Kragujevac J. Math. 30 (2007) 315–326.

HOPF ALGEBRAS OF WORDS AND OVERLAPPING SHUFFLE ALGEBRA Olivera Marković

Faculty of Education, University of Kragujevac, 31000 Užice, Trg Svetog Save 36, Serbia

(Received October 30, 2006)

Abstract. In this paper we consider the free Z-module generated by finite words in a certain alphabet and three multiplications on such modules and their dual comultiplications and we find which of these operations can be combined to obtain Hopf structures. We will direct a special attention on one of these structures, known as overlapping shuffle algebra and its properties.

WHAT IS HOPF ALGEBRA

Definition 1.1. An associative, unitary k-algebra is a pair (A, m), where A is a k-module and m $A \bigotimes A \to A$ is a k-linear map, called the multiplication, such that: 1. The following diagram is commutative:

$$\begin{array}{cccc} A \otimes A \otimes A & \stackrel{m \otimes id}{\longrightarrow} & A \otimes A \\ & & & \\ m \downarrow & & & \downarrow m \\ A \otimes A & \stackrel{m}{\longrightarrow} & A \end{array}$$

2. There exists k-linear map $u: k \to A$ such that the following diagrams commute:

where the maps $k \bigotimes A \to A$ and $A \bigotimes k \to A$ are the canonical ones. Such a u is necessarily unique. The first of these diagrams says that the algebra A is associative and the second gives the existence of a unit $u(1) = 1_A$ in A.

Definition 1.2. A coalgebra over k is a pair (C, Δ) , where C is a k-module and $\Delta : C \to C \bigotimes C$ is a k-linear map called the comultiplication, such that:

1. The following diagram commutes:

 $\begin{array}{ccc} C \otimes C \otimes C & \stackrel{\Delta \otimes id}{\longleftarrow} \\ id \otimes \Delta^{\uparrow} & \\ C \otimes C & \stackrel{\Delta}{\longleftarrow} \end{array}$

2. There exists a k-linear map ϵ : $C \rightarrow k$, such that the following diagrams commute:



The first of these diagrams expresses the so called coassociative property of the comultiplication. The map ϵ is called the counit and is uniquely determined by the pair (C, Δ) .

Definition 1.3. We say that a triple (A, m, Δ) is a bialgebra, if (A, m) is an algebra with unit u, (A, Δ) is a configebra with counit ϵ and $\Delta : A \to A \bigotimes A, \epsilon : A \to k$ are algebra maps.

In other words, algebra and coalgebra structures must be compatible. The compatibility is ensured by requiring either of the following equivalent conditions.

1. Δ and ϵ must be algebra morphisms.

and u must be coalgebra morphisms.

Definition 1.4. We say that a bialgebra (H, m, Δ) is a Hopf algebra if there exists a k-linear map $S : H \to H$, called the antipode, such that the following diagrams are commutative:

$H\otimes H$	$\stackrel{\Delta}{\longleftarrow}$	H	$\xrightarrow{\Delta}$	$H\otimes H$
$id \otimes S \downarrow$		$\downarrow u\epsilon$		
$H\otimes H$	$\overset{m}{\longrightarrow}$	H	$\stackrel{m}{\longleftarrow}$	$H\otimes H$

2. HOPF ALGEBRA OF WORDS

We consider the free Z-module generated by finite words in a certain alphabet and three multiplications on such modules and their dual comultiplications and we find which of these operations can be combined to obtain Hopf structures.

