Centrum voor Wiskunde en Informatica

REPORT*RAPPORT*

The Leibniz-Hopf algebra and Lyndon words

M. Hazewinkel

Department of Analysis, Algebra and Geometry

AM-R9612 September 30, 1996

Report AM-R9612
ISSN 0924-2953

CWI
P.O. Box 94079
1090 GB Amsterdam
The Netherlands

The Leibniz-Hopf Algebra and Lyndon Words*

Michiel Hazewinkel
CWI
P.O. Box 94079, 1090 GB Amsterdam, The Netherlands
e-mail: mich@cwi.nl

Abstract

Let $\mathcal{Z}$ denote the free associative algebra $\mathbb{Z}\langle Z_1, Z_2, \ldots\rangle$ over the integers. This algebra carries a Hopf algebra structure for which the comultiplication is $Z_n \mapsto \Sigma_{i+j=n} Z_i \otimes Z_j$. This the noncommutative Leibniz-Hopf algebra. It carries a natural grading for which $gr(Z_n) = n$. The Ditters-Scholtens theorem says that the graded dual, $\mathcal{M}$, of $\mathcal{Z}$, herein called the overlapping shuffle algebra (on the semigroup of natural numbers), is the free commutative polynomial algebra over $\mathbb{Z}$ with as polynomial generators certain words which are called elementary unreachable words (EUW). In this note unreachable words are shown to be precisely the (concatenation) powers of Lyndon words. More precisely it is shown that the block decomposition algorithm of [4] is in fact an algorithm for obtaining the Chen-Fox-Lyndon factorization of a word into decreasing Lyndon words. Further links are discussed between the shuffle algebra and the overlapping shuffle algebra.

AMS Subject Classification (1991): 16W30, 05A99, 17B01
Keywords & Phrases: Hopf algebra, Leibniz-Hopf algebra, Ditters-Scholtens theorem, shuffle algebra, Lyndon word, free Lie algebra, Chen-Fox-Lyndon theorem.

1. Introduction and statement of results

Let $\mathcal{Z} = \mathbb{Z}\langle Z_1, Z_2, \ldots\rangle$ be the free associative algebra over the integers in the (noncommuting) indeterminates $Z_1, Z_2, \ldots$. With $\varepsilon(Z_i) = 0$, $i = 1, 2, \ldots$, the comultiplication

$$\mu(Z_n) = \sum_{i+j=n} Z_i \otimes Z_j \tag{1.1}$$

where $Z_0 = 1$, and the antipole

$$\iota(Z_n) = \sum_{i_1+\ldots+i_k} (-1)^k Z_{i_1} Z_{i_2} \ldots Z_{i_k} \tag{1.2}$$

where the sum is over all strings $i_1, i_2, \ldots i_k$, $i_j \in \mathbb{N}$, such that $i_1 + i_2 + \ldots + i_k = n$, the algebra $\mathcal{Z}$ becomes a Hopf algebra. This is the *noncommutative Leibniz-Hopf algebra.* It is of course cocommutative.

Giving Z_n degree n turns $\mathcal{Z}$ into a graded Hopf algebra and in particular a cocommutative coalgebra, whose homogeneous components are finite dimensional free $\mathbb{Z}$-modules. Its graded dual, $\mathcal{M}$, is hence an algebra over $\mathbb{Z}$. The Ditters-Scholtens theorem, proved in [4], says that as an algebra $\mathcal{M}$ is a free commutative polynomial algebra on certain generators which are (indexed by) certain words over the alphabeth $\mathbb{N} = \{1, 2, \ldots\}$ which are called elementary unreachable words (EUW).

It is a main purpose of this note to point out that these are precisely the concatenation powers of elementary Lyndon words (see below for a definition of EUW and Lyndon word). At this point I would like to thank Guy Melançon, who first suggested that EUW's should have something to do with Lyndon words when I lectured on the Ditters-Scholtens theorem in early December 1995 at LABRI, Univ. de Bordeaux I.

