AN ALGORITHM FOR COMPUTING p-ADIC MULTIPLE ZETA VALUES

SEIDAI YASUDA

Contents

1. Introduction

1.1. **On this article.** Let p be a prime number. The aim of this article is to give an algorithm for computing p-adic multiple zeta values defined by Furusho [F]. A rough sketch of our algorithm is a follows:

- Let W denote the set of words of two letters 0, 1. We introduce in Section 2.3.2 a subset $W_1 \subset W$.
- Let $\widetilde{B}$ denote the (commutative) polynomial ring over $\mathbb{Z}$ in (infinitely many) variables indexed by $W \times W$. We introduce in Section 3.1.1 a certain quotient ring B of $\widetilde{B}$.
- Let us consider the free B module $B[W]$ with basis W.
- In section 3.1 we define a map $H : W_1 \times W \to B[W]$ by an inductive method. W, W_1, $\widetilde{B}$, B and H do not depend on the choice of p.
- We introduce in (3.1) an integer $C_{p,m}$ for each integer $m \geq 0$.
- We introduce in Section 3.3.1 a p-adic number $Z_p(\Bbbk_1, \ldots, \Bbbk_r) \in \mathbb{Q}_p$ for indices $\Bbbk_1, \ldots, \Bbbk_r$ (we refer Section 2.1 for the definition of an index).
- We introduce in Section 3.3.3 a map $\widetilde{Z}_p : W \times W \to \mathbb{Q}_p$. We extend this to a homomorphism $\widetilde{Z} : \widetilde{B} \to \mathbb{Q}_p$ of rings. This homomorphism factors

Date: 09 May 2014, modified for ss2018 on August 28, 2018.

through the quotient homomorphism $\widetilde{B} \to B$ and induces a homomorphism $Z : B \to \mathbb{Q}_p$ of rings.
- We can inductively compute the p-adic multiple zeta values by using (3.4). (See section 2.3.3 for the definition of the symbol $\Bbbk(w)$ which appears in (??).)

The reader can understand the algorithm only by reading the paragraphs and the equation referred above.

The author have made some numerical computation of p-adic multiple zeta values using the algorithm above, which have lead him to a conjecture relating the p-adic multiple zeta values with the mod. p multiple harmonic sums studied by [?] and [Zh].

2. Notation

2.1. Notation for modules. For a set S and for a commutative ring R, we denote by $R[S]$ the free R-module with basis S. For $s \in S$, we denote by the symbol $[s]$ the element s regard as a member of the basis of $R[S]$.

2.2. Notation for the multiple zeta values.

2.2.1. *Notation for indices.* Let $\mathbb{Z}_{\geq 0}$, $\mathbb{Z}_{\geq 1}$ denote the set of non-negative integers, the set of positive integer, respectively. Let us introduce the following set I:

$$I = \coprod_{n \in \mathbb{Z}_{\geq 0}} (\overbrace{\mathbb{Z}_{\geq 1} \times \cdots \times \mathbb{Z}_{\geq 1}}^{n \text{ times}}).$$

An element of I is called an index. Let $\Bbbk = (k_1, \ldots, k_n)$ be an index. The integer $|\Bbbk| = k_1 + \cdots + k_n$ is called the weight of $\Bbbk$ (when $n = 0$, we understand $|\Bbbk| = 0$.

The unique index with $|\Bbbk| = 0$ is called the empty index and is denoted by $\emptyset$.

2.2.2. *Multiple polylogarithms.* Let $\Bbbk = (k_1, \ldots, k_n)$ be an index. Let $\angle_n$ denote the set

$$\angle_n = \{(m_1, \ldots, m_n) \in \mathbb{Z}^n \mid 0 < m_1 < \cdots < m_n\}. \tag{2.1}$$

The following infinite sum is called the multiple polylogarithm with index $\Bbbk$:

$$\mathrm{Li}_{\Bbbk}(z) = \mathrm{Li}_{k_1, \ldots, k_d}(z) = \sum_{(m_1, \ldots, m_n) \in \angle_n} \frac{z^{m_n}}{m_1^{k_1} \cdots m_n^{k_n}}.$$

We regard it as a formal power series in t with coefficients in $\mathbb{Q}$. When $k = \emptyset$, we understand $\mathrm{Li}_{\Bbbk}(z) = 1$.

2.2.3. *Multiple zeta values.* We say that an index $\Bbbk = (k_1, \ldots, k_n)$ is admissible if $\Bbbk = \emptyset$ or $k_n \geq 2$.

Suppose that $\Bbbk = (k_1, \ldots, k_n)$ in an admissible index. Then the infinite sum $\mathrm{Li}_{\Bbbk}(1)$ converges to a real number which we denote by $\zeta(\Bbbk)$ or by $\zeta(k_1, \ldots, k_n)$. By definition we have

$$\zeta(\Bbbk) = \sum_{0 \leq m_1 < \ldots < m_n} \frac{1}{m_1^{k_1} \cdots m_n^{k_n}}.$$

2.3. Notation for words. Let W denote the (non-commutative) free monoid generated by the two elements 0, 1. We denote by e the unit element of W. We regard an element of W as a word in letters 0 and 1. Any $w \in W$ can be written as $w = w_1 \cdots w_k$, where $k \geq 0$ is an integer and $w_1, \ldots, w_k$ are elements of $\{0, 1\}$. The expression $w_1 \cdots w_k$ of w is called the *spelling of* w. The integer k is called the *length of* w and is denoted by $\ell(w)$. For $v, w \in W$, we denote by vw or by $w \circ v$ the word obtained by joining v and w.