Given a set S, thought of as a collection of letters, we can form the free monoid \overline{WS} consisting of finite words in S, the monoidal operation being composition. Here it is assumed that a word has positive length and word will be denoted by $w = [a_1, \dots, a_n], a_i \in S$; we let WS denote the unital monoid obtained by adjoining to \overline{WS} a unique "empty word" of length 0 (which will give the unit and counit in the algebras and coalgebras we consider). Then we can take the free abelian groups $\mathbf{Z}\overline{WS}$ and $\mathbf{Z}WS$ generated by these monoids, the elements of these groups being \mathbf{Z} -linear combinations of words. Of course, $\mathbf{Z}WS = \mathbf{Z}\overline{WS} \oplus \mathbf{Z}$

We will restrict ourselves to the graded setting, so we assume that S is given a grading where every element has positive degree and only finitely many elements have the same degree. The degree of a word is defined to be the sum of the degrees of the letters that form it and so $\mathbb{Z}WS$ becomes graded and of finite type, i.e., the degree n part, $\mathbb{Z}WS_n$, of $\mathbb{Z}WS$, has finite rank. We can then form the graded dual $(\mathbb{Z}WS)^* = \bigoplus_n (\mathbb{Z}WS_n)^*$, and when we speak of duality we will always mean this graded duality. Each $\mathbb{Z}WS_n$ has an obvious basis, consisting of the words of degree n, and we give $(\mathbb{Z}WS_n)^*$ the dual basis, collating all of these to provide a basis for $(\mathbb{Z}WS)^*$. Of course, the elements of this dual basis are indexed by words, giving a \mathbb{Z} becomes $\mathbb{Z}WS$ and $(\mathbb{Z}WS)^*$.

The first multiplication we consider is "concatenation", which we denote by m_c . The concatenation product is determined by

$$m_c([s_1,\ldots,s_k]\otimes[t_1,\ldots,t_l])=[s_1,\ldots,s_k,t_1,\ldots,t_l],$$

where $s_1, \ldots, s_k, t_1, \ldots, t_l$ are elements of S. With this multiplication $\mathbf{Z}WS$ is the free associative algebra on S, i.e., the tensor algebra on the free abelian group $\mathbf{Z}S$ generated by S.

We note that m_c is clearly not commutative, for example $m_c([s_1] \otimes [s_2]) = [s_1, s_2] \neq m_c([s_2] \otimes [s_1]) = [s_2, s_1]$ for $s_1 \neq s_2 \in S$.

The dual of this is the "**chop**" comultiplication, given by

$$\Delta_c([s_1,\ldots,s_k]) = \sum_{i=0}^k [s_1,\ldots,s_i] \otimes [s_{i+1},\ldots,s_k]$$

The next multiplication that is of interest is the "shuffle product", which we denote by m_s . This is given by

$$m_s([s_1,\ldots,s_k]\otimes[t_1,\ldots,t_l])=\sum_{\sigma}\sigma([s_1,\ldots,s_k,t_1,\ldots,t_l]),$$

summed over all permutations σ , of k + l symbols, which satisfy

$$\sigma(1) < \sigma(2) < \dots \sigma(k), \quad \sigma(k+1) < \sigma(k+2) < \dots < \sigma(l),$$

the permutation σ shuffling the letters in the word in the obvios way. For example $m_s([1,2] \otimes [3,4,5]) = [1,2,3,4,5] + [1,3,2,4,5] + [1,3,4,2,5]$

+[4,3,4,5,2] + [3,1,2,4,5] + [3,1,4,2,5] + [3,1,4,2,5] + [3,1,4,5,2] + [3,4,1,2,5] + [3,4,1,5,2]

+[3, 4, 5, 1, 2]There will be $\binom{k+l}{k}$ such permutations. This is commutative; but over **Z** it is not free commutative (i.e., **Z**WS with this product is not a polynomial algebra).

The dual comultiplication, Δ_s , seems to have no established name, so we call it the "excision" coproduct since it is given by

$$\Delta_s([s_1,\ldots,s_k]) = \sum [s_{i_1},\ldots,s_{i_j}] \otimes C([s_{i_1},\ldots,s_{i_j}]),$$

summed over all subwords $[s_{i_1}, \ldots, s_{i_j}]$ of $[s_1, \ldots, s_k]$ (including the empty subword), where $C([s_{i_1}, \ldots, s_{i_j}])$ denotes the complementary subword, i.e., the word obtained by excising the subword $[s_{i_1}, \ldots, s_{i_j}]$. For example,