*Work done while visiting LABRI, Univ. de Bordeaux I, Talence, France, in Dec. 1995 with partial support from LABRI.

I like to call $\mathcal{M}$ the *overlapping shuffle algebra* in analogy with the well known shuffle algebra which is obtained as follows.

Let $\mathcal{U} = \mathbb{Z}\langle U_1, U_2, \ldots\rangle$ be the free associative algebra over the integers in the (noncommuting) indeterminates $U_1, U_2, \ldots$. This time take

$$\begin{aligned} &\epsilon(U_i) = 0, \quad i = 1, 2, \ldots \\ &\mu(U_i) = 1 \otimes U_i + U_i \otimes 1 \\ &\iota(U_i) = -U_i \end{aligned} \tag{1.3}$$

to make $\mathcal{U}$ into a graded Hopf algebra. The graded dual of $\mathcal{U}$, as a coalgebra, is the socalled shuffle algebra, $\mathcal{S}$, over $\mathbb{Z}$. It is a well-known theorem that over $\mathbb{Q}$, $\mathcal{S}$ becomes a free commutative polynomial algebra with generators that are (indexed by) Lyndon words, see e.g. [3], Cor. 5.5, p. 111. This is definitely not true over $\mathbb{Z}$, that is, $\mathcal{S}$ is not free polynomial over $\mathbb{Z}$. And thus the overlapping shuffle algebra $\mathcal{M}$ can be seen as a rather nicer version of the shuffle algebra $\mathcal{S}$. For, indeed, over $\mathbb{Q}$ they become isomorphic, the isomorphism being determined by writing down the identity

$$1 + Z_1 t + Z_2 t^2 + \ldots = \exp(U_1 t + U_2 r^2 + \ldots) \tag{1.4}$$

where t is a counting variable that commutes with everything. Thus the Ditters-Scholtens theorem implies the shuffle algebra theorem (without explicitely specifying a set of generators for the latter).

The proof of the Ditters-Scholtens theorem by Astrid Scholtens in [4] rests on an algorithm called the block decomposition algorithm. A main result of the present note is that this algorithm is in fact an algorithm for the finding of the Chen-Fox-Lyndon factorization of a word into decreasing Lyndon words. It also seems to me to be a very efficient algorithm for doing so, much better than the standard algorithm. This, however, remains to be sorted out.

The identification of elementary unreachable words with powers of Lyndon words is an immediate consequence of the theorem that the block decomposition algorithm gives the Chen-Fox-Lyndon factorization.

2. Block decompositions

This section describes the block decomposition algorithm of [4]., which is the main tool for the proof of the Ditters-Scholtens theorem in [4].

Consider words in $\mathbb{N}$ and give $\mathbb{N}$ its natural ordering.

2.1 Lexicographical ordening on $\mathbb{N}^*$

Let $v = a_1 a_2 \ldots a_r$, $w = b_1 b_2 \ldots b_s$ be two elements of $\mathbb{N}^*$, i.e. two words in the alphabeth $\mathbb{N}$. Then $v < w$ (lexicographically ordering) iff there is a $k \geq 1$ such that $a_1 = b_1, \ldots, a_{k-1} = b_{k-1}$, $a_k < b_k$, where nothing is less than any $a \in \mathbb{N}$. Thus for example $1,1,2 < 1,1,3$ and $1,1 < 1,1,1$.

2.2 Block decomposition algorithm

Consider a nonempty word $w = a_1 a_2 \ldots a_r$. Let t be such that $a_1 = a_2 = \ldots = a_t \neq a_{t+1}$. Let $s \geq t$ be such that $a_{t+1} > a_1, \ldots, a_s > a_1$, $a_{s+1} \leq a_1$. Then the first level 1 block of w is $a_1 a_2 \ldots a_s$. Now consider the suffix $a_{s+1} \ldots a_r$ of w and repeat the procedure. This produces the level one block decomposition of w