2.3.1. *Some inversions of words.* Let $w \in W$ and let $w = w_1 \cdots w_k$ be the spelling of w. The word $w_k \cdots w_1$ is called the *order-inversion of* w and is denoted by $(w)^{\leftrightarrow}$. Let us write $w'_i = 1 - w_i$ for $i = 1, \ldots, k$. The word $w'_1 \cdots w'_k$ is called the *letter-inversion of* w and is denoted by $(w)^{\updownarrow}$. We have the equality $((w)^{\leftrightarrow})^{\updownarrow} = ((w)^{\updownarrow})^{\leftrightarrow} = w'_k \cdots w'_1$. We call the word $((w)^{\leftrightarrow})^{\updownarrow}$ the *dual of* w and is denoted by $\iota(w)$.

2.3.2. *The submonoid* $W_1 \subset W$. We let $W_1 \subset W$ denote the subset of words $w \in W$ which is either equal to e or a word which begins with 1. Then W_1 is a submonoid of W.

2.3.3. *The correspondence between indices and words.* Let $\Bbbk = (k_1, \ldots, k_n)$ be an index. The word

$$w(\Bbbk) = 1\,\overbrace{0\cdots\cdots0}^{k_1-1 \text{ times}}\,1\,\overbrace{0\cdots\cdots0}^{k_2-1 \text{ times}}\,1\cdots\cdots\cdots1\,\overbrace{0\cdots\cdots0}^{k_n-1 \text{ times}}$$

is called the word corresponding to the index $\Bbbk$. (Here we understand $w(\Bbbk) = e$ when $\Bbbk = \emptyset$.) By definition, $w(\Bbbk)$ is a word of length $|\Bbbk|$ which belongs to W_1.

For any $w \in W_1$, there exists a unique index $\Bbbk$ satisfying $w(\Bbbk) = w$. We denote this index by $\Bbbk(w)$.

3. An algorithm for computing p-adic MZV's

3.1. The map $H : W \times W \to B[W]$.

3.1.1. *Some more notation.* We denote by $\widetilde{B}$ the (commutative) polynomial ring with integral coeffieints in infinite variables indexed by $W \times W$. For $(v, w) \in W \times W$, we denote by $\widetilde{X}_{v,w}$ the element (v, w) regarded as a variable in $\widetilde{B}$. We denote by B the quotient of $\widetilde{B}$ by the ideal genrated by the set

$$\{\widetilde{X}_{v1,w} - \widetilde{X}_{v,1w} \mid v, w \in W\} \cup \{\widetilde{X}_{1v,w} - \widetilde{X}_{v,w1} \mid v, w \in W\} \cup \{\widetilde{X}_{v,e} \mid v \in W\}.$$

For $v, w \in W$, we denote by $X_{v,w}$ the image of $\widetilde{X}_{v,w}$ in B.

For a pair $(v, w) \in W \times W$ satisfying $vw \in W_1$, we denote by $X^{(2)}_{v,w}$ the following element in B:

$$X^{(2)}_{v,w} = \begin{cases} 0, & \text{if } v = w = e, \\ X_{e,w'0}, & \text{if } v = e, w \neq e \text{ (here we set } w = 1w'), \\ X_{v',w0}, & \text{if } v \neq e \text{ (here we set } v = 1v'). \end{cases}$$

3.1.2. *The map* $H : W \times W \to B[W]$. Let us consider the free B-module $B[W]$ with basis W. For $v \in W$, we set

$$Y(v) = \{(v', v'') \in W \times W \mid v = v'v''\},$$

$$Y_0(v) = \{(v', v'') \in W \times W \mid v = v'0v''\}$$

$$Y_1(v) = \{(v', v'') \in W \times W \mid v = v'1v''\}.$$

Let us define a map $H : W_1 \times W \to B[W]$ inductively by the following rules:

- For any $v \in W_1$, $w \in W$ with $vw \in W_1$,

$$
\begin{aligned}
H(v,w) = \quad & [vw] + \sum_{\substack{(v',v'')\in Y(v)\\ v''\neq e}} X_{v'',w}[v'] + \sum_{(w',w'')\in Y(w)} X_{e,w''}[vw'] \\
& - \sum_{(w',w'')\in Y_0(w)} \left(\begin{array}{l} \displaystyle\sum_{(v',v'')\in Y_1(v)} X_{v'',w'0}(H(v'0,w'')+H(v'1,w'')) \\ \displaystyle + \sum_{(v',v'')\in Y_1(w')} X_{e,v''0}(H(vv'0,w'')+H(vv'1,w'')) \end{array} \right) \\
& + \sum_{(w',w'')\in Y_1(w)} \left(\begin{array}{l} \displaystyle\sum_{(v',v'')\in Y_0(v)} X_{0v'',w'}(H(v'0,w'')+H(v'1,w'')) \\ \displaystyle + \sum_{(v',v'')\in Y_0(w')} X_{e,0v''}(H(vv'0,w'')+H(vv'1,w'')) \end{array} \right) \\
& + \sum_{(w',w'')\in Y(w)} X^{(2)}_{v,w'} H(e,w'').
\end{aligned}
$$

  Here any term of the form $H(0,w')$ are understood to be zero.
- For any $w \in W$ which begins with 0, we have $H(e,w) = 0$.

3.1.3. *The meaning of $H(v,w)$.* Let $(v,w) \in W_1 \times W$ with $vw \in W_1$. We explain the meaning of $H(v,w)$.

