used to verify the conjecture experimentally up to any given bound on the weight. Our choice to work with open subschemes of Z of the form $Z_{>q_M}$ (instead of searching through all open subschemes, as we do in [DC]) means that the scope of our search, as we attempt to construct a basis, is smaller. It has the disadvantage, however, that we may have to increase the auxiliary prime p.

2.3.9. *Remark.* Let us further explain the role played by the scheme $Z_{>q_M}$ in our point-counting algorithm. For general Z, $A^G(Z)$ may not be generated by polylogarithms $\operatorname{Li}^{\mathrm{u}}_i(a)$ with $a \in X(Z)$. For example, if $Z = \operatorname{Spec}\mathbb{Z}[1/q]$ for q a prime $\neq 2$ then

$$A^G(\mathbb{Z}) \neq A^G(\mathbb{Z}[1/q])$$

(and $A^G(\mathbb{Z}[1/q])$ is not even generated over $A^G(\mathbb{Z})$ by $\log^{\mathrm{u}}(q)$) but

$$X(Z) = \varnothing.$$

Moreover, we have no direct way of deciding if a given rational linear combination of $\mathrm{Li}_n^{\mathrm{u}}(a)$'s ($a \in X(\mathbb{Q})$) is unramified over Z (i.e. is contained in $A(Z)$). Our method, present already in a more general (but less precise) form in [DC], is rather indirect. We first *taper* Z down to a $Z_{>q_M}$. We then construct a polylogarithmic basis of $A^G(Z_{>q_M})$ (up to a given weight). If we insist that our basis be compatible with the extension spaces, we may then generate an associated shuffle basis. We then construct a change-of-basis matrix which relates our polylogarithmic basis to our shuffle basis. Finally, we use our shuffle basis to identify the subspace $A^G(Z) \subset A^G(Z_{>q_M})$.[4]

2.3.10. *Further to remark 2.3.9.* Actually, since our change of basis matrix is only a p-adic approximation, we can only identify the subspace $A^G(Z)$ inside $A^G(Z_{>q_M})$ up to given p-adic precision. This means that, for all we know, the polylogarithmic basis we construct may only be a linearly independent set of the right size, p-adically close to $A^G(Z)$. This issue may be dealt with roughly as follows. We make sure that our basis elements are sufficiently spread out (modifying if necessary) to ensure that their projection onto $A^G(Z)$ remains linearly independent. We refer to the resulting basis as our "abstract basis" since its definition is not constructive. We subsequently carry out all computations for both the abstract and the ("concrete") polylogarithmic basis, keeping track of the accumulated error.

Issues of this sort were already treated quite carefully in [DC], which is consequently littered with double-tildes. Here we limit ourselves to mentioning these issues only in passing, since they tend to cloud the exposition and obscure the essential features of our construction. Rather, we feel that these issues are best relegated to a future computational article in which the algorithm presented here is given in a sort of paragraph-style pseudo code, divorced entirely from its theoretical backdrop. *That* article, we hope, will come along with Sage code and a wealth of numerical results. In the meantime, in working out small-scale examples with a human touch (as we did in [CDC]), these issues can usually be circumvented by replacing p-adic approximations of relations between values of polylogarithms by actual known relations found in the literature about polylogarithms.[5]

---

[4] However, there's a caveat, which is why there's a further remark, which should be thought of as being in smaller print.

[5] But here again there is a caveat, which is why there's yet another remark, in an even smaller font.

2.3.11. *Further to remark 2.3.10.* Actually, this particular issue was dealt with differently in [DC]. There, we completely avoided construct-ing a basis of $A(Z)$. Instead, after finding an open subscheme $Z^o \subset Z$ (which plays the role played by our $Z_{>q_M}$) and a basis of $A(Z^o)$, we modified the universal evaluation map to allow coefficients in the larger $A(Z^o)$. This meant that the difference between $A(Z)$ and $A(Z^o)$ was dealt with within the *geometric algorithm.* However, as we noticed during our work on [CDC], this made our algorithm quite inefficient in cases of interest. For instance, it meant that the geometric algorithm for the case $Z = \operatorname{Spec} \mathbb{Z}[1/q]$ must grow with q.

A different issue, which comes up only for larger number fields, was, however, dealt with in a manner similar to that indicated in remark 2.3.10. When a basis for the extension spaces is not known, we are un-able to construct one algorithmically. Instead, we construct a linearly independent set p-adically close to the extension space in question and proceed as indicated above.

2.4. **Application to integral points.** Let $I_{\mathrm{BC}} = \mathrm{per}^\sharp$ denote the map

$$\operatorname{Spec} \mathbb{Q}_p \to \pi_1^{\mathrm{un}}(Z)$$

induced by the period map (since it is essentially given by *Besser-Coleman Integration*). Let $\pi_{\geq -n}^{\mathrm{PL}}(X)$ denote the quotient by the nth step of the descending central series. As explained in the proof of Proposition 2 of Kim [Kim1], the functor from $\mathbb{Q}$-algebras to sets

$$R \mapsto Z^1(\pi^G(Z)_R, \pi_{\geq -n}^{\mathrm{PL}}(X)_R)^{\mathbb{G}_m} = \operatorname{Hom}^{\mathbb{G}_m}(\pi^G(Z)_R, \pi_{\geq -n}^{\mathrm{PL}}(X)_R)$$

of $\mathbb{G}_m$-equivariant cocycles, is represented by an affine space

$$\mathbf{Z}^1(\pi^G(Z), \pi_{\geq -n}^{\mathrm{PL}}(X))^{\mathbb{G}_m}$$

over $\mathbb{Q}$.[6] Let $\mathfrak{ev}^G$ denote the universal evaluation map

$$\pi^G(Z) \times \mathbf{Z}^1\big(\pi^G(Z), \pi_{\geq -n}^{\mathrm{PL}}(X)\big)^{\mathbb{G}_m} \to \pi^G(Z) \times \pi_{\geq -n}^{\mathrm{PL}}(X)$$

$$\mathfrak{ev}^G(\gamma, \phi) = (\gamma, \phi(\gamma)).$$

2.4.1.   Upon taking $\mathbb{Q}_p$-points (as $\mathbb{Q}$-schemes), the evaluation map fits into a commuting square

$$\begin{array}{ccc} X(Z) & \longrightarrow & X(\mathbb{Z}_p) \\ {\scriptstyle \kappa}\downarrow & & \downarrow{\scriptstyle \beta} \\ \Big(\pi^G(Z) \times \mathbf{Z}^1\big(\pi^G(Z), \pi_{\geq -n}^{\mathrm{PL}}(X)\big)^{\mathbb{G}_m}\Big)(\mathbb{Q}_p) & \xrightarrow{\mathfrak{ev}^G} & \Big(\pi^G(Z) \times \pi_{\geq -n}^{\mathrm{PL}}(X)\Big)(\mathbb{Q}_p) \end{array}$$

---

[6] A particularly concrete construction of the isomorphism to affine space is given in [CDC, Corollary 3.11] and indicated in remark 7.4 below.

sending

$$
\begin{array}{c}
x \\
\Big\downarrow {\scriptstyle \kappa} \\
\Big(I_{\mathrm{BC}}, \kappa(x)\Big) \xmapsto{\;\mathfrak{ev}^G\;} \left(I_{\mathrm{BC}}, \begin{pmatrix} \log^p(x) \\ \mathrm{Li}_1^p(x) \\ \mathrm{Li}_2^p(x) \\ \vdots \end{pmatrix}\right)
\end{array}
\qquad
\begin{array}{c}
y \\
\Big\downarrow {\scriptstyle \beta} \\
\left(I_{\mathrm{BC}}, \begin{pmatrix} \log^p(y) \\ \mathrm{Li}_1^p(y) \\ \mathrm{Li}_2^p(y) \\ \vdots \end{pmatrix}\right)
\end{array}
$$

which constitutes our computable cousin of "Kim's cutter".[7]

2.4.2. For us, the *polylogarithmic Chabauty-Kim locus* $X(\mathbb{Z}_p)_n$ is a locally analytic (or "Coleman analytic") subspace of $X(\mathbb{Z}_p)$. To define it, we take the scheme theoretic image of $\mathfrak{ev}^G$, we pull back along β, and finally we symmetrize with respect to the S_3 action. This last step means that we close the set of generators under the two operations $F(z) \mapsto$

(*) $F(1-z),$ and $F\left(\dfrac{1}{z}\right).$

We also consider $X(Z)$ as a locally analytic subspace of $X(\mathbb{Z}_p)$ with reduced structure.[8]

Conjecture 2.4.3 (Convergence of polylogarithmic loci)**.** Let Z be an open subscheme of $\mathrm{Spec}\,\mathbb{Z}$ and let p be a closed point of Z. Then for n sufficiently large we have an equality of locally analytic subspaces of $X(\mathbb{Z}_p)$

$$X(Z) = X(\mathbb{Z}_p)_n.$$

(In particular, for such n, the points of $X(Z)$ are not double roots of the nth Chabauty-Kim ideal.)