 $\Delta_s([1,2,3]) = [0] \otimes [1,2,3] + [1] \otimes [2,3] + [2] \otimes [1,3] + [3] \otimes [1,2]$ $+ [1,2] \otimes [3] + [1,3] \otimes [2] + [2,3] \otimes [1] + [1,2,3] \otimes [0]$ For the third multiplication we assume that S is the set of positive integers (although it could be defined for any non-unital monoid), where the degree of $n \in S$ is n. The multiplication, m_o , is the "**overlapping shuffle product**" defined by

$$m_o([s_1,\ldots,s_k]\otimes[t_1,\ldots,t_l])=\sum_f f([s_1,\ldots,s_k,t_1,\ldots,t_l])$$

where f inserts a number of 0s into $[s_1, \ldots, s_k]$ (as many as l), and inserts a number of 0s into $[t_1, \ldots, t_l]$ (as many as k), and then adds the first letters together, then the second, etc. The sum is over all such f for which the result contains no 0s. For example,

$$m_o([1,2] \otimes [3,4]) = [1,2,3,4] + [1,3,2,4] + [3,1,2,4] + [1,3,4,2] + [3,1,4,2] + [3,4,1,2] + [1,5,4] + [1,3,6] + [4,6] + [4,2,4] + [4,4,2] + [3,1,6] + [3,5,2] = m_S(1,2] \otimes [3,4]) + [1,5,4] + [1,3,6] + [4,6] + [4,2,4] + [4,4,2] + [3,1,6] + [3,5,2]$$

In general, the product of a length k word and a length l word will have

$$\sum_{i=0}^{n(k,t)} \binom{k+l-j}{k-j,l-j,j}$$

terms.

The dual comultiplication is the "Leibniz" coproduct, given by

mir

$$\Delta_{\mathbf{a}}([s_1, \dots, s_k]) = \sum_{i_1+j_1=s_1} \sum_{i_2+j_2=s_2} \dots \sum_{i_k+j_k=s_k} [i_1, \dots, i_k] \otimes [j_1, \dots, j_k]$$

where, in each summation, i_n and j_n are taken to be elements of $S \cup \{0\}$. In a word, 0 is read as a blank letter. For example if $i_2 = 0$, then $[i_1, i_2, i_3]$ is understood as the word $[i_1, i_3]$, etc., and if each i_n is 0, then $[i_1, \ldots, i_k]$ is the empty word. For example, $\Delta_o([2,3]) = [0] \otimes [2,3] + [1] \otimes [2,2] + [2] \otimes [2,1] + [3] \otimes [2]$

$$+[1] \otimes [1,3] + [1,1] \otimes [1,2] + [1,2] \otimes [1,1] + [1,3] \otimes [1]$$
$$+[2] \otimes [3] + [2,1] \otimes [2] + [2,2] \otimes [1] + [2,3] \otimes [0]$$

With these three multiplications and three comultiplications there are, potentially, nine Hopf algebra structures. However, not all the multiplications and comultiplications are compatible. For example, m_C and Δ_c are not compatible. This is most easily seen by writting the multiplication m_c as \cdot using infix notation, so the compatibility condition becomes,

$$\Delta_c([a_1] \cdot [a_2]) = \Delta_c([a_1]) \cdot \Delta_c([a_2])$$

For example

and $deg(y_i) < n$

$$\Delta_c([1] \cdot [2]) \neq \Delta_c([1]) \cdot \Delta_c([2])$$

It is straightforward to verify that only four of these combinations give Hopf algebras, indicated by letters in the following table, the letters being used henceforth to denote these Hopf algebras

The antipode is detrained by the bialgebra structure.