Let p be a prime number. Let us define the formal power series $L_{(v,w)} \in \mathbb{Q}[[t]]$ inductively by the following rules:

- $L_{(v,e)}(z) = \mathrm{Li}_{\Bbbk(v)}(z)$
- Suppose $w \neq e$ and let us write $w = w'x$ with $x \in \{0,1\}$. Then

$$
dL_{(v,w)}(z) = \begin{cases} L_{(v,w')}(z)\frac{d(\varphi(z))}{\varphi(z)}, & x = 0, \\ L_{(v,w')}(z)\frac{d(\varphi(z))}{1-\varphi(z)}, & x = 1 \end{cases}
$$

  (here $\varphi(z) = 1-(1-z)^p$) and $L_{(v,w)}(0) = 0$.

Later we will introduce a ring homomorphism $Z : B \to \mathbb{Q}_p$. Let us write $H(v,w) = \sum_{w'} b_{w'}[w']$. Then $\sum_{w'} Z(b_{w'})\zeta_p(\Bbbk(w'))$ can be interpreted as the value at $z=1$ of an suitable analytic continuation of the power series $L_{(v,w)}(z)$.

3.1.4. *Variant. The map $H' : W \times W \to B[s][W]$.* Let us consider the polynomial ring $B[s]$ over B in one variable s. Let us define a map $H' : W_1 \times W \to B[s][W]$ inductively by the following rules:

- For any $v \in W_1$, $w \in W$ with $vw \in W_1$,

$$
\begin{aligned}
H'(v,w) = \quad & [vw] + \sum_{\substack{(v',v'')\in Y(v)\\ v''\neq e}} X_{v'',w}[v'] + \sum_{(w',w'')\in Y(w)} X_{e,w''}[vw'] \\
& - \sum_{(w',w'')\in Y_0(w)} \left(\begin{array}{l} \displaystyle\sum_{(v',v'')\in Y_1(v)} X_{v'',w'0}(H'(v'0,w'')+H'(v'1,w'')) \\ \displaystyle + \sum_{(v',v'')\in Y_1(w')} X_{e,v''0}(H'(vv'0,w'')+H'(vv'1,w'')) \end{array} \right) \\
& + \sum_{(w',w'')\in Y_1(w)} \left(\begin{array}{l} \displaystyle\sum_{(v',v'')\in Y_0(v)} X_{0v'',w'}(H'(v'0,w'')+H'(v'1,w'')) \\ \displaystyle + \sum_{(v',v'')\in Y_0(w')} X_{e,0v''}(H'(vv'0,w'')+H'(vv'1,w'')) \end{array} \right) \\
& + \sum_{\substack{(w',w'')\in Y(w)\\ w''\in W_1}} X^{(2)}_{v,w'} s^{\ell(w'')}[w''].
\end{aligned}
$$

Here all the terms of the form $H'(0,w')$ in the right hand side are assumed to be zero, and any term of the form $H'(1,w')$ is understood to be $s^{\ell(w')+1}[1w']$.

- For any $w \in W$ which begins with 0, we have $H'(e,w) = 0$.

3.2. **The constants $C_{p,m}$.** In this paragraph we fix a prime number p.

For an integer $m \geq 0$, we denote by $C_{p,m}$ the following integer

$$C_{p,m} = \sum_{0 \leq i \leq \lfloor \frac{m}{p} \rfloor} (-1)^{pi} \binom{m}{pi}. \tag{3.1}$$

If we let $\mu_p \subset \overline{\mathbb{Q}}_p$ denote the set of p-th roots of unity, then we have

$$C_{p,m} = \frac{1}{p} \sum_{\zeta \in \mu_p} (1-\zeta)^m.$$

This shows that the p-adic order of $C_{p,m}$ is at least $\max(\left\lceil \frac{m}{p-1} \right\rceil - 1, 0)$. We can check that this bound of $\mathrm{ord}_p(C_{p,m})$ is optimal when m is divisible by $p-1$. Moreover we have:

Lemma 3.1. *Let us write $m = pm' + r$ with $0 \leq r - 1$. Let s be the unique integer satisfying $0 \leq s \leq p-2$ and $m' + s \equiv 0 \mod (p-1)\mathbb{Z}$. We then have*

1. *If $r = s = 0$, then $\mathrm{ord}_p(C_{p,m})$ is equal to $\max(\left\lceil \frac{m}{p-1} \right\rceil - 1, 0) = \max(\frac{pm'}{p-1} - 1, 0)$.*
2. *If $r \neq 0$ and $s = 0$, then $\mathrm{ord}_p(C_{p,m})$ is equal to $\max(\left\lceil \frac{m}{p-1} \right\rceil - 1, 0) = \frac{pm'}{p-1}$.*
3. *Suppose that $s \neq 0$. Then*

$$\sum_{j=1}^{r} (-1)^j \binom{r}{j} j^s$$

is not divisible by p if and only if $\mathrm{ord}_p(C_{p,m})$ is equal to $\max(\left\lceil \frac{m}{p-1} \right\rceil - 1, 0) = \left\lceil \frac{pm'}{p-1} \right\rceil$.

□

When m is divisible by p and not divisible by $p-1$, then m does not satisfy any of the three conditions in the lemma above. In this case we can see that $\mathrm{ord}_p(C_{p,m})$ is strictly smaller that $\max(\left\lceil \frac{m}{p-1} \right\rceil - 1, 0)$. For example if m is odd and is divisible by p, then it can be checked easily that $C_{p,m} = 0$.