2.4.4. *Remark.* In segment 8.3 below, we complete the construction of an algorithm which upon halting computes the locus $X(\mathbb{Z}_p)_n$ to given precision; this is our *loci algorithm*. This algorithm proceeds in several steps. In one of these, which we refer to as the *geometric algorithm* (§7), we compute the scheme theoretic image of the map $\mathfrak{ev}^G$ with respect to coordinates induced by a shuffle basis for $A(Z)$. In a second step, we use the change of basis matrix constructed in the *change of basis algorithm* (§5) to convert the resulting equations into equations in coordinates associated to the polylogarithmic basis constructed in our *basis algorithm* (§4). The remaining steps amount to a straightforward application of *Lip service* [BdJ]. Pulling back along β merely means replacing unipotent motivic polylogarithms by p-adic

---

[7] We recall that the commutativity is a rather long story which, at least in one possible approach, starts with Olsson's nonabelian p-adic Hodge theory; see [DCW2].

[8] In [CDC] we use the notation $X(\mathbb{Z}_p)_n^{S_3}$ to distinguish this locus from the *un*-symmetrized version considered previously.

polylogarithms. The symmetrization was spelled out in 2.4.2(*). Finally, the algorithm of loc. cit. allows us to obtain local power series expansions to given p-adic and geometric precision.

2.4.5. *Remark.* In terms of the *loci algorithm* our *point counting algorithm* from [DC] remains unchanged. We review its construction in segment 9 below, referring back to [DC] for details. In terms of the conjectures above and the algorithm below, our point-counting theorem (which may equally be called a point-*finding* theorem) is as follows. If Z is an open subscheme of $\operatorname{Spec}\mathbb{Z}$ in which the largest prime *excluded* is q_M, we refer to $Z_{>q_M}$ as *the tapered scheme associated to Z*.

Theorem 2.4.6 (Point-counting)**.** Let Z be an open subscheme of $\operatorname{Spec}\mathbb{Z}$.
  (1) If the point-counting algorithm halts for the input Z, then its output is equal to $X(Z)$.
  (2) Assume the conjectured nonvanishing of the p-adic zeta values $\zeta^p(k)$ (k odd $\geqslant 3$). If the integral depth-1 conjecture (2.3.6) holds for the tapered scheme associated to Z, and if convergence of polylogarithmic loci (2.4.3) holds for Z, then the point-counting algorithm halts for the input Z.

Unlike in [DC], here we do not separate the proof of the *point-counting theorem* from the construction of the *point-counting algorithm*. Rather, we set ourselves the task of computing the data to be computed, and explain in down to earth terms, how we go about computing algorithmically. Thus, we consider the theorem to be proved as soon as the algorithm has been constructed. This task occupies the remainder of the article.

3. Setup

3.1. We continue to work with an open subscheme Z of $\operatorname{Spec}\mathbb{Z}$ and a prime $p \in \mathbb{Z}$. Recall that $\pi_1^{\mathrm{un}}(Z)$ denotes the unipotent part of the fundamental group of mixed Tate motives unramified over Z and $\mathfrak{n}(Z)$ denotes its Lie algebra, which has a natural grading — we call the graded degree of a homogeneous element its *half-weight*. Recall that $\mathfrak{n}^G(Z)$ denotes the Goncharov quotient of $\mathfrak{n}(Z)$ and that

$$\pi^G(Z) = \exp\mathfrak{n}^G(Z)$$

denotes the associated quotient of $\pi_1^{\mathrm{un}}(Z)$. Recall that $A(Z) = \mathcal{O}(\pi_1^{\mathrm{un}}(Z))$ denotes the graded Hopf algebra of functions on $\pi_1^{\mathrm{un}}(Z)$, and that $A^G(Z)$ denotes the subalgebra associated to $\pi^G(Z)$.

Let

$$d_i = \dim_{\mathbb{Q}}\mathfrak{n}^G(Z)_i.$$

Let $D_n^G(Z)$ denote the image of the product map

$$\bigoplus_{i+j=n,\ i,j\geqslant 1} A_i^G \otimes A_j^G \to A_n^G.$$

The Lie coalgebra $L^G := (\mathfrak{n}^G)^\vee$ is equal to the quotient
$$L^G = A^G_{>0}/D^G = A^G_{>0}/(A^G_{>0})^2$$
of the augmentation ideal by its square.

Recall that $\mathcal{U}(Z) = A(Z)^\vee$ denotes the completed universal enveloping algebra of $\pi_1^{\mathrm{un}}(Z)$ and, adding the decoration 'G' as usual, $\mathcal{U}^G(Z) = A^G(Z)^\vee$ denotes the completed universal enveloping algebra of $\pi^G(Z)$.

Proposition 3.2. Any set of homogeneous elements of $A^G_{>0}$ which maps to a basis of L^G forms an algebra basis for A^G.

Proof. After forgetting the counit and comultiplication, A^G has the structure of a graded free $\mathbb{Q}$-algebra
$$A^G = \mathbb{Q}[S]$$
with $S = \bigcup_{i=1}^\infty$ and S_i finite for each i. This is simply because A^G is the coordinate ring of a prounipotent group with $\mathbb{G}_m$-action such that the graded pieces of the abelianization are finite dimensional. Let $I = A^G_{>0}$ denote the ideal of $\mathbb{Q}[S]$ of positively graded elements.

Let
$$S' = \bigcup_{i=1}^\infty S'_i$$
be a set of homogeneous elements of $A^G_{>0}$ which maps to a basis of $L^G = I/I^2$ and let I' be the ideal of positively graded elements in $\mathbb{Q}[S']$. Then the induced map of $\mathbb{Q}$-algebras
$$\phi : \mathbb{Q}[S'] \to \mathbb{Q}[S]$$
preserves the grading and induces an isomorphism $I'/I'^2 \to I/I^2$. Hence by [DC, 3.1.1], ϕ is an isomorphism. $\qquad\square$

3.3. **Remark.** Recall from §2.1 that the kernel $E_n = E_n(Z)$ of the reduced coproduct on $A(Z)_n$ is canonically isomorphic to the space
$$\mathrm{Ext}^1_Z(\mathbb{Q}(0), \mathbb{Q}(n))$$
of extensions in mixed Tate motives over Z. Similarly, the kernel $E_n^G = E_n^G(Z)$ of the reduced coproduct on $A_n^G(Z)$ is equal to a space of extensions in the full subcategory of the category of mixed Tate motives consisting of objects whose associated representation factors through the Goncharov quotient. We will refer to such objects as "Goncharov motives".

It follows directly from the definition however, that we have an equality of spaces of extensions $E_n^G = E_n$; in the case at hand, both are spanned by logarithms and by the motivic zeta elements $\zeta^{\mathrm{u}}(n)$ for n odd. Consequently, the category of Goncharov motives must have nontrivial higher extension groups. This complicates the structure of the Hopf algebra A^G. As mentioned in the introduction, instead of analyzing its structure, we will work inside of A.

Let q_M denote a prime sufficiently large compared to q_s and n, and let $Z_{>q_M}$ denote the subscheme of $\operatorname{Spec}\mathbb{Z}$ obtained by removing all primes $\leqslant q_M$ as above. After constructing a polylogarithmic algebra basis $\mathcal{B}^G$ for $A^G(Z_{>q_M})$ (which includes the zeta elements) in half-weights $\leqslant n$, we will extend our basis arbitrarily to an algebra basis $\mathcal{B}$ of $A(Z_{>q_M})$. We will then define the generators σ_r, r odd $\geqslant 3$, to be dual to the zeta elements relative to the given choice of basis. We will then have according to proposition 3.2.3 of [DC],

$$\mathcal{U}(Z_{>q_M}) = \mathbb{Q}\langle\!\langle \{\tau_q\}_{q\leqslant q_M}, \{\sigma_r\}_{r \text{ odd }\geqslant 3}\rangle\!\rangle$$

but with the σ_r well defined only in the quotient

$$\mathcal{U} \twoheadrightarrow \mathcal{U}^G.$$

3.4. Returning to $X = \mathbb{P}^1\backslash\{0, 1, \infty\}$, we recall that $\pi_1^{\mathrm{un}}(X)$ denotes the unipotent fundamental group at the tangent vector $\vec{1}_0$, and that $\pi^{\mathrm{PL}}(X)$ denotes its polylogarithmic quotient. We recall that the polylogarithmic quotient has canonical coordinates, which we denote by $\log^{\mathrm{u}}, \operatorname{Li}_1^{\mathrm{u}}, \operatorname{Li}_2^{\mathrm{u}}, \ldots$, so that

$$\mathcal{O}(\pi^{\mathrm{PL}}(X)) = \mathbb{Q}[\log^{\mathrm{u}}, \operatorname{Li}_1^{\mathrm{u}}, \operatorname{Li}_2^{\mathrm{u}}, \ldots]$$

with $\log^{\mathrm{u}}$ in degree 1 and $\operatorname{Li}_i^{\mathrm{u}}$ in degree i. Recall that in §2.2 we associated to a Z-valued base-point a of X a 1-cocycle

$$\kappa(a) : \pi_1^{\mathrm{un}}(Z) \to \pi^{\mathrm{PL}}(X)$$

and defined the (unipotent) motivic n-logarithm of a by

$$\operatorname{Li}_n^{\mathrm{u}}(a) := \kappa(a)^\sharp(\operatorname{Li}_n^{\mathrm{u}}).$$