Lema 2.1. Let H be a graded biologbra. That is, $H = \bigoplus_{n\geq 0} H_n$, $H_0 = \mathbf{k}$, $H_i \cdot H_j \subseteq H_{i+j}$, $\Delta(H_n) \subseteq \bigoplus_{i+j=n} H_i \otimes H_j$. Then H is a Hopf algebra and the antipode may be recursively defined by S(1) = 1, and for $x \in H_n$, $n \geq 1$,

$$S(x) = -\sum_{i=1}^{m} S(y_i) \cdot z_i,$$

$$\Delta(x) = x \otimes 1 + \sum_{i=1}^{m} y_i \otimes z_i$$

Proof. Let assume that for $x \in H_n$, $n \ge 1$

$$\Delta(x) = x \otimes 1 + \sum_{i=1}^{m} y_i \otimes z_i$$

Then, from the relation satisfied by the counit we have,

$$(id \otimes \epsilon)\Delta(x) = x \otimes \epsilon(1) + \sum_{i=1}^{m} y_i \otimes \epsilon(z_i) = x \otimes 1$$

From this we can conclude that in a graded bialgebra $\epsilon(1) = 1$ and $\epsilon(z) = 0$ for all $z \in H_i$ with $i \ge 1$. Now we can substitute our formula for $\Delta(x)$ into the relation for the antipode.

$$m \circ (S \otimes id) \circ \Delta(x) = u \circ \epsilon(x)$$

$$m \circ (S \otimes id)(x \otimes 1 + \sum_{i=1}^{m} y_i \otimes z_i) = 0$$

$$m(S(x) \otimes 1 + \sum_{i=1}^{m} S(y_i) \otimes z_i) = 0$$

$$S(x) + \sum_{i=1}^{m} S(y_i)z_i = 0$$

$$S(x) = -\sum_{i=1}^{m} S(y_i)z_i.$$

 $,\cdots,t_n],$

In the Hopf algebras A and A^* the antipode is given by

$$[s_1,\cdots,s_k]\mapsto (-1)^k[s_k,\cdots,s_1]$$

In B, the antipode is given by B. ven b

the summation being over all words
$$[t_1, \dots, t_n]$$
 that admit $[s_k, \dots, s_1]$ as a refinement.
For example, $[2, 3, 1] \mapsto -[1, 3, 2] + [4, 2] + [1, 5] - [6]$. Dually, in B^* , the antipode is given by

$$[s_1, \cdots, s_k] \mapsto \sum (-1)^n [t_1, \cdots, t_n].$$

here now the symmetry is over all refinements $[t_1, \dots, t_n]$ of $[s_k, \dots, s_1]$.

Theorem 2.2. These four Hopf structures are, integrally, distinct - no two are isomorphic as Hopf algebras.

Proof. Since m_c is not commutative, a Hopf algebra with this product cannot be isomorphic to a Hopf algebra with m_s or m_o as product. Similarly, m_s is not polynomial, so a m_s Hopf algebra cannot be isomorphic to a m_o one. Similarly with the coproduct - Δ_s is not copolynomial, so a Hopf algebra with this comultiplication could not be isomorphic to one with Δ_o as comultiplication.

is

Duality is, of course, given by reflection in the main diagonal in the table, so in fact we have only two Hopf algebras up to duality: A and B. The algebra A is what Hazewinkel [4] refers to as \mathcal{N} , the shuffle algebra, whose dual, A^* , is the Lie-Hopf algebra, i.e., the free associative algebra (or tensor algebra) on S with the Hopf algebra structure where each element of S is primitive $(\Delta(x) = 1 \otimes x + x \otimes 1)$. The algebra B, denoted \mathcal{M} by Hazewinkel, is overlapping shuffle algebra, and the dual algebra B^* is Leibniz-Hopf algebra.