3.3. **An algorithm.**

3.3.1. *The sum $Z_p(\mathbb{k}_1, \ldots, \mathbb{k}_r)$.* Let $\mathbb{k}_1, \ldots, \mathbb{k}_r$ be finitely many non-empty indices. Let us write $\mathbb{k}_i = (k_{i,1}, \ldots, k_{i,n_i})$. We set

$$\angle_{n_1,\ldots,n_r} = \left\{ ((m_{i,1}, \ldots, m_{i,n_i}))_{1 \leq i \leq r} \in \angle_{n_1} \times \cdots \times \angle_{n_r} \mid m_{1,n_1} \geq m_{2,1}, \ldots, m_{r-1,n_{r-1}} \geq m_{r,1} \right\}$$

We define $Z_p(\mathbb{k}_1, \ldots, \mathbb{k}_r) \in \mathbb{Q}_p$ to be the sum

$$Z_p(\mathbb{k}_1, \ldots, \mathbb{k}_r) = \sum_{((m_{i,1},\ldots,m_{i,n_i}))_{1 \leq i \leq r} \in \angle_{n_1,\ldots,n_r}} \frac{C_{p,m_{1,n_1}-m_{2,1}} \cdots C_{p,m_{r-1,n_{r-1}}-m_{r,1}} C_{p,m_{r,n_r}}}{\prod_{1 \leq i \leq r} \prod_{1 \leq j \leq n_i} m_{i,j}^{k_{i,j}}}. \tag{3.2}$$

3.3.2. *Words in three letters.* Let $\mathbb{W}$ denote the set of words in the three letters 0, 1, and 2. We regard W as a subset of $\mathbb{W}$. We denote by $\mathbb{W}_2 \subset \mathbb{W}$ the subset of elements of $\mathbb{W}$ which is either equal to e or a word which ends with the letter 2. Any element w of $\mathbb{W}_2$ is uniquely written as

$$w = w^{(1)} 2 w^{(2)} 2 \cdots 2 w^{(r-1)} 2 w^{(r)} 2$$

with $w^{(1)}, \ldots, w^{(r)} \in W$. We denote by $\mathbb{K}(w)$ the sequence

$$\mathbb{K}(w) = (\Bbbk(1w^{(1)}), \Bbbk(1w^{(2)}), \ldots, \Bbbk(1w^{(r)}))$$

of indices. This gives a one-to-one correspondence between the elements in $\mathbb{W}_2$ and a finite sequence of indices.

Let $T_2 : W \to \mathbb{W}$ denote the map defined as follows: for $w \in W$, $T_2(w)$ is the word obtained by replacing the letters 0 in $(w)^{\leftrightarrow}$ with 2. For example we have $T_2(01001) = 12212$.

We have the following (non-trivial) formula, whose proof will be given in Section A.3 of the appendix.

Proposition 3.2. *Let $w \in \mathbb{W}_2$. Suppose $w \neq e$ and w does not contain the letter 0. Then we have $Z_p(\mathbb{K}(w)) = 0$.* □

3.3.3. *The sum $Z_p(v,w)$.* Let $v, w \in W$. In the computation of p-adic MZV's, the sum

$$(-1)^{\ell(w)+1} \sum_{w'} Z_p(\mathbb{K}(w'2))$$

(here $\ell(w)$ denotes the length of the word w, and w' in the sum runs over the shuffles of the words v and $T_2(w)$) plays an important role. We denote this sum by $Z_p(v,w)$.

It seems important to compute the p-adic orders of $Z_p(v,w)$ for various $v, w \in W$. The following formula is non-trivial, and is proved by using a strengthened version of Proposition 3.2 and the theory of Coleman integrals. Details of the proof will be given in Section A.5 of the appendix.

Proposition 3.3. *Let $v, w \in W$. Then we have*

$$Z_p(1v, w) = Z_p(v, w1).$$

□

For $(v,w) \in W \times W$, we set

$$\widetilde{Z}_p(v,w) = \sum_{(w',w'') \in Y_0(w)} Z_p(vw', w'').$$

Proposition 3.4. *Let $v, w \in W$. We then have*
1. $\widetilde{Z}_p(v1, w) = \widetilde{Z}_p(v, 1w)$,
2. $\widetilde{Z}_p(1v, w) = \widetilde{Z}_p(v, w1)$,
3. $\widetilde{Z}_p(v, e) = 0$.

□

Proof. The claims (1), (3) are obvious. The claim (2) follows from Proposition 3.3. □

3.3.4. *The algorithm.* Let $\widetilde{Z} : \widetilde{B} \to \mathbb{Q}_p$ be the ring homomorphism defined as follows: for $(v,w) \in W \times W$, the homomorphism $\widetilde{Z}$ sends $\widetilde{X}_{v,w}$ to $\widetilde{Z}_p(v,w)$. It follows from Proposition 3.4 that the homomorphism $\widetilde{Z} : \widetilde{B} \to \mathbb{Q}_p$ factors through the projection $\widetilde{B} \to B$. We denote by Z the induced homomorphism $B \to \mathbb{Q}_p$.

Theorem 3.5. *Let $w \in W_1$ and let us write $H(e,w) = \sum_{v \in W} b_v[v]$. We then have*

(1) *If* $\ell(v) \geq \ell(w)$ *and* $v \neq w$*, then we have* $b_v = 0$*.*
(2) *We have* $b_w = 1$*.*
(3) *If* $v \notin W_1$*, then we have* $Z(b_v) = 0$*.*
(4) *We have*

$$p^{-\ell(w)}\zeta_p(\Bbbk(w)) = \sum_{v \in W_1} Z_p(b_v)\zeta_p(\Bbbk(v)). \tag{3.3}$$

By using this theorem, we can inductively compute $\zeta_p(\Bbbk)$.