$$w = b_1^{(1)} b_2^{(1)} \ldots b_{r_1}^{(2)}.$$

Now treat w as a word made up out of the symbols $b_1^{(1)}, \ldots, b_{r_1}^{(2)}$ with the lexicographic ordering described above and repeat the procedure to obtain the level two block decomposition

$$w = b_1^{(2)} b_2^{(2)} \ldots b_{r_2}^{(2)}.$$

Write $a_i = b_i^{(0)}$, $r = r_0$. Note that $r_{i+1} \leq r_i$ and that if $r_{i+1} = r_i$ then $b_j^{(i+1)} = b_j^{(i)}$, $j = 1, \ldots, r_i$. Thus after some time the procedure stops. The smallest i for which $r_{i+1} = r_i$ is the *complexity* of w, and the final stabilized decomposition of w

$$w = b_1^{(c)} b_2^{(c)} \ldots b_{r_c}^{(c)}, \quad c = \text{complexity } (w)$$

is the *block decomposition* of w.

For example 3,2,1 has complexity zero and block decomposition $b_1^{(c)} = 3$; $b_2^{(c)} = 2$; $b_3^{(c)} = 1$. Here is another example

level 0 $\quad w = 1,1,3,\ 1,1,3,\ 1,1,4,\ 1,1,2,\ 1,1,2,\ 1,1,\ 1,2,2,\ 1,1,4,\ 1,2,2,3,\ 1,1,1,1$

level 1 $\quad w = (1,1,3)(1,1,3)(1,1,4)(1,1,2)(1,1,2)(1,1,1,2,2)(1,1,4)(1,2,2,3)(1,1,1,1)$

level 2 $\quad w = (1,1,3,\ 1,1,3,\ 1,1,4)(1,1,2,\ 1,1,2)(1,1,1,2,2,\ 1,1,4,\ 1,2,2,3)(1,1,1,1,)$

and this is the block decomposition of w, which hence has complexity 2.

2.3 Elementary unreachable words

A nonempty word $w = a_1 a_2 \ldots a_r$ is elementary if the greatest common divisor of $a_1, \ldots, a_r$ is 1. The nonempty word w is unreachable if its (final) block decomposition consists of one block.

2.4 Lyndon words

A *strict suffix* of a nonempty word $w = a_1 \ldots a_r$ is a word $a_i \ldots a_r$, $1 < i \leq r$. A *Lyndon word* is a word w such that $w < v$ for each strict suffix v of w.

A central theorem about Lyndon words is the *Chen-Fox-Lyndon theorem*, [1], which says that every word w has a unique factorization in decreasing Lyndon words $u_1, \ldots, u_s$.

$$w = u_1 u_2 \ldots u_s, \quad u_i \geq u_{i+1},\ i = 1, \ldots, s-1.$$

As will be shown in section 4 the blocks $b_1^{(c)}, \ldots, b_r^{(c)}$ of the block decomposition of w are (concatenation) powers of Lyndon words, $b_i^{(c)} = v_i^{*s_i} = v_i v_i \ldots v_i$ (s_i factors) and $v_i > v_{i+1}$, $i = 1, \ldots, r-1$. Thus the block decomposition algorithm of [4] is a (left to right) algorithm for obtaining the Chen-Fox-Lyndon factorization of a word. (The standard algorithm is right to left). It also looks like the block algorithm is a much more efficient algorithm but that still needs to be sorted out in detail.

3. Overlapping shuffle algebra

As in the introduction, let $\mathcal{M}$ be the graded dual of $\mathcal{Z} = \mathbb{Z}\langle Z_1, Z_2, \ldots \rangle$. As an Abelian group $\mathcal{M}$ has as basis all words over $\mathbb{N}$ where

$$\langle w, Z_{i_1} Z_{i_2} \ldots Z_{i_r} \rangle = \begin{cases} 1 & \text{if} \quad w = i_1 i_2 \ldots i_r \\ 0 & \text{otherwise} \end{cases} \tag{3.1}$$

