AN ALGORITHM FOR COMPUTING $p$-ADIC MULTIPLE ZETA VALUES

SEIDAI YASUDA

CONTENTS

1. Introduction 1
   1.1. On this article 1
2. Notation 2
   2.1. Notation for modules 2
   2.2. Notation for the multiple zeta values 2
   2.3. Notation for words 2
3. An algorithm for computing $p$-adic MZV’s 3
   3.1. The map $H : W \times W \to B[W]$ 3
   3.2. The constants $C_{p,m}$ 5
   3.3. An algorithm 5
References 7
Appendix A. Proofs of Proposition 3.2 and 3.3 7
A.1. Notation 7
A.2. The function $L_w(z)$ 8
A.3. Proof of Proposition 3.2 8
A.4. A description of $Z_p(v, w)$ 10
A.5. Proof of Proposition 3.3 11
A.6. A consequence 12

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 as 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 $\tilde{B}$ 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 $\tilde{B}$.
- 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. $W, W_1, \tilde{B}, B$ 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 $Z_p(k_1, \ldots, k_r) \in \mathbb{Q}_p$ for indices $k_1, \ldots, k_r$ (we refer Section 2.1 for the definition of an index).
- We introduce in Section 3.3.3 a map $\tilde{Z}_p : W \times W \to \mathbb{Q}_p$. We extend this to a homomorphism $\tilde{Z} : \tilde{B} \to \mathbb{Q}_p$ of rings. This homomorphism factors.

Date: 09 May 2014, modified for ss2018 on August 28, 2018.
through the quotient homomorphism $\overline{B} \to B$ 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 $k(w)$ 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 $\mathbb{Z}_{\geq 0}$, $\mathbb{Z}_{>0}$ denote the set of non-negative integers, the set of positive integer, respectively. Let us introduce the following set $I$:

$$I = \prod_{n \in \mathbb{Z}_{\geq 0}} (\mathbb{Z}_{\geq 1} \times \cdots \times \mathbb{Z}_{\geq 1}).$$

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

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

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

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

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

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

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

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

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

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

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 $w$. 

\begin{align*}
& \text{\textit{Notation for words.}} \\
& \text{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 $W$} \\
& \text{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 $w_1, \ldots, w_k$} \\
& \text{are elements of $\{0, 1\}$. The expression $w_1 \cdots w_k$ of $w$ is called the spelling of $w$. The integer $k$} \\
& \text{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 $w$.}
\end{align*}
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 \( (w)^{o} \). 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 \( (w)^{l} \). We have the equality \((w)^{o} = (w)^{l} \). We call the word \((w)^{o} \) the dual of \( w \) and is denoted by \( i(w) \).

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 \( k = (k_1, \ldots, k_n) \) be an index. The word

\[
w(k) = 1 \cdot 0 \cdots 0 \cdot 1 \cdot 0 \cdots 1 \cdot \ldots \cdot 1 \cdot 0 \cdots 0
\]

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

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

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 coefficients 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 generated by the set

\[
\{ \widetilde{X}_{v, 1w} - \widetilde{X}_{v, 1w} | v, w \in W \} \cup \{ \widetilde{X}_{1v, w} - \widetilde{X}_{v, w1} | v, w \in W \} \cup \{ \widetilde{X}_{v, e} | v \in W \}.
\]

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 \( X_{v, w}^{(2)} \) the following element in \( B \):

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

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

\[
Y(v) = \{(v', v'') \in W \times W | v = v'v''\},
\]

\[
Y_0(v) = \{(v', v'') \in W \times W | v = v'0v''\}
\]

\[
Y_1(v) = \{(v', v'') \in W \times W | v = v'1v''\}.
\]

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

- $L_{(v, w)}(z) = \text{Li}_{k(v)}(z)$
- Suppose $w \neq e$ and let us write $w = w'x$ with $x \in \{0, 1\}$. Then
  
  $$dL_{(v, w)}(z) = \begin{cases} \frac{d\varphi(z)}{\varphi(z)}, & x = 0, \\ L_{(v, w)}(z) \frac{d\varphi(z)}{\varphi(z)}, & x = 1 \end{cases}$$