3.3.5. *A variant.* We extend the homomorphism $Z : B \to \mathbb{Q}_p$ to the homomorphism $Z : B[s] \to \mathbb{Q}_p$ by setting $Z(s) = 1/p$.

Theorem 3.6. *Let* $w \in W_1$ *and let us write* $H'(e, w) = \sum_{v \in W} b'_v[v]$*. We then have:*

(1) *If* $\ell(v) \geq \ell(w)$ *and* $v \neq w$*, then we have* $b'_v = 0$*.*
(2) *We have* $b'_w = 1$*.*
(3) *If* $v \notin W_1$*, then we have* $Z(b'_v) = 0$*.*
(4) *We have*

$$p^{-\ell(w)}\zeta_p(\Bbbk(w)) = \sum_{v \in W_1} Z_p(b'_v)\zeta_p(\Bbbk(v)). \tag{3.4}$$

We can inductively compute $\zeta_p(\Bbbk)$ also by using this theorem. It seems that the latter algorithm is more effective.

References

[F] Furusho, H.: *p-adic multiple zeta values I.* Invent. Math. **155**, 253–286 (2004)

[H] Hoffman, M. E.: *Quasi-symmetric functions and mod p multiple harmonic sums.* Preprint math/0401319

[Zh] Zhao, J.: *Wolstenholme type theorem for multiple harmonic sums.* Int. J. Number Theory **4**, no. 1, 73–106 (2008)

Appendix A. Proofs of Proposition 3.2 and 3.3

In this appendix we give proofs of Proposition 3.2 and 3.3.

A.1. **Notation.**

A.1.1. In this appendix we fix a prime number p. We denote by $\mathbb{Q}_p$ the field of p-adic numbers. For $x \in \mathbb{Q}_p$, we denote by $|x|_p$ the p-adic absolute value of x satisfying $|p|_p = 1/p$. Let us fix an algebraic closure $\overline{\mathbb{Q}}_p$ of $\mathbb{Q}_p$. The absolute value $|\ |_p$ on $\mathbb{Q}_p$ can be uniquely extended to an absolute value on $\overline{\mathbb{Q}}_p$, which we denote by the same symbol $|\ |_p$.

A.1.2. *Formal power series.* We denote by $\mathbb{Q}_p[[z]]$ the ring of formal power series with coefficients in $\mathbb{Q}_p$ in the formal variable z. Let $R \subset \mathbb{Q}_p[[z]]$ denote the subring of formal power series $f(z)$ which are p-adically convergent on $|z| < 1$. By definition, a formal power series $f(z) = \sum_{n\geq 0} a_n z^n \in \mathbb{Q}_p[[z]]$ belongs to R if and only if $\lim_{n\to\infty} |a_n|_p r^n = 0$ for any real number r with $0 < r < 1$. Let $f(z) \in R$ and $\zeta \in \mu_p$. Let us write $f(z) = \sum_{n\geq 0} a_n z^n$. For an element $\alpha \in \overline{\mathbb{Q}}_p$ with $|\alpha|_p < 1$, the series $\sum_{n\geq 0} a_n \alpha^n$ is p-adically convergent to an element in $\overline{\mathbb{Q}}_p$. We denote this element by $f(\alpha)$.

A.1.3. *Notation for words.* We use the following notation for a word with letters in $\{0,1,2\}$, most of which we have already introduced in Section 2.3 for a word with letters in $\{0,1\}$. We denote by e the empty word. For a word w, we denote by $\ell(w)$ the length of w. For a word $w = w_1 \cdots w_k$, we denote by $w^{\leftrightarrow} = w_k \cdots w_1$ the word obtained by reversing the order of w. For two words v, w, we let $\mathrm{Sh}(v,w)$ denote the multiset of shuffles of v and w.

A.2. **The function $\mathcal{L}_w(z)$.** Let $w = w_1 \cdots w_k$, with $w_1, \dots w_k \in \{0,1,2\}$, be a word of letters $0,1,2$. For $i = 0,1,2$ let us write

$$S_i(w) = \{j \in \{1,\dots,k\} \mid w_j = i\}.$$

We denote by M_w the set of $(k+1)$-tuples $(m_1,\dots,m_{k+1})$ of positive integers satisfying the following three conditions:

- For any $i \in S_0(w)$, we have $m_i = m_{i+1}$,
- For any $i \in S_1(w)$, we have $m_i < m_{i+1}$,
- For any $i \in S_2(w)$, we have $m_i \geq m_{i+1}$.

Let us introduce the following formal power series:

$$\mathcal{L}_w(z) = \sum_{(m_1,\dots,m_{k+1}) \in M_w} \frac{\prod_{j \in S_2(w)} C_{p,m_j - m_{j+1}}}{m_1 \cdots m_{k+1}} \cdot z^{m_{k+1}}.$$

We regard this as an element in $\mathbb{Q}_p[[z]]$. One can check easily that $\mathcal{L}_w(z)$ belongs to R.