and the empty word is 1 on $Z_0 = 1 \in \mathcal{Z}$ and zero on all nontrivial monomials in the Z_i. The comultiplication on $\mathcal{Z}$ induces a multiplication on $\mathcal{M}$, the *overlapping shuffle product.* Explicitely the overlapping shuffle products looks as follows. Let $v = a_1 \ldots a_r$, $w = b_1 \ldots b_s$ be two elements of $\mathbb{N}^*$, i.e. two basis elements of $\mathcal{M}$. Then the overlapping shuffle product of v and w is equal to

$$v \otimes_{osh} w = \sum_{f,g} c_1 c_2 \ldots c_t \tag{3.2}$$

where the sum is over all t and pairs of maps $f : \{1, \ldots, r\} \to \{1, \ldots, t\}$ $g : \{1, \ldots, s\} \to \{1, \ldots, t\}$ such that f and g are order preserving and injective and $Im(f) \cup Im(g) = \{1, \ldots, t\}$, and where

$$c_i = a_{f^{-1}(i)} + b_{g^{-1}(i)}, \quad i = 1, \ldots, t \tag{3.3}$$

with $a_{f^{-1}(i)} = 0$ if $f^{-1}(i) = \emptyset$ and similarly for $b_{g^{-1}(i)}$.

The Ditters-Scholtens theorem now says that the overlapping shuffle algebra $\mathrm{OSH}(\mathbb{N}) = \mathcal{M} = \oplus_w \mathbb{Z}w$ with this multiplication is the free commutative polynomial algebra over $\mathbb{Z}$ with as polynomial generators the elementary unreachable words: $\mathcal{M} = \mathbb{Z}[w : w \in EUW]$.

The shuffle algebra $\mathrm{Sh}(\mathbb{N}) = S$ also has the words over $\mathbb{N}$ as basis, but the multiplication differs

$$v \otimes_{sh} w = \sum_{f,g} c_1 c_2 \dots c_{r+s} \tag{3.4}$$

where f, g and c_i are as before. The difference is that t is required to be equal to $r + s$ so that each c_i is equal to an a_j or b_k.

Obviously a shuffle algebra $\mathrm{Sh}(A)$ can be defined for any alphabeth A instead of $\mathbb{N}$.

Similarly an overlapping shuffle algebra $\mathrm{OSh}(S)$ is defined for any semigroup S. A basis of $\mathrm{OSh}(S)$ as a free abelian group over $\mathbb{Z}$ is formed by S^*, the words over S. The multiplication is given by (3.2) and (3.3) with in (3.3) the "+" replaced by the multiplication in S. I have done some preliminary exploratory calculations on $\mathrm{OSh}(S)$, expecially in the case that S is a free semigroup. It looks like the $\mathrm{OSh}(S)$ will well repay further study.

4. Chen-Fox-Lyndon factorization

In this section is shown that the block decomposition of a word in fact yields the Chen-Fox-Lyndon factorization.

4.1. Lemma. Let $u, v \in \mathbb{N}^*$ be two Lyndon words and $u < v$ (lexicographically) then uv is a Lyndon words.

This is a known lemma, cf. e.g. [3], p. 106 or [2], p. 6. A slight extension is:

4.2. Lemma. Let $u_1 \le \dots \le u_n$ be Lyndon words and let $u_1 < u_n$. Then $u_1 u_2 \dots u_n$ is Lyndon.

Proof. With induction on n, the case $n = 2$ being taken care of by lemma 4.1. Now let $n > 2$.

If $u_2 < u_n$, then $u_2 \dots u_n$ is Lyndon by induction and $u_1 \le u_2 < u_2 \dots u_n$ so that $u_1 \dots u_n$ is Lyndon by lemma 4.1.

If $u_2 = \dots = u_n$, then $u_1 u_2$ is Lyndon by lemma 4.1 and $u_1 u_2 < u_2 = u_3 \le u_3 \dots u_n$ and so $u_1 u_2 \dots u_n$ is Lyndon by lemma 4.1.