More generally, if R is a $\mathbb{Q}$-algebra and

$$c : \pi_1^{\mathrm{un}}(Z)_R \to \pi^{\mathrm{PL}}(X)_R$$

is a family of cocycles parametrized by $\operatorname{Spec} R$, we set

$$\operatorname{Li}_n^{\mathrm{u}}(c) := c^\sharp(\operatorname{Li}_n^{\mathrm{u}}),$$

an element of $A(Z) \otimes R$. Similarly, we set

$$\log^{\mathrm{u}}(c) := c^\sharp(\log^{\mathrm{u}}).$$

Proposition 3.5. We denote the reduced coproduct by Δ'. We have

$$\Delta' \operatorname{Li}_n^{\mathrm{u}} = \sum_{i=1}^{n-1} \frac{(\log^{\mathrm{u}})^i}{i!} \otimes \operatorname{Li}_{n-i}^{\mathrm{u}}.$$

Proof. In view of the formula

$$(\operatorname{Li}_{e_0}^{\mathrm{u}})^m = m! \operatorname{Li}_{(e_0)^m}^{\mathrm{u}},$$

this is just the deconcatenation coproduct of shuffle coordinates on a free prounipotent group. $\qquad\square$

Corollary 3.6. A similar formula holds for $\Delta' \operatorname{Li}_n^{\mathrm{u}}(c)$ for any cocycle c:

$$\Delta' \operatorname{Li}_n^{\mathrm{u}}(c) = \sum_{i=1}^{n-1} \frac{(\log^{\mathrm{u}}(c))^i}{i!} \otimes \operatorname{Li}_{n-i}^{\mathrm{u}}(c),$$

as well as for $\Delta' \operatorname{Li}_n^{\mathrm{u}}(z)$ for any $z \in X(Z)$.

Proof. Since $\pi_1^{\mathrm{un}}(Z)$ acts trivially on $\pi^{\mathrm{PL}}(X)$, a cocycle

$$c : \pi_1^{\mathrm{un}}(Z) \to \pi^{\mathrm{PL}}(X)$$

is simply a group homomorphism. This means $c^\sharp$ preserves coproducts. Hence,

$$\begin{aligned}
\Delta' \operatorname{Li}_n^{\mathrm{u}}(c) &= \Delta' c^\sharp \operatorname{Li}_n^{\mathrm{u}} \\
&= (c^\sharp \otimes c^\sharp)(\Delta' \operatorname{Li}_n^{\mathrm{u}}) \\
&= (c^\sharp \otimes c^\sharp) \left(\sum_{i=1}^{n-1} \frac{(\log^{\mathrm{u}})^i}{i!} \otimes \operatorname{Li}_{n-i}^{\mathrm{u}} \right) \\
&= \sum_{i=1}^{n-1} \frac{(\log^{\mathrm{u}}(c))^i}{i!} \otimes \operatorname{Li}_{n-i}^{\mathrm{u}}(c).
\end{aligned}$$

$\square$

3.7. Remark. Corollary 3.6 may be upgraded in (at least) four different ways: (1) by replacing c by a cocycle $\pi_1^{\mathrm{un}}(Z) \to \pi_1^{\mathrm{un}}(X, x)$ which is no longer a homomorphism, (2) by further puncturing X at a finite number of rational points, (3) by replacing $\operatorname{Li}_n^{\mathrm{u}}$ by the function $\pi_1^{\mathrm{un}}(X, x) \to \mathbb{A}_{\mathbb{Q}}^1$ associated to an arbitrary word in a basis of $H_1^{\mathrm{dR}}(X)$, and (4) by replacing $\mathbb{Q}$ by a general number field. The result (at least when c comes from a rational point y) is Theorem 1.2 of Goncharov [Gon2], which has come to be known as the *Goncharov coproduct formula*. As we mentioned in the introduction, one advantage of working with n-logarithms is that we can make do with the much simpler formula of Corollary 3.6.

3.8. Fix arbitrarily a set

$$\Sigma = \bigcup_{i \leqslant -1} \Sigma_i$$

of homogeneous free generators for $\mathfrak{n}(Z)$. Any word w in the generators is naturally an element of the completed universal enveloping algebra $\mathcal{U}(Z)$. We denote the natural pairing

$$A(Z) \otimes_{\mathbb{Q}} \mathcal{U}(Z) \to \mathbb{Q}$$

by $\langle -, - \rangle$, and the same after base-change to any $\mathbb{Q}$-algebra R.

Proposition 3.9. Continuing with the situation and the notation of segments 3.4, 3.8, fix natural numbers $0 \leqslant r < n$ and elements $\tau_1, \ldots, \tau_r \in \Sigma_{-1}$, and $\sigma \in \Sigma_{r-n}$. We then have

$$\langle \operatorname{Li}_n^{\mathrm{u}}(c), \sigma \tau_1 \cdots \tau_r \rangle = \langle \operatorname{Li}_r^{\mathrm{u}}(c), \sigma \rangle \langle \log^{\mathrm{u}}(c), \tau_1 \rangle \cdots \langle \log^{\mathrm{u}}(c), \tau_r \rangle$$

and all other values $\langle \mathrm{Li}_n^{\mathrm{u}}(c), w \rangle$ (w a word in Σ) vanish.

Proof. This formula appeared in a letter written by Francis Brown to I. Dan-Cohen and is proved in [CDC, Proposition 3.10]. $\square$

3.10. **Definition.** Let k be a field with an absolute value. We say that vectors
$$v_1, \ldots, v_d \in k^n$$
are ϵ-*linearly independent* if there exists a $d \times d$ minor whose determinant has absolute value $> \epsilon$.

3.11. **Proposition.** Let k be a field with an absolute value $|\cdot|$ and $\tilde{v}_1, \ldots, \tilde{v}_d$ vectors in k^n which are ϵ-*linearly independent*. Then there exists a number $\epsilon' > 0$, algorithmically computable from the data $(\epsilon, \tilde{v}_1, \ldots, \tilde{v}_d)$, which goes to 0 as $\epsilon \to 0$, and such that for any family $v_1, \ldots, v_d$ of vectors in k^n, if
$$|v_i - \tilde{v}_i| < \epsilon'$$
for each $i = 1, \ldots, d$, then the vectors $v_1, \ldots, v_d$ are linearly independent.

Proof. The proof reduces to the case $d = n$, to which we now restrict attention. The algorithmic computability will remain implicit. Given $v = (v_1, \ldots, v_d)$, $\tilde{v} = (\tilde{v}_1, \ldots, \tilde{v}_d)$ as in the proposition, we can bound
$$|\det v - \det \tilde{v}|$$
by a positive number δ which depends only on ϵ' and on $\tilde{v}_1, \ldots, \tilde{v}_d$, and decreases monotone to 0 as $\epsilon' \to 0$. We outline the construction. For each $i = 1, \ldots, n$, we let Δ_i denote the norm of the linear functional
$$\det(\tilde{v}_1, \ldots, \tilde{v}_{i-1}, \bullet, \tilde{v}_{i+1}, \ldots, \tilde{v}_n).$$
Then there is a positive number δ_i (with the same properties as above) such that the norm of the linear functional
$$\det(v_1, \ldots, v_{i-1}, \bullet, \tilde{v}_{i+1}, \ldots, \tilde{v}_n)$$
is bounded by $\Delta_i + \delta_i$ whenever
$$|v_j - \tilde{v}_j| < \epsilon'$$

for $j = 1, \ldots, i{-}1$. Setting Δ equal to the maximum among $\Delta_1 + \delta_1, \ldots, \Delta_d + \delta_d$, we find that

$$|\det v - \det \tilde{v}|$$

$$\leqslant \sum_{i=1}^{d} \big| \det(v_1, \ldots, v_i, \tilde{v}_{i+1}, \ldots, \tilde{v}_d) - \det(v_1, \ldots, v_{i-1}, \tilde{v}_i, \ldots, \tilde{v}_d) \big|$$

$$= \sum_{i=1}^{d} \big| \det(v_1, \ldots, v_{i-1}, v_i - \tilde{v}_i, \tilde{v}_{i+1}, \ldots, \tilde{v}_d) \big|$$

$$\leqslant \sum_{i=1}^{d} \big| \det(v_1, \ldots, v_{i-1}, \bullet, \tilde{v}_{i+1}, \ldots, \tilde{v}_d) \big| \cdot |v_i - \tilde{v}_i|$$

$$< \sum_{i=1}^{d} (\Delta_i + \delta_i) \cdot \epsilon'$$

$$\leqslant d \cdot \Delta \cdot \epsilon'$$

whenever $|v_j - \tilde{v}_j| < \epsilon'$ for $j = 1, \ldots, d$. Thus, we set $\delta := d \cdot \Delta \cdot \epsilon'$ to complete our outline of the construction of δ. The monotonicity of δ as a function of ϵ' ensures that $\epsilon' \mapsto \delta$ can be inverted.