Let w be a word of letters 0, 1, 2 which ends with 2. Let us write $w = w'2$. By definition we have

$$Z(\mathbb{K}(w)) = \frac{1}{p} \sum_{\zeta \in \mu_p} \mathcal{L}_{w'}(1-\zeta).$$

Let (v,w) be a pair of words of letters 0, 1. We denote by $T_2(w)$ the word of letters 1, 2 obtained by replacing the letter 0 in $w^{\leftrightarrow}$ with the letter 2. Recall that we have defined in Section 3.3.3 the p-adic number $Z_p(v,w)$ to be

$$Z_p(v,w) = (-1)^{\ell(w)+1} \sum_{w' \in \mathrm{Sh}(v, T_2(w))} Z(\mathbb{K}(w'2)).$$

A.3. **Proof of Proposition 3.2.**

Proposition A.1. *For any word w of letters $1,2$ and for any $\zeta \in \mu_p$, we have $\mathcal{L}_w(1-\zeta) = 0$.*

A.3.1. *A strategy of a proof of Proposition A.1.* We set

$$q(z) = \log(1-z) = -\sum_{n \geq 1} \frac{z^n}{n}.$$

Observe that $q(1-\zeta) = 0$ for $\zeta \in \mu_p$, and that $|q(\alpha)|_p \leq |\alpha|_p < 1$ for any $\alpha \in \overline{\mathbb{Q}}_p$ with $|\alpha|_p \leq 1/p^{1/(p-1)}$. Hence it suffices to show the following lemma:

Lemma A.2. *There exists a formal power series $f_w \in R$ satisfying $f_w(0) = 0$ and $\mathcal{L}_w(z) = f_w(q(z))$.*

We prove Lemma A.2 by induction on the length of the word w.

A.3.2. *Two operators* J_1 *and* J_2. For $f(z) = \sum_{n\geq 0} a_n z^n \in \mathbb{Q}[[t]]$, we denote the formal power series $\sum_{n\geq 1} a_{n-1}z^n/n$ by $\int_0^z f(t)dt$. One can check easily that $\int_0^z f(t)dt \in R$ if $f(z) \in R$.

Let us introduce the following three $\mathbb{Q}_p$-linear endomorphisms $J_0, J_1, J_2 : R \to R$ of R: for $f(z) \in R$, we set

$$J_0(f) = \int_0^z \frac{f(t) - f(0)}{t} dt,$$

$$J_1(f) = \int_0^z \frac{f(t)}{1-t} dt,$$

and

$$J_2(f) = \frac{1}{p} \int_0^z \sum_{\zeta \in \mu_p} \frac{f(t) - f(1-\zeta)}{t - (1-\zeta)} dt.$$

Let $w = w_1 \cdots w_k$ be a word of letters $1, 2$. We then have

$$\mathcal{L}_w(z) = J_{w_k} \circ \cdots \circ J_{w_1} \circ J_1(1).$$

Proof of Lemma A.2. If $w = e$ is an empty word, then $\mathcal{L}_e = -q(z)$ and the claim is obvious. Let us assume that $w \neq e$. Let j denote the last letter in w and let us write $w = w'j$. By induction hypothesis, there exists a formal power series $f_{w'}(z) \in R$ satisfying $\mathcal{L}_{w'}(z) = f_{w'}(q(z))$. Let us write $f_{w'}(z) = \sum_{n\geq 1} a_n z^n$.

First suppose that $j = 1$. We then have

$$\mathcal{L}_w(z) = J_1(f_{w'}(q(z))) = \sum_{n\geq 1} a_n \int_0^z \frac{q(t)^n dt}{1-t}.$$

Hence we have $\mathcal{L}_w(z) = f_w(q(z))$ where

$$f_w(z) = -\sum_{n\geq 2} \frac{a_{n-1} z^n}{n}.$$

Next suppose that $j = 2$. By induction hypothesis we have

$$\mathcal{L}_w(z) = J_2(f_{w'}(q(z))) = \frac{1}{p} \int_0^z \sum_{\zeta \in \mu_p} \frac{1}{t - (1-\zeta)} f_{w'}(q(t)) dt.$$

For $\zeta \in \mu_p$, we have

$$\frac{1-t}{(1-\zeta) - t} = \frac{e^{q(t)}}{e^{q(t)} - \zeta}$$

Since

$$\frac{p}{1 - y^p} = \sum_{\zeta \in \mu_p} \frac{1}{1 - \zeta y},$$

we have

$$\begin{aligned} \sum_{\zeta \in \mu_p} \frac{t-1}{t-(1-\zeta)} &= \sum_{\zeta^p = 1} \frac{e^{q(t)}}{e^{q(t)} - \zeta} \\ &= \frac{p}{1 - e^{-pq(t)}} = \frac{1}{q(t)} \cdot \frac{-pq(t)}{e^{-pq(t)} - 1} \\ &= \sum_{k \geq 0} \frac{(-p)^k B_k}{k!} q(t)^{k-1}. \end{aligned}$$

Here B_k denotes the k-th Bernoulli number. Observe that the formal power series $\sum_{k\geq 0}\frac{(-p)^k B_k}{k!}z^k$ belongs to R. Hence we have

$$\mathcal{L}_w(z)=J_2(f_{w'}(q(z)))=\frac{1}{p}\int_0^z\frac{1}{t-1}\sum_{k\geq 0,n\geq 1}\frac{(-p)^k B_k a_n}{k!}q(t)^{k+n-1}dt=f_w(q(z)),$$

where

$$f_w(z)=\frac{1}{p}\sum_{k\geq 0,n\geq 1}\frac{(-p)^k B_k a_n}{(k+n)k!}z^{k+n}.$$

This proves the claim. □

This completes the proof of Proposition A.1.