(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 $\sum_w Z(b_{w'}) \zeta_p(k(w'))$ 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 $vw \in W_1$,
  
  $$H'(v, w) = [vw] + \sum_{(v', w') \in Y(v)} X_{v', w'}[v'] + \sum_{(w', w') \in Y(w)} X_{e, w'}[vw']$$

  $$- \sum_{(w', w') \in Y_0(w)} \left( \sum_{(v', w') \in Y_1(v)} X_{v', w'}(H'(v', w') + H'(v'1, w'')) + \sum_{(v', w') \in Y_1(w)} X_{e, w'}(H'(vv1, w') + H'(vv'1, w'')) \right)$$

  $$+ \sum_{(w', w') \in Y_1(v)} \left( \sum_{(v', w') \in Y_0(v)} X_{v', w'}(H'(v', w') + H'(v'1, w'')) + \sum_{(v', w') \in Y_0(w)} X_{e, w'}(H'(vv0, w') + H'(vv'1, w'')) \right)$$

  $$+ \sum_{(w', w') \in Y_0(v)} \left( \sum_{(v', w') \in Y_1(w)} X_{v', w'}(H'(v', w') + H'(v'1, w'')) + \sum_{(v', w') \in Y_1(v)} X_{e, w'}(H'(vv0, w') + H'(vv'1, w'')) \right)$$

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 $H(e, w) = 0$. 

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

$$H(v, w) = [vw] + \sum_{(v', w') \in Y(v)} X_{v', w'}[v'] + \sum_{(w', w') \in Y(w)} X_{e, w'}[vw']$$

$$- \sum_{(w', w') \in Y_0(w)} \left( \sum_{(v', w') \in Y_1(v)} X_{v', w'}(H'(v', w') + H'(v'1, w'')) + \sum_{(v', w') \in Y_1(w)} X_{e, w'}(H'(vv1, w') + H'(vv'1, w'')) \right)$$

$$+ \sum_{(w', w') \in Y_1(v)} \left( \sum_{(v', w') \in Y_0(v)} X_{v', w'}(H'(v', w') + H'(v'1, w'')) + \sum_{(v', w') \in Y_0(w)} X_{e, w'}(H'(vv0, w') + H'(vv'1, w'')) \right)$$

$$+ \sum_{(w', w') \in Y_0(v)} \left( \sum_{(v', w') \in Y_1(w)} X_{v', w'}(H'(v', w') + H'(v'1, w'')) + \sum_{(v', w') \in Y_1(v)} X_{e, w'}(H'(vv0, w') + H'(vv'1, w'')) \right)$$
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 $s^{(w')^2 + 1}[1w'].$

- 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

\begin{equation}
C_{p,m} = \sum_{0 \leq s \leq \lfloor \frac{m}{p^1} \rfloor} (-1)^s \left( \frac{m}{p^s} \right).
\end{equation}

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

\begin{equation}
C_{p,m} = \frac{1}{p} \sum_{s \in \mu_p} (1 - \zeta)^m.
\end{equation}

This shows that the $p$-adic order of $C_{p,m}$ is at least $\max\left( \frac{m}{p - 1} - 1, 0 \right)$. We can check that this bound of $\ord_p(C_{p,m})$ 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 $\ord_p(C_{p,m})$ is equal to $\max(\left\lfloor \frac{m}{p - 1} \right\rfloor - 1, 0) = \max(\frac{pm'}{p - 1} - 1, 0)$.

2. If $r \neq 0$ and $s = 0$, then $\ord_p(C_{p,m})$ is equal to $\max(\left\lfloor \frac{m}{p - 1} \right\rfloor - 1, 0) = \frac{pm'}{p - 1}$.

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 $\ord_p(C_{p,m})$ is equal to $\max\left( \left\lfloor \frac{m}{p - 1} \right\rfloor - 1, 0 \right) = \left\lfloor \frac{pm'}{p - 1} \right\rfloor$.

\[\square\]

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 $\ord_p(C_{p,m})$ is strictly smaller that $\max\left( \frac{m}{p - 1} - 1, 0 \right)$. 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 $Z_p(k_1, \ldots, k_r)$

Let $k_1, \ldots, k_r$ be finitely many non-empty indices. Let us write $k_i = (k_{i,1}, \ldots, k_{i,n_i})$. We set

\[\zeta_{n_1, \ldots, n_r} = \{(m_{1,1}, \ldots, m_{i,n_i}) | 1 \leq i \leq r \in \zeta_{n_1} \times \cdots \times \zeta_{n_r}, m_{1,1} \geq m_{2,1}, \ldots, m_{r-1,n_{r-1}} \geq m_{r,1}\}\]