4.3. Lemma. Let u, v be two Lyndon words and suppose that $u^{*r} \le v^{*s}$ for some $r, s \in \mathbb{N}$. Then $u \le v$.

Proof. There are three cases to distinguish.

Case 1. $\mathrm{length}(u) = \mathrm{length}(v)$. Let $u = a_1 \dots a_m$, $v = b_1 \dots b_m$. Now suppose that $u^{*r} \le v^{*s}$. There are two possibilities : (i) $a_1 = b_1, \dots, a_m = b_m$ (the first inequality of $u^{*r} \le v^{*s}$ shows up after m); (ii) $a_1 = b_1, \dots, a_{k-1}$, $a_k < b_k$, $k \le m$, the first inequality shows up at or before m.

In the first case we have $u = v$ (and $r \le s$). In the second case $u < v$.

Case 2. $\mathrm{length}(u) < \mathrm{length}(v)$, $u = a_1 \dots a_m$, $v = b_1 \dots b_n$, $m < n$. Again it could happen that $a_1 = b_1, \dots, a_m = b_m$ (the first inequality of $u^{*r} < v^{*s}$ shows up after m) and then $v = ub_{m+1} \dots v_n > u$. Or it could happen that $a_1 = b_1, \dots, a_{k-1} = b_{k-1}$, $a_k < v_k$ for $k \le m$ and then also $u < v$.

Case 3. $\mathrm{length}(u) > \mathrm{length}(v)$, $u = a_1 \dots a_m$, $v = b_1 \dots b_n$, $m > n$. Write $m = kn + t$, with $0 \le t \le n - 1$. Then

$$u = a_1 \dots a_n a_1^{(2)} \dots a_n^{(2)} \dots a_1^{(k)} \dots a_n^{(k)} a_1^{(k+1)} \dots a_t^{(k+1)}$$

$$v = b_1 \dots b_n$$

Now if $b_1 \dots b_n < a_1 \dots a_n$, then definitely not $u^{*r} \le v^{*s}$. Therefore $a_1 \dots a_n \le b_1 \dots b_n$. If $a_n \dots a_n <$

$b_1 \dots b_n$ also $u < v$ and we are through. There remains the case that $a_1 \dots a_n = b_1 \dots b_n$. Then necessarily $s \geq 2$ and

$$a_1^{(2)} \dots a_n^{(2)} \dots a_1^{(k)} \dots a_n^{(k)} a_1^{(k+1)} \dots a_t^{(k+1)} \dots \leq b_1 \dots b_n \dots$$

This implies that $a_1^{(2)} \dots a_n^{(2)} \leq b_1 \dots b_n$. If $a_1^{(2)} \dots a_n^{(2)} < b_1 \dots b_n = a_1^{(1)} \dots a_n^{(1)}$ then the suffix $a_1^{(2)} \dots a_n^{(2)} \dots a_t^{(k+1)} < a_1^{(1)} \dots a_n^{(1)} \dots a_t^{(k+1)} = u$ which would contradict that u is Lyndon. Hence $a_1^{(2)} \dots a_n^{(2)} = b_1 \dots b_n$. Continuing in this way we see that

$$a_1^{(1)} a_2^{(1)} \dots a_n^{(1)} = a_1^{(2)} \dots a_n^{(2)} = \dots = a_1^{(k)} \dots a_n^{(k)} = b_1 \dots b_n$$

and

$$a_1^{(k+1)} \dots a_t^{(k+1)} a_1^{(1)} \dots a_{n-t}^{(1)} \dots \leq b_1 \dots b_t b_{t+1} \dots b_n \dots, \quad t < n$$