Proof of Proposition 3.2. Let w be a word of letters 1, 2 which ends with 2. We prove that $Z(\mathbb{K}(w))=0$. Let us write $w=w'2$. By definition $Z(\mathbb{K}(w))$ is equal to the sum

$$\frac{1}{p}\sum_{\zeta\in\mu_p}\mathcal{L}_{w'}(1-\zeta).$$

Hence the claim follows from Proposition A.1. □

A.4. **A description of $Z_p(v,w)$.**

A.4.1. *Some iterated integrals.* We set $S=\{1,2\}\amalg\{1-\zeta\mid\zeta\in\mu_p\}$. When $p=2$, we distinguish $2\in\{1,2\}$ with $1-(-1)$. For $\alpha\in S$, we set

$$\omega_\alpha=\begin{cases}\frac{dz}{1-z} & \text{if } \alpha=1,\\ \frac{dz}{z-\alpha} & \text{if } \alpha=1-\zeta \text{ for some } \zeta\in\mu_p,\\ \frac{1}{p}\sum_{\zeta\in\mu_p}\omega_{1-\zeta}, & \text{if } \alpha=2.\end{cases}$$

Let $\log_p:\overline{\mathbb{Q}}_p^\times\to\overline{\mathbb{Q}}$ denote the branch of p-adic logarithm characterized by $\log_p(p)=0$. For a word $\alpha=\alpha_1\cdots\alpha_k$ of letters in S and for $\beta\in S$ we let $\widetilde{\mathrm{II}}(\alpha,\beta)$ denote the regularized iterated integral

$$\widetilde{\mathrm{II}}(\alpha,\beta)=\int_0^\beta\omega_{\alpha_k}\circ\cdots\circ\omega_{\alpha_1}$$

with respect to the branch $\log_p$ of p-adic logarithm. This regularized iterated integral is an element of $\mathbb{Q}_p[T]$. We denote by $\mathrm{II}(\alpha,\beta)$ the constant term of $\widetilde{\mathrm{II}}(\alpha,\beta)$.

A.4.2. *Auxiliary lemmas.* For a word w of letters 0, 1, 2 which ends with 2 and for an integer $r\geq 1$, let us introduce the following set of r-tuples of words of letters 0, 1, 2:

$$D_r(w)=\{(w^{(1)},\ldots,w^{(r)})\mid w=w^{(1)}2w^{(2)}\cdots 2w^{(r)}2\}.$$

The following lemma can be checked easily:

Lemma A.3. *Let w be a word of letters 0, 1, 2. Then $\zeta\in\mu_p$, the value $\mathcal{L}_w(1-\zeta)$ is equal to the sum*

$$\sum_{r\geq 1}\frac{(-1)^{r-1}}{p^{r-1}}\sum_{\substack{(w^{(1)},\ldots,w^{(r)})\in D_r(w2)\\ \zeta_1,\ldots,\zeta_{r-1}\in\mu_p}}\widetilde{\mathrm{II}}(1w^{(1)},1-\zeta_1)\prod_{j=2}^{r}\widetilde{\mathrm{II}}((1-\zeta_{j-1})w^{(j)},1-\zeta_j).$$

Here in the summand we set $\zeta_r=\zeta$. □

Lemma A.4. *Let w be a word of letters 1, 2. Then for any $\zeta\in\mu_p$ we have $\widetilde{\mathrm{II}}(1w,1-\zeta)=0$.*

Proof. This follows from Proposition A.1 and Lemma A.3 by induction of the length of w. □

Lemma A.5. *Let w be a word of letters* 1, 2.

(1) *Suppose that* $w = \overbrace{2\cdots 2}^{k \text{ times}}$ *for some* $k \geq 0$*. Then for any* $\zeta \in \mu_p$*, we have* $\widetilde{\mathrm{II}}(w, 1-\zeta) = T^k/k!$.

(2) *Suppose that* w *contains the letter* 1*. Then for any* $\zeta \in \mu_p$ *we have* $\widetilde{\mathrm{II}}(w, 1-\zeta) = 0$.

Proof. The claim (1) can be checked directly. We prove the claim (2). Let us write $w = \overbrace{2\cdots 2}^{k \text{ times}} v$ where v begins with 1. We prove the claim by induction on k. If $k = 0$, then the claim follows from Lemma A.4. Suppose that $k \geq 1$. Let us write $w = 2w'$. By induction hypothesis we have $\widetilde{\mathrm{II}}(w', 1-\zeta) = 0$. By applying the shuffle product formula to $\widetilde{\mathrm{II}}(w', 1-\zeta)\widetilde{\mathrm{II}}(2, 1-\zeta) = 0$ and by using induction hypothesis, we have $\widetilde{\mathrm{II}}(w, 1-\zeta) = 0$. □

A.5. **Proof of Proposition 3.3.**

Proposition A.6. *Let v and w be words of letters* 0, 1*. We set* $w'' = T_2(w)2$*. Then* $Z_p(v, w)$ *is equal to the sum*

$$-\sum_{r\geq 1}\frac{1}{p^{r-1}}\sum_{\substack{(w^{(1)},\ldots,w^{(r)})\in D_r(w'')\\ v=v^{(1)}\cdots v^{(r)}}}\sum_{\zeta_1,\ldots,\zeta_r\in\mu_p}\left(\begin{array}{l}\mathrm{II}((w^{(1)})^{\leftrightarrow}1v^{(1)}, 1-\zeta_1)\\ \times\prod_{j=2}^{r}\mathrm{II}((w^{(j)})^{\leftrightarrow}(1-\zeta_{j-1})v^{(j)}, 1-\zeta_j)\end{array}\right).$$