We define $Z_p(k_1, \ldots, k_r) \in \mathbb{Q}_p$ to be the sum

\begin{equation}
Z_p(k_1, \ldots, k_r) = \sum_{(m_{1,1}, \ldots, m_{i,n_i})_1 \leq i \leq r \in \zeta_{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}}}
\end{equation}

\[\prod_{1 \leq i \leq r} \prod_{1 \leq j \leq n_i} m_{i,j}^{k_{i,j}} \]
3.3.2. Words in three letters. Let \( W \) 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

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

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

\[
   K(w) = (k(1w^{(1)}), k(1w^{(2)}), \ldots, k(1w^{(r)}))
\]

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 \( (w)^* \) 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 \( Z_p(K(w)) = 0 \). \( \square \)

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

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

(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

\[
   Z_p(1v, w) = Z_p(v, w 1).
\]

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

\[
   \tilde{Z}_p(v, w) = \sum_{(w', w'') \in Y_0(w)} Z_p(vw', w'').
\]

**Proposition 3.4.** Let \( v, w \in W \). We then have

1. \( \tilde{Z}_p(v 1, w) = \tilde{Z}_p(v, 1w) \),
2. \( \tilde{Z}_p(1v, w) = \tilde{Z}_p(v, w 1) \),
3. \( \tilde{Z}_p(v, e) = 0 \).

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

3.3.4. The algorithm. Let \( \tilde{Z} : \tilde{B} \to \mathbb{Q}_p \) be the ring homomorphism defined as follows: for \( (v, w) \in W \times W \), the homomorphism \( \tilde{Z} \) sends \( \tilde{X}_{v, w} \) to \( \tilde{Z}_p(v, w) \). It follows from Proposition 3.4 that the homomorphism \( \tilde{Z} : \tilde{B} \to \mathbb{Q}_p \) factors through the projection \( \tilde{B} \to B \). 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
\begin{equation}
\sum_{\ell(v) \geq \ell(w) \text{ and } v \neq w} a_{v} x^{v} = \sum_{n \geq 0} a_{n} x^{n} \in \mathbb{Q}_{p}[x].
\end{equation}

(1) If \( \ell(v) \geq \ell(w) \) and \( v \neq w \), then we have \( b_{w} = 0 \).

(2) We have \( b_{w} = 1 \).

(3) If \( v \notin W_{1} \), then we have \( Z(b_{v}) = 0 \).

(4) We have

\begin{equation}
p^{-\ell(w)}\zeta_{p}(k(w)) = \sum_{v \in W_{1} \setminus W} Z_{p}(b_{v})\zeta_{p}(k(v)).
\end{equation}

By using this theorem, we can inductively compute \( \zeta_{p}(k) \).

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 \( b'_{w} = 0 \).
2. We have \( b'_{w} = 1 \).
3. If \( v \notin W_{1} \), then we have \( Z(b'_{v}) = 0 \).
4. We have

\begin{equation}
p^{-\ell(w)}\zeta_{p}(k(w)) = \sum_{v \in W_{1} \setminus W} Z_{p}(b'_{v})\zeta_{p}(k(v)).
\end{equation}

We can inductively compute \( \zeta_{p}(k) \) also by using this theorem. It seems that the latter algorithm is more effective.

**References**


**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 \( | \cdot |_{p} \) on \( \mathbb{Q}_{p} \) can be uniquely extended to an absolute value on \( \overline{\mathbb{Q}}_{p} \), which we denote by the same symbol \( | \cdot |_{p} \).

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 \( \zeta \in \mathbb{Q}_{p}^{*} \). 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 \(w^* = w_k \cdots w_1\) the word obtained by reversing the order of \(w\). For two words \(v, w\), we let \(\text{Sh}(v, w)\) denote the multiset of shuffles of \(v\) and \(w\).

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

\[ S_i(w) = \{ j \in \{1, \ldots, k\} \mid w_j = i \}. \]

We denote by \(M_w\) the set of \((k + 1)\)-tuples \((m_1, \ldots, m_{k+1})\) 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:

\[
L_w(z) = \sum_{(m_1, \ldots, m_{k+1}) \in M_w} \prod_{j \in S_2(w)} C_{p, m_j - m_{j+1}} \frac{z^{m_{k+1}}}{m_1 \cdots m_{k+1}}.
\]

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

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

\[
Z(\mathbb{K}(w)) = \frac{1}{p} \sum_{\xi \in \mu_p} L_w(1 - \xi).
\]

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 \(w^*\) with the letter 2. Recall that we have defined in Section 3.3.3 the \(p\)-adic number \(Z_p(v, w)\) to be

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


Proposition A.1. For any word \(w\) of letters 1, 2 and for any \(\zeta \in \mu_p\), we have \(L_w(1 - \zeta) = 0\).