Turning to the proof of the proposition, we assume that $\det v > \epsilon$ and we find that

$$|\det v| \geqslant |\det \tilde{v}| - |\det v - \det \tilde{v}| > \epsilon - \frac{\epsilon}{2} = \frac{\epsilon}{2} > 0$$

whenever

$$|v_j - \tilde{v}_j| < \epsilon'(\delta = \epsilon/2)$$

for $j = 1, \ldots, d$, as required. $\qquad\square$

4. Basis for receding Z

We construct an algorithm which takes as input a prime q_s and a natural number n, and outputs two primes $q_s \leqslant q_M < p$ and a doubly indexed family

$$\{a_{i,j}\}_{\substack{2 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant d_i}}.$$

For i odd, we will set $a_{i,1} = -\vec{1}_1$, so that

$$\mathrm{Li}_i^{\mathrm{u}}(a_{i,1}) = \zeta^{\mathrm{u}}(i).$$

The remaining elements $a_{i,j}$ are $Z_{>q_M}$-points of X. We name this algorithm *basis for receding Z*. We first announce the meaning of the output in a proposition. If A is a graded algebra, we let $A_{[\leqslant n]}$ denote the subalgebra generated by elements of graded degrees $\leqslant n$. If A is a polynomial algebra, we refer to a set of free generators as an *algebra basis*.

Proposition 4.1. Suppose the algorithm *basis for receding* Z (mentioned above and constructed in segments 4.2–4.3 below) halts on the input (q_s, n) and, upon halting, outputs the data

$$\left(q_M, p, \{a_{i,j}\}_{\substack{2 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant d_i}} \right).$$

Then the unipotent logarithms $\log^{\mathrm{u}} q$ for q prime $\leqslant q_M$, together with the unipotent polylogarithms and zeta elements

$$\mathrm{Li}_i^{\mathrm{u}}(a_{i,j})$$

for $2 \leqslant i \leqslant n$ and $1 \leqslant j \leqslant d_i$, form an algebra basis for $A^G_{[\leqslant n]}(Z_{>q_M})$. In particular, the integral depth-one conjecture (2.3.6) holds for q_s in half-weights $\leqslant n$. Additionally, the p-adic zeta values $\zeta^p(m)$ for m odd $\in [3, n]$ are nonzero.

4.2. **Subalgorithm.** We begin by constructing a subalgorithm that will be applied recursively within the main algorithm. The input consists of

- two primes $q_M < p$,
- an $\epsilon \in p^{-\mathbb{N}}$,
- a height-bound $b \in \mathbb{N}$; we denote by $X(Z_{>q_M})_b \subset X(Z_{>q_M})$ the set of elements of height $\leqslant b$,
- a family of elements $a_{i,j} \in X(Z_{>q_M})_b$ such that the associated family of motivic polylogarithms

$$L_{i,j} = \mathrm{Li}_i^{\mathrm{u}}(a_{i,j})$$

forms an algebra basis

$$\mathcal{B}^G = \{L_{i,j}\}_{i \leqslant n}$$

for $A^G_{[\leqslant n]}(Z_{>q_M})$; we set $L_{1,j} = \log^{\mathrm{u}}(q_j)$, and $L_{i,1} = \zeta^{\mathrm{u}}(i)$ for i odd $\geqslant 3$.

The output is a function (in the form of a list or a "dictionary") which assigns to any $a \in X(Z_{>q_M})_b$, and any $m \leqslant n$, an expansion of $\mathrm{Li}_m^{\mathrm{u}}(a)$ in the monomial vector-space basis associated to the algebra basis $\mathcal{B}^G$ to precision ϵ. The construction is recursive in m.

4.2.1. In the presence of the basis $\mathcal{B}^G$, the $\mathbb{Q}$-algebra $A^G_{[\leqslant n]}(Z_{>q_M})$ may be identified as a vector space with a space of vectors with entries in the field $\mathbb{Q}$ of rational numbers equipped with the p-adic absolute value, and the computations that follow are carried out there. As a matter of notation, we let

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

denote the monomial vector space basis associated to the algebra basis $\mathcal{B}^G$, numbered so that

$$\mathcal{A}_{m,j} = L_{m,j}$$

for $j = 1, \ldots, \dim \mathfrak{n}^G_{-m}$, and $\mathcal{A}_{m,j}$ is a shuffle monomial in $L_{m',j'}$ with $m' < m$ for $j > \dim \mathfrak{n}^G_{-m}$. For the base case of our recursive construction, we have

$$\mathrm{Li}^{\mathrm{u}}_1(a) = -\log^{\mathrm{u}}(1-a) \in A^G_1 \cong \mathbb{Q}^{\{q_1, \ldots, q_M\}},$$

which we may expand in the logarithms $\log^{\mathrm{u}} q_j$ by decomposing $1 - a$ as a product of primes.

4.2.2.   Assume we've expanded the polylogarithmic values $\mathrm{Li}^{\mathrm{u}}_{<m}(a)$ in our basis for $A^G_{[<m]}(Z_{>q_M})$ up to precision ϵ. Our basis gives us in particular a basis

$$\mathcal{A}' = \mathcal{A}_1 \times \mathcal{A}_{m-1} \cup \mathcal{A}_2 \times \mathcal{A}_{m-1} \cup \cdots \cup \mathcal{A}_{m-1} \times \mathcal{A}_1$$

for the direct sum of tensor products

$$A^G_1 \otimes A^G_{m-1} + A^G_2 \otimes A^G_{m-2} + \cdots + A^G_{m-1} \otimes A^G_1,$$

and allows us to identify the latter with a space $\mathbb{Q}^N$ of vectors.

Assume m odd (the case m even is simpler). Recall from 2.1.1($*^\vee$) that in this case, the reduced coproduct Δ' on A^G_m is injective modulo the motivic zeta value $\zeta^{\mathrm{u}}(m)$. Because of our imperfect approximations, $\Delta' \mathrm{Li}^{\mathrm{u}}_m(a)$ may not quite be in the linear span of the images $\Delta' \mathcal{A}_{m,j}$ of the basis elements $\mathcal{A}_{m,j} \in A^G_m$. We may nevertheless *project* $\Delta' \mathrm{Li}^{\mathrm{u}}_m(a)$ onto the subspace spanned by the $\Delta' \mathcal{A}_{m,j}$ (relative to the basis $\mathcal{A}'$) and compute the coefficients:

$$\Delta' \mathrm{Li}^{\mathrm{u}}_m(a) = \sum_{j=2}^{\dim A^G_m} c_j \Delta' \mathcal{A}_{m,j}.$$

To do so, we expand each vector $\Delta' \mathcal{A}_{m,j}$ in the basis $\mathcal{A}'$ to precision ϵ, and we expand the new vector $\Delta' \mathrm{Li}^{\mathrm{u}}_m(a)$ in the basis $\mathcal{A}'$ to precision ϵ as well. We then set

$$c_j := \langle \Delta' \mathrm{Li}^{\mathrm{u}}_m(a), \Delta' \mathcal{A}_{m,j} \rangle$$

where the inner product is the standard inner product on $\mathbb{Q}^N$.

This gives us all coefficients except for the coefficient c_1 of $\zeta^{\mathrm{u}}(m)$. To determine the latter, we use the period map as follows. Letting $\mathrm{Li}^\epsilon_m(a)$, $\mathcal{A}^\epsilon_{m,j}$ denote ϵ-approximations of the p-adic periods of $\mathrm{Li}^{\mathrm{u}}_m(a)$, $\mathcal{A}_{m,j}$ produced by the algorithm of Besser–de Jeu [BdJ], we set

$$c_1 := \frac{\mathrm{Li}^\epsilon_m(a) - \sum_{j=2}^{\dim A^G_m} c_j \mathcal{A}^\epsilon_{m,j}}{\zeta^\epsilon(m)}$$

(decreasing ϵ if needed so as to achieve $|\zeta^\epsilon(m)| > \epsilon$). We then have the expansion

$$\mathrm{Li}^{\mathrm{u}}_m(a) \underset{\epsilon}{\sim} \sum c_j \mathcal{A}_{m,j}$$

we hoped for. This completes the construction of the subalgorithm.

4.3. **Main algorithm.** We now construct the main algorithm of this section. Recall that we are given as input a prime q_s and a natural number n. Our primary goal is to construct a basis for $A^G_{[\leqslant n]}(Z_{>q_M})$ using p-adic approximations, where q_M is a prime $\geqslant q_s$ and p is a prime $> q_M$. Along the way we will search for potential basis elements among the points

$$X(Z_{>q_M})_b \subset X(Z_{>q_M})$$

of height $\leqslant b$. Since there may not be enough of these points, we will enthusiastically increase b while reluctantly considering the possibility of increasing q_M, and hence p. Our secondary goal is to ensure that our p-adic approximations are good enough to witness the nonvanishing (known for p regular, conjectured in general) of the p-adic zeta values $\zeta^p(m)$ for m odd $\in [3, n]$.