Proof. By Lemma A.3, $Z_p(v, w)$ is equal to $(-1)^{\ell(w)+1}$ times the sum

(A.1)

$$\sum_{r\geq 1}\frac{(-1)^{r-1}}{p^{r-1}}\sum_{\substack{(w^{(1)},\ldots,w^{(r)})\in D_r(w'')\\ v=v^{(1)}\cdots v^{(r)}}}\sum_{\substack{(w'^{(1)},\ldots,w'^{(r)}),\\ w'^{(i)}\in\mathrm{Sh}(v^{(i)},w^{(i)})}}\sum_{\zeta_1,\ldots,\zeta_r\in\mu_p}\left(\begin{array}{l}\mathrm{II}(1w'^{(1)}, 1-\zeta_1)\\ \times\prod_{j=2}^{r}\mathrm{II}((1-\zeta_{j-1})w'^{(j)}, 1-\zeta_j)\end{array}\right).$$

Let us write $w^{(i)} = w_1^{(i)}\cdots w_{k_i}^{(i)}$. By the shuffle product formula we have

$$\begin{aligned}&\sum_{w'^{(1)}\in\mathrm{Sh}(v^{(1)},w^{(1)})}\mathrm{II}(1w'^{(1)}, 1-\zeta_1)\\ =&\sum_{i=0}^{k_1}(-1)^i\mathrm{II}(w_i^{(1)}\cdots w_1^{(1)}1v^{(1)}, 1-\zeta_1)\mathrm{II}(w_{i+1}^{(1)}\cdots w_{k_1}^{(1)}, 1-\zeta_1),\end{aligned}$$

and

$$\begin{aligned}&\sum_{w'^{(j)}\in\mathrm{Sh}(v^{(j)},w^{(j)})}\mathrm{II}((1-\zeta_{j-1})w'^{(j)}, 1-\zeta_j)\\ =&\sum_{i=0}^{k_1}(-1)^i\mathrm{II}(w_i^{(j)}\cdots w_1^{(j)}(1-\zeta_{j-1})v^{(1)}, 1-\zeta_j)\mathrm{II}(w_{i+1}^{(j)}\cdots w_{k_j}^{(j)}, 1-\zeta_j)\end{aligned}$$

for $j = 2, \ldots, r$.

Hence by Lemma A.5, we have

(A.2)
$$\sum_{w'^{(1)}\in\mathrm{Sh}(v^{(1)},w^{(1)})}\mathrm{II}(1w'^{(1)}, 1-\zeta_1) = (-1)^{k_1}\mathrm{II}((w^{(1)})^{\leftrightarrow}1v^{(1)}, 1-\zeta_1),$$

and

(A.3)
$$\sum_{w'^{(j)}\in\mathrm{Sh}(v^{(j)},w^{(j)})}\mathrm{II}((1-\zeta_{j-1})w'^{(j)}, 1-\zeta_j) = (-1)^{k_j}\mathrm{II}((w^{(j)})^{\leftrightarrow}(1-\zeta_{j-1})v^{(j)}, 1-\zeta),$$

for $j = 2, \dots, r$. By applying (A.2) and (A.3) to (A.1), we have the desired equality. □

Proof of Proposition 3.3. The claim follows from Proposition A.6 and Proposition A.1. □

A.6. **A consequence.** For a word w in letters 0, 1, 2, for a word $\alpha = \alpha_1 \cdots \alpha_k$ in letters S, and for $\beta \in S$ we set

$$\widetilde{\mathrm{II}}(w, \alpha, \beta) = \int_0^\beta \omega_{\alpha_k} \circ \cdots \circ \omega_{\alpha_2} \circ \mathcal{L}_w(z) \omega_{\alpha_1}$$

and denote by $\mathrm{II}(w, \alpha, \beta)$ the constant term of $\widetilde{\mathrm{II}}(w, \alpha, \beta)$.

Proposition A.7. *Let v and w be words of letters 0, 1. We set $w'' = T_2(w)2$. Then $Z_p(v, w)$ is equal to the sum*

$$-\sum_{r \geq 1} \frac{1}{p^{r-1}} \sum_{\substack{(w^{(1)}, \dots, w^{(r)}) \in D_r(w'') \\ v = v^{(1)} \cdots v^{(r)}}} \sum_{\zeta_1, \dots, \zeta_r \in \mu_p} \left(\begin{array}{l} \mathrm{II}((w^{(1)})^{\leftrightarrow}, 1v^{(1)}, 1 - \zeta_1) \\ \times \displaystyle\prod_{j=2}^{r} \mathrm{II}((w^{(j)})^{\leftrightarrow}, (1 - \zeta_{j-1}) v^{(j)}, 1 - \zeta_j) \end{array} \right).$$

Remark A.8. *The sum in Corollary A.7 is easier to calculate than that in Proposition A.6, since $\mathrm{II}(w', 1v^{(1)}, 1 - \zeta_1)$ and $\mathrm{II}(w', (1 - \zeta_{j-1}) v^{(j)}, 1 - \zeta_j)$ can be easily written as a p-adically convergent series if w is a non-empty word of letters 1 and 2.*

Proof. We can show, by using Proposition A.1, that

$$\mathrm{II}((w^{(1)})^{\leftrightarrow} 1v^{(1)}, 1 - \zeta_1) = \mathrm{II}((w^{(1)})^{\leftrightarrow}, 1v^{(1)}, 1 - \zeta_1)$$

and

$$\mathrm{II}((w^{(j)})^{\leftrightarrow} (1 - \zeta_{j-1}) v^{(j)}, 1 - \zeta_j) = \mathrm{II}((w^{(j)})^{\leftrightarrow}, (1 - \zeta_{j-1}) v^{(j)}, 1 - \zeta_j)$$

for $j = 2, \dots, r$. Hence the claim follows from Proposition A.6. □

(S. Yasuda) Department of Mathematics, Osaka university, Tokyonaka, Osaka 560-0043, Japan

E-mail address: s-yasuda@math.sci.osaka-u.ac.jp