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 \(\alpha \in \mathbb{T}_p\) 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 \(f_w \in \mathbb{R}\) satisfying \(f_w(0) = 0\) and \(L_w(z) = f_w(q(z))\).

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

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

Proof of Lemma A.2. If $w = e$ is an empty word, then $L_w = -q(z)$ 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 $L_{w'}(z) = f_{w'}(q(z))$. Let us write $f_w(z) = \sum_{n \geq 1} a_n z^n$.

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

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

Hence we have $L_w(z) = f_w(q(z))$ where

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

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

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

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

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

Since

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

we have

$$\sum_{\zeta \in \mu_p} \frac{t - 1}{t - (1 - \zeta)} = \sum_{\zeta = 1}^{p-1} \frac{e^{q(t)}}{e^{q(t)} - \zeta}.$$

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

$$= \sum_{k \geq 0} (-p)^k B_k \frac{k!}{k!} q(t)^{k-1}.$$
Lemma A.4. This follows from Proposition A.1 and Lemma A.3 by induction of the length of $w$.

Proof. II(1)

Here in the summand we set $e_k = 10 S. YASUDA$

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 $Z(K(w)) = 0$. Let us write $w = w'2$. By definition $Z(K(w))$ is equal to the sum

$$\frac{1}{p} \sum_{\zeta \mu_p} L_w(1 - \zeta).$$

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 $S = \{1, 2\} \cap \{1 - \zeta \mid \zeta \in \mu_p\}$. When $p = 2$, we distinguish $2 \in \{1, 2\}$ with $1 - (-1)$. For $\alpha \in S$, we set

$$\omega_\alpha = \left\{ \begin{array}{ll}
\frac{d}{dx} & \text{if } \alpha = 1, \\
\frac{1}{p} \sum_{\zeta \mu_p} \omega_{1 - \zeta} & \text{if } \alpha = 1 - \zeta \text{ for some } \zeta \in \mu_p, \\
\omega_{1 - \zeta} & \text{if } \alpha = 2.
\end{array} \right.$$

Let $\log_p : \nu_p^\times \to \mathbb{Q}$ denote the branch of $p$-adic logarithm characterized by $\log_p(2) = 0$. For a word $\alpha = \alpha_1 \cdots \alpha_k$ of letters in $S$ and for $\beta \in S$ we let $\tilde{\Pi}(\alpha, \beta)$ denote the regularized iterated integral

$$\tilde{\Pi}(\alpha, \beta) = \int_0^\beta \omega_{\alpha_k} \circ \cdots \circ \omega_{\alpha_1}$$

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

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 $L_w(1 - \zeta)$ is equal to the sum

$$\sum_{r \geq 1} \frac{(-1)^{r-1}}{p^{r-1}} \sum_{(w^{(1)}, \ldots, w^{(r)}) \in D_r(w)} \tilde{\Pi}(1w^{(1)}, 1 - \zeta_1) \prod_{j=2}^r \tilde{\Pi}((1 - \zeta_{j-1})w^{(j)}, 1 - \zeta_j).$$

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 $\tilde{\Pi}(1w, 1 - \zeta) = 0$.

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 \( w = 2 \cdots 2 \) for some \( k \geq 0 \). Then for any \( \zeta \in \mu_p \), we have
\[
\tilde{\Pi}(w, 1 - \zeta) = T^k/k!.
\]

2. Suppose that \( w \) contains the letter 1. Then for any \( \zeta \in \mu_p \) we have \( \tilde{\Pi}(w, 1 - \zeta) = 0 \).

Proof. The claim (1) can be checked directly. We prove the claim (2). Let us write \( w \) as \( w = 2w' \) 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 \( k \geq 1 \), and that \( w = 2w' \) for some \( v \). By induction hypothesis we have \( \tilde{\Pi}(w', 1 - \zeta) = 0 \). By applying the shuffle product formula to \( \tilde{\Pi}(w', 1 - \zeta) \tilde{\Pi}(2, 1 - \zeta) = 0 \) and by using induction hypothesis, we have \( \tilde{\Pi}(w, 1 - \zeta) = 0 \).

\[ \square \]