Let I denote the set of quadruples (q_M, p, b, ϵ) with $p > q_M \geqslant q_s$ primes, $b \in \mathbb{N}$, and $\epsilon \in p^{-\mathbb{N}}$. Let $J \subset I$ be a subset with the following properties. (1) The projection of J onto the coordinate plane (b, ϵ) defines ϵ as a decreasing function of b. (2) There exists an increasing function $b \mapsto p_b$ from the natural numbers to the set of primes, such that for fixed (b, ϵ), the fiber of J above (b, ϵ) is equal to the set of all pairs of primes $q_M < p \leqslant p_b$ in which p is the *next* prime after q_M. We *arbitrarily* impose an ordering on the set J.

4.3.1. *Remark.* Psychologically, we may imagine q_M, p and b to be *increasing* while ϵ *decreases*. However, it is important that after decreasing ϵ, we also *decrease* q_M and p. Thus, as the algorithm proceeds, we occasionally revisit past primes in order to give them a second chance.

4.3.2. *Remark.* Given $(q_M, p, b, \epsilon) \in J$ then, the algorithm attempts to verify the nonvanishing of the p-adic zeta values and to build a basis for

$$A^G_{[\leqslant n]}(Z_{>q_M})$$

using the points of $X(Z_{>q_M})_b$ and using p-adic approximations of precision ϵ. This may fail for several reasons. One reason is that an ϵ-approximation of one of the p-adic zeta values $\zeta^p(m)$ may equal 0. A second reason is that, having potentially succeeded in constructing a partial basis, there may not be another linearly independent polylogarithm available among the points of $X(Z_{>q_M})_b$ and this may be because b is too small or because the entire set of $Z_{>q_M}$-points $X(Z_{>q_M})$ is too small. Finally, even if an appropriate choice of next basis element *can* be found inside $X(Z_{>q_M})_b$, our ϵ-approximations may be too coarse to see the linear independence.

4.3.3. We now assume, in preparation for the recursive step, that we've reached a data point $(q_M, p, b, \epsilon) \in J$. Assume further that we have constructed an algebra basis for $A^G_{[<m]}(Z_{>q_M})$ for some $m \leqslant n$ consisting of motivic logarithms, motivic zeta values, and motivic polylogarithms $\mathrm{Li}^{\mathrm{u}}_i(a_{i,j})$

with $a_{i,j} \in X(Z_{>q_M})_b$. Assume further that we've constructed a partial algebra basis in weight m given by unipotent m-logarithms

$$L_1 = \mathrm{Li}_m^{\mathrm{u}}(a_{m,1}), \ldots, L_r = \mathrm{Li}_m^{\mathrm{u}}(a_{m,r})$$

($a_{m,j} \in X(Z_{>q_M})_b$) which are linearly independent modulo the space D_n^G of decomposables. We choose arbitrarily a point $a \in X(Z_{>q_M})_b$ and an $\epsilon \in p^{-\mathbb{N}}$ and consider adding $L := \mathrm{Li}_m^{\mathrm{u}}(a)$ to our basis. We use the subalgorithm of segment 4.2 above to expand Δ' of the decomposables in weight m, the $\Delta' L_i$, as well as our new candidate $\Delta' L = \Delta' \mathrm{Li}_m^{\mathrm{u}}(a)$ with p-adic precision ϵ in our polylogarithmic basis

$$\bigcup_{i+j=m,\ i,j \geqslant 1} \mathcal{A}_i \times \mathcal{A}_j$$

for the space

$$\bigoplus_{i+j=m,\ i,j \geqslant 1} A_i^G \otimes A_j^G$$

and check the result for ϵ-linear independence (ignoring L_1 if m is odd).

- If the result is negative, we go on to the next quadruple $(q_M, p, b, \epsilon) \in J$. If p has changed, we verify the nonvanishing of an ϵ-approximation $\zeta^\epsilon(m)$ of $\zeta^p(m)$ for m odd $\in [3, n]$, decreasing ϵ as needed.
- If the result is positive, we set $a_{m,r+1}$ equal to a and continue the process.

We halt when we reach $r = \dim \mathfrak{n}_m^G$ for each $m \leqslant n$. This completes the construction.

Proposition 4.4. Assume p regular (or nonvanishing of the p-adic zeta values $\zeta^p(m)$ for m odd $\geqslant 3$). Assume the integral depth-1 conjecture (2.3.6) holds for q_M in half weights $\leqslant n$. Then the algorithm of segment 4.3 halts.

5. Change of basis

5.1. We continue to work with the scheme $Z_{>q_M}$ produced in §4 and we drop the repeated argument '$(Z_{>q_M})$' throughout this section. Recall that $A_{[\leqslant n]} \subset A$ denotes the subalgebra generated by elements of half-weight $\leqslant n$, and similarly for $A_{[\leqslant n]}^G$. Given our polylogarithmic algebra-basis

$$\mathcal{B}_{\leqslant n}^G = \bigcup_{i=1}^n \mathcal{B}_i^G$$

for $A_{[\leqslant n]}^G$, there exists an algebra basis $\mathcal{B}_{\leqslant n} = \bigcup_{i=1}^n \mathcal{B}_i$ for $A_{[\leqslant n]}$ which extends $\mathcal{B}_{\leqslant n}^G$, as well as associated free generators

$$\tau_1, \ldots, \tau_M, \ \sigma_3, \sigma_5, \sigma_7, \ldots$$

of the Lie algebra $\mathfrak{n} = \mathfrak{n}(Z_{>q_M})$ (in half-weights bounded below by $-n$), where we identify the latter with the set of Lie-like elements in the completed universal enveloping algebra (c.f. remark 3.3 above). We detail the construction of this algebra basis, in notation chosen to accord with [DC,

§3.1]. Let $\mathcal{P}^G_{\leqslant n} \subset \mathcal{B}^G_{\leqslant n}$ denote the subset obtained by removing the extension classes (i.e. the logarithms and zeta elements). In half-weight 1 we set

$$\mathcal{P}_1 = \mathcal{P}^G_1 = \varnothing.$$

In half-weight $i \geqslant 2$ we extend the set $\mathcal{P}^G_i$ (by choosing arbitrary linearly independent elements of $A_i \subset A$) to a linearly independent subset $\mathcal{P}_i$ of A_i which spans a linear complement to the subspace

$$E_i \oplus D_i \subset A_i$$

spanned by extensions and decomposables. Set

$$\mathcal{E}_i := \begin{cases} \{\log^{\mathrm{u}} q_1, \ldots, \log^{\mathrm{u}} q_M\} & i = 1 \\ \zeta^{\mathrm{u}}(i) & i > 1 \text{ odd} \\ \varnothing & i > 1 \text{ even,} \end{cases} \qquad \mathcal{E}_{\leqslant n} := \bigcup_{i=1}^{n} \mathcal{E}_i, \quad \mathcal{P}_{\leqslant n} := \bigcup_{i=1}^{n} \mathcal{P}_i,$$

and

$$\mathcal{B}_{\leqslant n} := \mathcal{E}_{\leqslant n} \cup \mathcal{P}_{\leqslant n}.$$

Let τ_i be the element of $\mathcal{U}_{-1}$ (half-weight -1 part of the completed universal enveloping algebra) dual to $\log^{\mathrm{u}} q_i$ relative to the basis

$$\mathcal{B}_1 = \{\log^{\mathrm{u}} q_1, \ldots, \log^{\mathrm{u}} q_M\}$$

of A_1. For $q = q_i$ a prime $\leqslant q_M$, we sometimes write τ_q in place of τ_i.

Let $\mathcal{A}_r$ denote the set of monomials of half-weight r in the set $\mathcal{B}_{\leqslant n} \subset A$. For r odd $(3 \leqslant r \leqslant n)$ let σ_r be the element of $\mathcal{U}_{-r}$ dual to $\zeta^{\mathrm{u}}(r)$ relative to the vector space basis $\mathcal{A}_r$ of A_r. Then according to propositions 3.2.2 and 3.2.3 of [DC],

$$A_{[\leqslant n]} = \mathbb{Q}[\mathcal{B}_{\leqslant n}].$$

as $\mathbb{Q}$-algebras, and the τ_q, σ_r form free generators as hoped.[9]

5.2.   If w is a word in the generators τ_q, σ_r, and $\mathcal{A}$ is an element of the vector-space basis for A^G generated by the polylogarithmic algebra basis (i.e. a monomial in $\mathcal{B}^G_{\leqslant n}$), then the value

$$\langle \mathcal{A}, w \rangle \in \mathbb{Q}$$

is independent of the choice of basis for A beyond the polylogarithmic basis constructed for A^G.

We now construct an algorithm which takes as input a polylogarithmic basis, a word w in the generators τ_q, σ_r, an element $\mathcal{A}$ of the vector space basis generated by the algebra basis, and an ϵ, and computes $\langle \mathcal{A}, w \rangle$ to precision ϵ. The construction is a dévissage in three steps. An example is worked out for instance in §7.6.3 of [DCW2] as well as in [CDC].