It follows that $a_1^{(k+1)} \dots a_t^{(k+1)} \leq b_1 \dots b_t = a_1^{(1)} \dots a_t^{(1)}$. If $a_1^{(k+1)} \dots a_t^{(k+1)} < b_1 \dots b_t$, u would not be Lyndon. Hence $a_1^{(k+1)} \dots a_t^{(k+1)} = b_1 \dots b_t$. Thus u is of the form $u = v^{*k}\rho$ where ρ is a strict prefix of v, or empty. If ρ is not empty $\rho < v < v^{*k}\rho = u$ contradicting that u is Lyndon (because ρ is a strict suffix of u). Hence ρ is empty and $u = v^{*k}$. But u is Lyndon and no power ≥ 2 of a word can be Lyndon. Hence in this case $k = 1$ and $u = v$. □

4.4. Remark. The lemma still holds if v is not necessarily Lyndon. Indeed the proof did not use that v is Lyndon.

4.5. Theorem. *The block decomposition algorithm of section 2 yields the Chen-Fox-Lyndon factorization. More precisely, for a nonempty word $w \in \mathbb{N}^*$*

(i) *All blocks formed during the block decomposition algorithm are (concatenation) power of Lyndon words*

(ii) *If $w = b_1^{(c)} \dots b_r^{(c)}$, $b_i^{(c)} = u_i^{*r_i}$, is the block decomposition of w, then $u_1 > u_2 > \dots > u_r$.*

Proof. With induction. At level zero all blocks are single letters and hence Lyndon. Now if b is a block at level $i+1$, then b is of one of the forms

$$b = c_1 \dots c_r, \qquad c_1 = c_2 = \dots = c_r$$

$$b = c_1 \dots c_k \dots c_r, \quad c_1 = \dots = c_k, c_{k+1} > c_1, \dots, c_r > c_1, r > k$$

where in both cases all the c_i are Lyndon words. In the first case b is a power of a Lyndon word. In the second case b is a Lyndon word by lemma 4.2. This proves (i). Now let

$$w = b_1^{(c)} \dots b_r^{(c)}, \quad b_i^{(c)} = u_i^{*r_i} \tag{4.5}$$

be the block decomposition of w. By (i), $b_i^{(c)}$ is the power of a Lyndon word u_i. Because this is the (final) block decomposition

$$b_1^{(c)} > b_2^{(c)} > \dots > b_r^{(c)}$$

and it now follows from lemma 4.3 that $u_1 > u_2 > \dots u_r$ proving (ii) and that

$$w = u_1^{*n_1} \dots u_r^{*n_r}$$

is the Chen-Fox-Lyndon factorization of w (which is know to be unique). □

4.7. Corollary. *A word is unreachable if and only if it is a power of a Lyndon word. A word is elementary unreachable if and only if it is a power of an elementary Lyndon word.*

4.8. Remark. There is a very natural bijection between the set of Lyndon words and the set of elementary unreachable words (i.e. the powers of elementary Lyndon words.) It is given by

$$a_1 \dots a_r \mapsto ((a_1/d) \dots (a_r/d))^{*d}$$

where d is the greatest common divisor of $a_1, \dots, a_r$.

5. Comparing $\mathcal{U}$ and $\mathcal{Z}$ over $\mathbb{Q}$

Over the rational numbers the Hopf algebras $\mathcal{U}$ and $\mathcal{Z}$ become isomorphic. To see this consider the identity

$$1 + Z_1 t + Z_2 t^2 + \dots = \exp(U_1 t + U_2 t^2 + \dots) \tag{5.1}$$

The explicit formula for Z_n in terms of the U_i is

$$Z_n = \sum_{\substack{i_1 + \dots + i_k = n \\ i_j \in \mathbb{N}}} \frac{U_{i_1} U_{i_2} \dots U_{i_k}}{k!} \tag{5.2}$$

5.3. Theorem. *Define $\phi : \mathcal{Z}_{\mathbb{Q}} \to \mathcal{U}_{\mathbb{Q}}$ by (5.3), i.e. $\phi(Z_n)$ is equal to the right hand side of (5.2). Then ϕ is an isomorphism of Hopf algebras.*