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

\[ \sum_{r \geq 1} \frac{1}{2^{r-1}} \sum_{(v^{(1)}, \ldots, v^{(r)}) \in D_r(v''1)} \sum_{(w^{(1)}, \ldots, w^{(r)}) \in Sh(v''1, w^{(1)})} \left( \frac{\Pi((w^{(1)})^{\leftrightarrow}1v^{(1)}, 1 - \zeta_1)}{\times \prod_{j = 2}^{r} \Pi((w^{(j)})^{\leftrightarrow}(1 - \zeta_{j-1})v^{(j)}, 1 - \zeta_j)} \right). \]

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

\[
\sum_{r \geq 1} \frac{(-1)^{r-1}}{2^{r-1}} \sum_{(v^{(1)}, \ldots, v^{(r)}) \in D_r(v''1)} \sum_{(w^{(1)}, \ldots, w^{(r)}) \in Sh(v''1, w^{(1)})} \sum_{(\zeta_1, \ldots, \zeta_r) \in \mu_p} \left( \Pi((1w^{(1)}), 1 - \zeta_1) \times \prod_{j = 2}^{r} \Pi((1 - \zeta_{j-1})w^{(j)}, 1 - \zeta_j) \right). \]

Let us write \( w^{(j)} = w^{(j)}_{k_1} \cdots w^{(j)}_{k_l} \). By the shuffle product formula we have

\[ \sum_{w^{(1)} \in Sh(v''1, w^{(1)})} \Pi(1w^{(1)}, 1 - \zeta_1) \]

\[ = \sum_{i = 0}^{k_1} (-1)^i \Pi(w^{(1)}_{1} \cdots w^{(1)}_{i} 1v^{(1)}, 1 - \zeta_1) \Pi(w^{(1)}_{i+1} \cdots w^{(1)}_{k_1}, 1 - \zeta_i), \]

and

\[ \sum_{w^{(j)} \in Sh(v^{(j)}, w^{(j)})} \Pi((1 - \zeta_{j-1})w^{(j)}, 1 - \zeta_j) \]

\[ = \sum_{i = 0}^{k_1} (-1)^i \Pi(w^{(j)}_{1} \cdots w^{(j)}_{i} (1 - \zeta_{j-1})v^{(j)}, 1 - \zeta_j) \Pi(w^{(j)}_{i+1} \cdots w^{(j)}_{k_1}, 1 - \zeta_j) \]

for \( j = 2, \ldots, r \).

Hence by Lemma A.5, we have

\[ \sum_{w^{(1)} \in Sh(v''1, w^{(1)})} \Pi(1w^{(1)}, 1 - \zeta_1) = (-1)^{k_1} \Pi((w^{(1)})^{\leftrightarrow}1v^{(1)}, 1 - \zeta_1), \]

and

\[ \sum_{w^{(j)} \in Sh(v^{(j)}, w^{(j)})} \Pi((1 - \zeta_{j-1})w^{(j)}, 1 - \zeta_j) = (-1)^{k_1} \Pi((w^{(j)})^{\leftrightarrow}(1 - \zeta_{j-1})v^{(j)}, 1 - \zeta_j), \]
for $j = 2, \ldots, r$. 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

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

and denote by $\Pi(w, \alpha, \beta)$ the constant term of $\tilde{\Pi}(w, \alpha, \beta)$.

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

$$-\sum_{r \geq 1} \frac{1}{p^{r-1}} \sum_{\substack{w(1) \cdots w(r) \in D_2(w'')}} \sum_{\xi_1 \cdots \xi_r \in \mu_p} \left( \Pi((w(1))^{\ast}, 1v^{(1)}, 1 - \zeta_1) \times \prod_{j=2}^r \Pi((w(j))^{\ast}, (1 - \zeta_{j-1})v^{(j)}, 1 - \zeta_j) \right).$$

Remark A.8. The sum in Corollary A.7 is easier to calculate than that in Proposition A.6, since $\Pi(w', 1v^{(1)}, 1 - \zeta_1)$ and $\Pi(w', (1 - \zeta_{j-1})v^{(j)}, 1 - \zeta_j)$ 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

$$\Pi((w(1))^{\ast}1v^{(1)}, 1 - \zeta_1) = \Pi((w(1))^{\ast}, 1v^{(1)}, 1 - \zeta_1)$$

and

$$\Pi((w(j))^{\ast}, (1 - \zeta_{j-1})v^{(j)}, 1 - \zeta_j) = \Pi((w(j))^{\ast}, (1 - \zeta_{j-1})v^{(j)}, 1 - \zeta_j)$$

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

(S. Yasuda) Department of Mathematics, Osaka University, Toyonaka, Osaka 560-0043, Japan

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