---

[9] The resulting algebra basis $\mathcal{B}_{\leqslant n}$ is a mixture of concrete polylogarithmic elements of A^G which we have constructed algorithmically on the one hand, with abstract elements of A on the other hand, whose construction does not intervene in the algorithm. If we were to separate our construction of the algorithm from our verification that its output has the desired meaning, then these last elements would serve as a mere book-keeping device in the construction.

5.2.1.   If $\mathcal{A} = \mathcal{A}'\mathcal{A}''$ is a product of two or more algebra-basis elements, we use the relationship

$$\langle \mathcal{A}'\mathcal{A}'', w \rangle = \langle \mathcal{A}' \otimes \mathcal{A}'', \mu(w) \rangle$$

between the shuffle product on A and the coproduct μ on its completed universal enveloping algebra $\mathcal{U}$ repeatedly to reduce to the case that $\mathcal{A} = L$ is itself an algebra-basis element.

5.2.2.   The values $\langle L, w \rangle$ for L a logarithm, an n-logarithm, or a zeta value obey the following rules. We have

$$\langle \log^{\mathrm{u}} a, \tau_q \rangle = v_q(a)$$

(the q-adic valuation of a) and all other values $\langle \log^{\mathrm{u}} a, w \rangle$ vanish. We have

$$\langle \mathrm{Li}_1^{\mathrm{u}} a, \tau_q \rangle = \langle -\log^{\mathrm{u}}(1 - a), \tau_q \rangle = -v_q(1 - a).$$

By proposition 3.9, we have

$$\langle \mathrm{Li}_n^{\mathrm{u}} a, \tau_1 \cdots \tau_n \rangle = \langle \mathrm{Li}_1^{\mathrm{u}} a, \tau_1 \rangle \langle \log^{\mathrm{u}} a, \tau_2 \rangle \cdots \langle \log^{\mathrm{u}} a, \tau_n \rangle,$$

and

$$\langle \mathrm{Li}_n^{\mathrm{u}} a, \sigma_r \tau_1 \cdots \tau_s \rangle = \langle \mathrm{Li}_r^{\mathrm{u}} a, \sigma_r \rangle \langle \log^{\mathrm{u}} a, \tau_1 \rangle \cdots \langle \log^{\mathrm{u}} a, \tau_s \rangle$$

$(r + s = n)$, and all other values $\langle \mathrm{Li}_n^{\mathrm{u}} a, w \rangle$ vanish. Finally, by definition

$$\langle \zeta^{\mathrm{u}}(n), \sigma_n \rangle = 1$$

and all other values $\langle \zeta^{\mathrm{u}}(n), w \rangle$ vanish. Using these formulas, we reduce to the computation of the values $\langle \mathrm{Li}_r^{\mathrm{u}}(a), \sigma_r \rangle$, noting, however, that $\mathrm{Li}_r^{\mathrm{u}}(a)$ may not be an algebra basis element.

5.2.3.   We use the method of §4.2 to expand $\mathrm{Li}_r^{\mathrm{u}}(a)$ in our polylogarithmic basis in half-weight r to precision ϵ. We have thus reduced to the case that $\mathcal{A} = L$ is again an algebra-basis element, while $w = \sigma_r$ is a one-letter word. Finally, by our very definition of σ_r, we have

$$\langle L, \sigma_r \rangle = \begin{cases} 1 \text{ if } L = \zeta^{\mathrm{u}}(r), \text{ and} \\ 0 \text{ otherwise.} \end{cases}$$

This completes the construction of the algorithm.

5.3. **Remark.** Given $w \in \mathcal{U}_{-k}$ a word in the generators τ_p, σ_r (with $k \leqslant n$), we let $f_w \in A_k$ denote the dual element relative to the basis consisting of such words. In terms of the resulting shuffle basis, the above computations can be rewritten as follows:

$$\log^{\mathrm{u}} q = f_{\tau_q},$$
$$\zeta^{\mathrm{u}}(n) = f_{\sigma_n},$$

and

$$\mathrm{Li}_i^{\mathrm{u}}(a) = \sum \langle \mathrm{Li}_r^{\mathrm{u}} a, \sigma_r \rangle v_{q_1}(a) \cdots v_{q_s}(a) f_{\sigma \tau_{q_1} \cdots \tau_{q_s}} + \sum v_{q_0}(a) \cdots v_{q_i}(a) f_{\tau_{q_0} \cdots \tau_{q_i}}$$

$(a = a_{i,j},\ r + s = i)$.

6. Basis for $Z \subset \operatorname{Spec} \mathbb{Z}$ arbitrary

6.1.   We now consider $Z \subset Z_{>q_M}$ arbitrary. At this point we have a polylog-arithmic basis $\{\mathcal{A}_{i,j}\}$ for $A^G_{[\leqslant n]}(Z_{>q_M})$, a shuffle basis $\{f_w\}$ for all of $A(Z_{>q_M})$ (both in bounded weights $\leqslant n$), and a matrix M expanding the former in the latter to precision ϵ, which we think of as the matrix associated to the inclusion

$$A^G_{\leqslant n}(Z_{>q_M}) \subset A_{\leqslant n}(Z_{>q_M})$$

(where the subscript $\leqslant n$ refers to the vector subspace of elements in graded degrees $\leqslant n$) relative to the polylogarithmic basis on the source and the shuffle basis on the target. Relative to the shuffle basis, $A_{\leqslant n}(Z) \subset A_{\leqslant n}(Z_{>q_M})$ is the hyperplane spanned by f_w with w not involving the generators τ_q for primes $q \in Z$. Pulling back via M, we obtain a system of linear equations. We may then construct a basis for the space of solutions by basic methods of linear algebra. The result is a vector space basis $\mathcal{A}^G$ of $A^G_{\leqslant n}(Z)$.

7. Geometric algorithm

7.1.   The *geometric algorithm* takes as input a finite set

$$\Sigma_{-1} = \{\tau_1, \ldots, \tau_s\}$$

and a natural number n, and outputs a finite set

$$\{F_1^a, \ldots, F_N^a\}$$

of elements of the polynomial algebra

$$\mathbb{Q}[\{f_\lambda\}_\lambda, \log^{\mathrm{u}}, \mathrm{Li}_1^{\mathrm{u}}, \mathrm{Li}_2^{\mathrm{u}}, \ldots, \mathrm{Li}_n^{\mathrm{u}}]$$

where λ ranges over the set of Lyndon words in the (suitably ordered) set

$$\Sigma = \bigcup_{i=1}^{n} \Sigma_{-i}$$

where Σ_{-i} contains one element σ_i for i odd $\geqslant 3$ and no elements for i even. (The superscript 'a' stands for *abstract*.)

7.2.   This algorithm is independent of the previous algorithms, and its halting is unconditional. We first explain the meaning of its output. Let $\pi^{\mathrm{un}}(\Sigma)$ be the free prounipotent group on the set Σ with $\mathbb{G}_m$-action induced by placing Σ_i in graded degree i. Let $\mathfrak{n} = \mathfrak{n}(\Sigma)$ be its Lie algebra — the free pronilpotent Lie algebra on the set Σ. Let $\mathfrak{n}^G(\Sigma)$ be the quotient

$$\mathfrak{n}^G(\Sigma) := \mathfrak{n}/[\mathfrak{n}_{\leqslant -2}, \mathfrak{n}_{\leqslant -2}],$$

let $\pi^G(\Sigma)$ be the associated quotient of $\pi^{\mathrm{un}}(\Sigma)$ and let $A^G(\Sigma) = \mathcal{O}(\pi^G(\Sigma))$ be the associated Hopf algebra. There is a canonical isomorphism

$$A(\Sigma) := \mathcal{O}(\pi_1^{\mathrm{un}}(\Sigma)) = \mathbb{Q}[\{f_\lambda\}_\lambda],$$

hence an inclusion

$$A^G(\Sigma) \subset A(\Sigma) = \mathbb{Q}[\{f_\lambda\}_\lambda].$$

Let $\mathfrak{n}^{\mathrm{PL}}_{\geqslant -n}$ be the graded Lie algebra

$$\mathfrak{n}^{\mathrm{PL}}_{\geqslant -n} = \mathbb{Q}(1) \ltimes \prod_{i=1}^{n} \mathbb{Q}(i)$$

(with $\mathbb{Q}(i)$ placed in graded degree $-i$) and let $\pi^{\mathrm{PL}}_{\geqslant -n}$ denote the associated unipotent $\mathbb{Q}$-group. Let

$$\log^{\mathrm{u}} = f_0, \qquad \mathrm{Li}^{\mathrm{u}}_1 = f_1, \qquad \mathrm{Li}^{\mathrm{u}}_2 = f_{10}, \qquad \dots \qquad \mathrm{Li}^{\mathrm{u}}_n = f_{10\cdots 0}$$

denote shuffle coordinates on $\pi^{\mathrm{PL}}_{\geqslant -n}$ associated to its presentation as a quotient

$$\pi^{\mathrm{un}}(e_0, e_1) \twoheadrightarrow \pi^{\mathrm{PL}}_{\geqslant -n}$$

of the free prounipotent group on two generators e_0, e_1. Endow $\pi^{\mathrm{PL}}_{\geqslant -n}$ with the trivial $\pi^G(\Sigma)$-action. Let $\mathfrak{ev}^G_n(\Sigma)$ denote the evaluation map

$$\pi^G(\Sigma) \times Z^1(\pi^G(\Sigma), \pi^{\mathrm{PL}}_{\geqslant -n})^{\mathbb{G}_m} \to \pi^G(\Sigma) \times \pi^{\mathrm{PL}}_{\geqslant -n}.$$

$$\mathfrak{ev}^G_n(\Sigma)(\gamma, c) = (\gamma, c(\gamma)).$$

Then the functions $F^a_1, \dots, F^a_N$ produced by the algorithm are contained in

$$A^G(\Sigma)[\log^{\mathrm{u}}, \mathrm{Li}^{\mathrm{u}}_1, \dots, \mathrm{Li}^{\mathrm{u}}_n]$$

where they generate the ideal associated to the scheme theoretic image of $\mathfrak{ev}^G_n(\Sigma)$.