Proof. Because $\mathcal{Z}$ is free, ϕ certainly defines a unique homomorphism of algebras. It is also degree preserving and $\phi(Z_n) \equiv U_n \bmod(U_1, \dots, U_{n-1})$ so that ϕ is an isomorphism. Further ϕ respects the augmentation ε. It remains to show that ϕ respects the comultiplication (it is then automatic in this case that ϕ respects the antipode). Thus it remains to show that if $\mu(U_i) = 1 \otimes U_i + U_i \otimes 1$ is applied to (the right hand side) of (5.2) then the result is $\Sigma_{i+j=n} \phi(Z_i) \otimes \phi(Z_j)$. Now

$$\mu(U_{i_1} \dots U_{i_k}) = \sum U_{a_1} \dots U_{a_r} \otimes U_{b_1} \dots U_{b_s}$$

where $r + s = k$ and the $a_1, \dots, a_r; b_1, \dots, b_s$ are all pairs of complementary subsequences of $i_1, \dots, i_k$. In other words $i_1 \dots i_k$ is one of the terms of the shuffle product (or merge) of $a_1 \dots a_r$ and $b_1 \dots b_s$. It remains to figure out how many $i_1 \dots i_k$ there are that yield the term $U_{a_1} \dots U_{a_r} \otimes U_{b_1} \dots U_{b_s}$. This amounts precisely to choosing r places of k (where the $a_1, \dots, a_r$ are inserted in that order, and the $b_1, \dots, b_s$ are inserted in the remaining $k - r = s$ places in that order). This number is $\frac{k!}{r!s!}$. Hence

$$\mu(\phi(Z_n)) = \sum \frac{1}{k!} U_{a_1} \dots U_{a_r} \otimes U_{b_1} \dots U_{b_s} \left(\frac{k!}{r!s!}\right)$$

$$\sum \frac{U_{a_1} \dots U_{a_r}}{r!} \otimes \frac{U_{b_1} \dots U_{b_s}}{s!} = (\phi \otimes \phi)(\sum_{r+s=n} Z_r \otimes Z_s)$$

which proves what is desired.

Another way, more conceptual, but less immediately convincing to me, is as follows. Note that $U_i \otimes 1$ and $1 \otimes U_j$ are commuting variables in $\mathbb{Q}\langle U \rangle \otimes \mathbb{Q}\langle U \rangle$. Hence $A = (1 \otimes U_1)t + (1 \otimes U_2)t^2 + \dots$ and $B = (U_1 \otimes 1)t + (U_2 \otimes 1)t^2 + \dots$ are commuting elements in $\mathbb{Q}\langle U \rangle \otimes \mathbb{Q}\langle U \rangle[t]$. Hence $\exp(A + B) = \exp(A)\exp(B)$ and the desired results follows by applying μ to (5.1).

5.4. Corollary. *The overlapping shuffle algebra $\mathcal{M} = \mathrm{OSh}(\mathbb{N})$ and the shuffle algebra $\mathcal{S} = \mathrm{Sh}(\mathbb{N})$ become isomorphic over $\mathbb{Q}$.*

If now follows as a corollary of the Ditters-Scholtens theorem that $S \otimes_{\mathbb{Z}} \mathbb{Q} = S_{\mathbb{Q}}$ is a free commutative polynomial algebra over $\mathbb{Q}$. This does not yet specify a set of polynomial generators for $S_{\mathbb{Q}}$. It is somewhat natural at this stage to suspect that the isomorphism given by theorem 5.3 recovers a correspondence like that of Remark 4.8 by taking suitable highest order terms.

References

1. K.T. Chen, R.H. Fox, R.C. Lyndon, Free differential calculus IV, *Ann. Math,* **68** (1958), 81–95.
2. M. Lothaire (ed.), Combinatorics on words, Chapter 5, Addison-Wesley, 1983.
3. Chr. Reutenauer, Free Lie algebras, Oxford UP, 1993.
4. A.C.J. Scholtens, S-typical curves in non-commutative Hopf algebras, thesis, Free Univ. of A'dam, March 1996.