7.3. We now construct the algorithm. As a corollary of proposition 3.9 above, we find in [CDC, Corollary 3.11] that the *full* cocycle evaluation map

$$\mathfrak{ev}_n(\Sigma) : \pi^{\mathrm{un}}(\Sigma) \times Z^1\big(\pi^{\mathrm{un}}(\Sigma), \pi^{\mathrm{PL}}_{\geqslant -n}\big)^{\mathbb{G}_m} \to \pi^{\mathrm{un}}(\Sigma) \times \pi^{\mathrm{PL}}_{\geqslant -n}$$

(i.e. without passing to the Goncharov quotient) is given in coordinates by the map of finite type polynomial algebras over $\mathbb{Q}$

$$\mathbb{Q}[\{f_\lambda\}_\lambda, \{\Phi^\rho_\Lambda\}_{\mathrm{wt}(\rho)=\mathrm{wt}(\Lambda)}] \leftarrow \mathbb{Q}[\{f_\lambda\}_\lambda, \log^{\mathrm{u}}, \mathrm{Li}^{\mathrm{u}}_1, \mathrm{Li}^{\mathrm{u}}_2, \dots, \mathrm{Li}^{\mathrm{u}}_n],$$

(where λ ranges over Lyndon words in the generators τ, σ of $\pi^{\mathrm{un}}_1(Z)$, Λ ranges over the set of polylogarithmic words in e_0, e_1 of weight $\leqslant n$, and ρ ranges over the set of generators τ, σ of $\pi^{\mathrm{un}}_1(Z)$) given by

$$\sum_{\tau \in \Sigma_{-1}} f_\tau \Phi^\tau_0 \leftarrow\!\shortmid \log^{\mathrm{u}}$$

and

$$\sum_{\substack{\tau_1, \dots, \tau_r \in \Sigma_{-1} \\ \sigma \in \Sigma_{-s} \\ r + s = n \\ 1 \leqslant s \leqslant n}} f_{\tau_1 \cdots \tau_r \sigma} \Phi^{\tau_1}_0 \cdots \Phi^{\tau_r}_0 \Phi^\sigma_{\underbrace{0 \cdots 0 1}_{s}} \leftarrow\!\shortmid \mathrm{Li}^{\mathrm{u}}_n.$$

Since

$$Z^1\big(\pi^G(\Sigma), \pi^{\mathrm{PL}}\big)^{\mathbb{G}_m} = Z^1\big(\pi^{\mathrm{un}}(\Sigma), \pi^{\mathrm{PL}}\big)^{\mathbb{G}_m},$$

the scheme theoretic image of $\mathfrak{ev}_n^G(\Sigma)$ is the same as the scheme theoretic image of the composite

$$\pi^{\mathrm{un}}(\Sigma) \times Z^1\big(\pi^{\mathrm{un}}(\Sigma), \pi^{\mathrm{PL}}_{\geqslant -n}\big)^{\mathbb{G}_m} \to \pi^{\mathrm{un}}(\Sigma) \times \pi^{\mathrm{PL}}_{\geqslant -n} \to \pi^G(\Sigma) \times \pi^{\mathrm{PL}}_{\geqslant -n}.$$

In terms of coordinate rings, this means restricting the map $\mathfrak{ev}_n(\Sigma)^\sharp$ to the subalgebra

$$A^G(\Sigma)[\log^{\mathrm{u}}, \mathrm{Li}_1^{\mathrm{u}}, \mathrm{Li}_2^{\mathrm{u}}, \ldots, \mathrm{Li}_n^{\mathrm{u}}].$$

By proposition 3.2 (which, in turn, is a direct application of [DC, 3.1.1]), a basis for the latter may be constructed out of the basis $\{f_\lambda\}$ for $\pi^{\mathrm{un}}(\Sigma)$ by elementary linear algebra. Subsequently, a set of generators for the kernel of

$$\mathbb{Q}[\{f_\lambda\}_\lambda, \{\Phi_\Lambda^\rho\}_{\mathrm{wt}(\rho)=\mathrm{wt}(\Lambda)}] \leftarrow A^G(\Sigma)[\log^{\mathrm{u}}, \mathrm{Li}_1^{\mathrm{u}}, \mathrm{Li}_2^{\mathrm{u}}, \ldots, \mathrm{Li}_n^{\mathrm{u}}]$$

may be constructed by standard methods of elimination theory. This completes our construction of the geometric algorithm.

7.4. **Remark.** If $\mathcal{C}$ is the universal cocycle

$$\pi_1^{\mathrm{un}}(Z) \times Z^1\big(\pi_1^{\mathrm{un}}(Z), \pi^{\mathrm{PL}}(X)\big)^{\mathbb{G}_m} \to \pi^{\mathrm{PL}}(X) \times Z^1\big(\pi_1^{\mathrm{un}}(Z), \pi^{\mathrm{PL}}(X)\big)^{\mathbb{G}_m},$$

then

$$\Phi^\rho_{\underbrace{0\cdots 01}_{n}}(\mathcal{C}) = \langle \mathrm{Li}_n^{\mathrm{u}}(\mathcal{C}), \rho \rangle$$

(this equality takes place inside the coordinate ring of Z^1, or, in terms of our shuffle basis, inside $\mathbb{Q}[\{\Phi_\Lambda^\rho\}]$). In other words, $\Phi^\rho_{0\ldots 01}$ corresponds to the function on cocycles $\langle \mathrm{Li}_n^{\mathrm{u}}(?), \rho \rangle$.

8. Loci algorithm

In terms of the basis algorithms, the change of basis algorithm, and the geometric algorithm, our *loci algorithm* is similar to the algorithm of [DC, §4.2]; we repeat the construction, making adjustments as needed.

8.1.   The loci algorithm takes as input an open subscheme $Z \subset \mathrm{Spec}\,\mathbb{Z}$, a natural number n and an ϵ. As output, it returns a prime $p \in Z$, a polylogarithmic algebra basis $\mathcal{B}_{\leqslant n}^G$ of the polynomial ring $A_{[\leqslant n]}^G(Z)$ and a family $\{F_i\}_i$ of elements of the polynomial ring

$$\mathbb{Q}[\mathcal{B}_{\leqslant n}^G, \log^{\mathrm{u}}, \mathrm{Li}_1^{\mathrm{u}}, \ldots, \mathrm{Li}_n^{\mathrm{u}}].$$

8.2.   Before constructing the algorithm, we explain the meaning of its output upon halting. There's an obvious homomorphism

$$\mathbb{Q}[\mathcal{B}_{\leqslant n}^G, \log^{\mathrm{u}}, \mathrm{Li}_1^{\mathrm{u}}, \ldots, \mathrm{Li}_n^{\mathrm{u}}] \to \mathrm{Col}(X(\mathbb{Z}_p))$$

to the ring of Coleman functions. Let F_i^p denote the image of F_i. We symmetrize the family $\{F_i^p\}_{i \in I}$ with respect to the S_3 action as indicated in segment 2.4.2 to obtain a bigger family $\{F_j^p\}_{j \in J}$. Then the family $\{F_j^p\}_{j \in J}$ is within ϵ of a set of generators for the ideal of $\mathrm{Col}(X(\mathbb{Z}_p))$ which defines the (symmetrized) polylogarithmic Chabauty-Kim locus $X(\mathbb{Z}_p)_n$.

8.3.   The algorithm is constructed as follows. We run the *geometric algorithm* (§7) on the set of symbols

$$\Sigma_{-1} = \{q_1, \ldots, q_s\}$$

with s equal to the number of primes excluded from Z. This gives us a family $\{F_i^a\}$ of elements of the polynomial $\mathbb{Q}$-algebra

$$\mathbb{Q}[\{f_\lambda\}_\lambda, \log^{\mathrm{u}}, \mathrm{Li}_1^{\mathrm{u}}, \mathrm{Li}_2^{\mathrm{u}}, \ldots, \mathrm{Li}_n^{\mathrm{u}}].$$

Thus, the *coefficients* of F_i^a are elements of the vector space $\mathbb{Q}[\{f_w\}]$ with basis indexed by words w in the set $\{\tau_1, \ldots, \tau_s,\ \sigma_{-3}, \sigma_{-5}, \ldots\}$. (In fact, by their construction, the coefficients will belong to the subspace corresponding to the Goncharov quotient.)

We run the algorithm *basis for receding Z* (§4) on the input (q_s, n) to obtain a pair of primes $q_s \leqslant q_M < p$ and a polylogarithmic algebra basis

$$\text{(*)} \qquad\qquad\qquad {}_{>q_M}\mathcal{B}_{\leqslant n}^G$$

(hence also an associated monomial vector space basis ${}_{>q_M}\mathcal{A}_{\leqslant n}^G$) of

$$A_{[\leqslant n]}^G(Z_{>q_M}).$$

We run the *change of basis algorithm* (§5) on the polylogarithmic algebra basis (*) and we run the *basis algorithm for arbitrary Z* (§6) on the further input Z. By elementary linear algebra, we obtain

(1) a polylogarithmic algebra basis $\mathcal{B}_{\leqslant n}^G$ for $A_{[\leqslant n]}^G(Z)$, and

(2) for each element $\mathcal{A}$ of the associated vector space basis $\mathcal{A}_{\leqslant n}^G$, an associated vector $M(\mathcal{A})$ in the vector space $\mathbb{Q}[\{f_w\}]$.

We now expand the coefficients of each F_i^a in the vectors $M(\mathcal{A})$ to obtain a family $\{F_i\}$ of elements of the polynomial ring

$$\mathbb{Q}[\mathcal{B}_{\leqslant n}^G, \log^{\mathrm{u}}, \mathrm{Li}_1^{\mathrm{u}}, \ldots, \mathrm{Li}_n^{\mathrm{u}}]$$

as hoped. This completes the construction of the algorithm.

9. POINT COUNTING ALGORITHM

9.1.   Our *root criterion algorithm* from [DC, §5] combines standard methods of Newton polygons together with a growth estimate obtained by Besser–de Jeu [BdJ] to decide whether the number of zeroes of a p-adic power series in a given ball is zero or one, given a sufficiently close approximation. We do not repeat it here.

9.2.   Our *point-counting algorithm* from [DC, §7] remains unchanged; we nevertheless do repeat it for the reader's convenience, while avoiding the double tildes of loc. cit. as indicated in remark 2.3.10. This algorithm takes as input an open subscheme Z of $\operatorname{Spec} \mathbb{Z}$ and proceeds by running two processes simultaneously. One process is simply a naive search for points of $X(Z)$. This produces a gradually increasing subset $X(Z)_n \subset X(Z)$.

The other process locates an appropriate prime $p \in Z$ and computes the loci $X(\mathbb{Z}_p)_n$ to given precision. It then verifies if it is possible, with the given level of precision, to declare an equality

$$X(Z)_n = X(\mathbb{Z}_p)_n.$$

9.3.   We begin by running our basis algorithm. In addition to the polylogarithmic basis of $A^G_{[\leqslant n]}(Z)$ which will remain fixed throughout the remainder of the construction, this also gives us the auxiliary prime p.

Having done so, 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. The boolean output will be constructed in segments 9.4–9.7. 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 simply search for points up to a suitable hight-bound depending on n which goes to infinity with n. The remainder of the construction concerns the boolean output.

9.4.   We partition $X(\mathbb{Z}_p)$ 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). We run our loci algorithm to produce a family $\{F_i\}_i$ of polylogarithmic functions on $X(\mathbb{Z}_p)$.

9.5.   We now focus our attention on an ϵ-ball B containing a rational representative $y \in B$. Using *Lip service* [BdJ], we expand each polylogarithmic function F_i to arithmetic precision ϵ and geometric precision e^{-N} about y. In a technical step explained in the proof of theorem 7.2.1 of [DC], we must check that all nonzero coefficients are larger than ϵ, returning *False* if not.

9.6.   Let b be the number of points (0 or 1) in $X(Z)_n \cap B$. We run the root-criterion algorithm on the ball B, on the precision-levels N and ϵ, and on each of the functions F_i, to verify if B contains no more than b roots.

9.7.   We repeat steps 9.5-9.6 in each ball. This completes the construction of the algorithm.

REFERENCES

[BDCKW]   J. Balakrishnan, I. Dan-Cohen, M. Kim, and S. Wewers. A non-abelian conjecture of Birch and Swinnerton-Dyer type for hyperbolic curves. Preprint. arXiv:1209.0640v1.

[BdJ]   Amnon Besser and Rob de Jeu. Li$^{(p)}$-service? An algorithm for computing p-adic polylogarithms. *Math. Comp.*, 77(262):1105–1134, 2008.

[Bor1]   Armand Borel. Sur la cohomologie des espaces fibrés principaux et des espaces homogènes de groupes de Lie compacts. *Ann. of Math. (2)*, 57:115–207, 1953.

[Bor2]   Armand Borel. Cohomologie de SL_n et valeurs de fonctions zeta aux points entiers. *Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4)*, 4(4):613–636, 1977.

[Bro1]   Francis Brown. Integral points on curves, the unit equation, and motivic periods. arXiv:1704.00555v1.

[Bro2]   Francis Brown. Mixed Tate motives over $\mathbb{Z}$. *Ann. of Math. (2)*, 175(2):949–976, 2012.

[BW]   A. Baker and G. Wüstholz. *Logarithmic forms and Diophantine geometry*, volume 9 of *New Mathematical Monographs*. Cambridge University Press, Cambridge, 2007.

[CDC]   David Corwin and Ishai Dan-Cohen. The polylog quotient and the Goncharov quotient in computational Chabauty-Kim theory I. arXiv:1812.05707v3.

[DC]   Ishai Dan-Cohen. Mixed Tate motives and the unit equation II. arXiv:1510.01362v3.

[DCS]   Ishai Dan-Cohen and Tomer Schlank. Rational motivic path spaces and Kim's relative unipotent section conjecture. arXiv:1703.10776.

[DCW1]   Ishai Dan-Cohen and Stefan Wewers. Explicit Chabauty-Kim theory for the thrice punctured line in depth two. *Proceedings of the London Math Society*. To appear. arXiv:1209.0276v1.

[DCW2]   Ishai Dan-Cohen and Stefan Wewers. Mixed Tate motives and the unit equation. *Int. Math. Res. Not. IMRN*, (17):5291–5354, 2016.

[Del]   Pierre Deligne. Le groupe fondamental de la droite projective moins trois points. In *Galois groups over **Q** (Berkeley, CA, 1987)*, volume 16 of *Math. Sci. Res. Inst. Publ.*, pages 79–297. Springer, New York, 1989.

[DG]   P. Deligne and A. B. Goncharov. Groupes fondamentaux motiviques de Tate mixte. *Ann. Sci. École Norm. Sup. (4)*, 38(1):1–56, 2005.

[dW]   B. M. M. de Weger. *Algorithms for Diophantine equations*, volume 65 of *CWI Tract*. Stichting Mathematisch Centrum, Centrum voor Wiskunde en Informatica, Amsterdam, 1989.

[EG]   Jan-Hendrik Evertse and Kálmán Győry. *Unit equations in Diophantine number theory*, volume 146 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2015.

[Fur]   Hidekazu Furusho. p-Adic multiple zeta values. I. p-adic multiple polylogarithms and the p-adic KZ equation. *Invent. Math.*, 155(2):253–286, 2004.

[Gon1]   Alexander B. Goncharov. Polylogarithms and motivic Galois groups. In *Motives (Seattle, WA, 1991)*, volume 55 of *Proc. Sympos. Pure Math.*, pages 43–96. Amer. Math. Soc., Providence, RI, 1994.

[Gon2]   Alexander B. Goncharov. Galois symmetries of fundamental groupoids and noncommutative geometry. *Duke Math. J.*, 128(2):209–284, 2005.

[Kim1]   Minhyong Kim. The motivic fundamental group of $\mathbb{P}^1 \backslash \{0, 1, \infty\}$ and the theorem of Siegel. *Invent. Math.*, 161(3):629–656, 2005.

[Kim2]   Minhyong Kim. Tangential localization for Selmer varieties. *Duke Math. J.*, 161(2):173–199, 2012.

[Lev]   Marc Levine. Tate motives and the fundamental group. In *Cycles, motives and Shimura varieties*, Tata Inst. Fund. Res. Stud. Math., pages 265–392. Tata Inst. Fund. Res., Mumbai, 2010.

[vKM]   Rafael von Känel and Benjamin Matschke. Solving S-unit, Mordell, Thue, Thue–Mahler and generalized Ramanujan–Nagell equations via Shimura–Taniyama conjecture. arXiv:1605.06079.

 David Corwin
Department of mathematics
970 Evans Hall #3840
University of California
Berkeley, CA 94720-3840
Email Address: `corwind@alum.mit.edu`

 Ishai Dan-Cohen
Department of mathematics
Ben-Gurion University of the Negev
Be'er Sheva, Israel
Email address: `ishaidc@gmail.com`