3. THE OVERLAPPING SHUFFI E ALGER

As an Abelian group, i.e., as a \mathbb{Z} -module B is free with as basis all words on $\mathbf{N} = \{1, 2, \ldots\}$ including the empty word. The overlapping shuffle multiplication of two words $w = [a_1, a_2, \dots, a_n]$ and $v = [b_1, b_2, \dots, b_m]$ is the sum of all words that can be obtained as it is already said before. For example,

$$\begin{aligned} [a,b] \cdot_{osh} [c,d] &= [a+c,b+d] + [a+c,b,d] + [a+c,d,b] + [a,b+c,d] \\ & \neq [a,a+d,b] + [a,c,b+d] + [c,a,b+d] + [a,b,c,d] \\ & + [a,c,b,d] + [a,c,d,b] + [c,a,b,d] + [c,a,d,b] + [c,d,a,b], \end{aligned}$$

 $[1] \cdot_{osh} [1,1,1] = [2,1,1] + [1,2,1] + [1,1,2] + 4[1,1,1,1]$ A good way of thinking about this multiplication is the so-called rifle shuffle from card-playing. In agine the two words as two stacks of cards. Perform a rifle shuffle where it can happen that two cards, one from the left stack and one from the right ne, stick together; then their values are to be added.

With this multiplication the Abelian group B obviosly becomes an associative commutative algebra over \mathbf{Z} with unit element (the empty word), i.e., an associative and computative ring with unit element.

4. LYNDON WORDS

Let the elements of N^* , i.e., the words over N, be ordered lexicographically, where any symbol is larger than nothing. Thus $[a_1, a_2, \ldots a_n] > [b_1, b_2, \ldots b_m]$ if and only if there is an *i* such that $a_1 = b_1, \ldots a_{i-1} = b_{i-1}$, $a_i > b_i$ (with, necessarily, $1 \le i \le min\{m,n\}$), or n > m and $a_1 = b_1, \ldots, a_m = b_m$.

A strict suffix of a word $[a_1, \ldots a_n]$ is a word of the form $[a_i, \ldots a_n]$ with $1 < i \le n$. (The empty word and one-symbol words have no strict suffix.)

A word is *Lyndan* if all its strict suffix are larger than the word itself. For example, the words [1, 1, 3], [1, 2, 1, 3], [2, 2, 3, 2, 4] are all Lyndon and the words [2, 1], [1, 2, 1, 1, 2], [1, 3, 1, 3] are not Lyndon. The set of Lyndon words is denoted by Lyn.

Obviously, these definitions make sense for any totally ordered set and not just for the set of natural numbers.

Now consider \mathbf{N}^* a semigroup under the concatenation product (which is, of course, very different from the overlapping shuffle product on B).

Theorem 4.1. (Chen-Fox-Lyndon factorization) Every word w in N^* factors uniquely into a decreasing concatenation product of Lyndon words:

$$w = v_1 \star v_2 \star \cdots v_k, \quad v_i \in Ly_1, \quad v_1 \ge v_2 \ge \cdots \ge v_k.$$

For example,

$$[3, 1, 3, 1, 4, 1, 3, 1, 1] = [2, 3] \star [1, 3, 1, 4] \star [1, 3] \star [1] \star [1]$$

One efficient algorithm for finding the Chen-Fox-Lyndon factorization of word is the block decomposition algorithm[4].

5. THE DITTERS CONJECTURE

The Lyndon words are the right kind of thing for the shuffle algebra over the rational numbers \mathbf{Q} and also for the overlapping shuffle algebra over \mathbf{Q} . Indeed, both these algebras are free polynomial over \mathbf{Q} with as generators the words from Lyn. However, over the integers Lyn most definitely is not a free generating set for the overlapping shuffle algebra.

A word $w = [a_1, a_2, \ldots, a_n] \in \mathbf{N}^*$ is called *elementary* if the greatest common divisor of its symbols is 1, $gcd\{a_1, a_2, \ldots, a_n\} = 1$. A concatenation power of w (or star power) is a word of the form

$$w^{\star m} = \underbrace{w \star w \star \cdots \star w}_{m \text{ times}}$$

Let ESL denote the set of words which are star powers of elementary Lyndon words. For instance, the words [1, 1, 1, 1] and [1, 2, 1, 2] are in ESD (but are not Lyndon), and the words [4], [2, 4] are not in ESL but are in Lyn. The *Differs conjecture* now states that the elements of ESL form a free (communicating) generating set for the overlapping shuffle algebra B over the integers.

The Ditters conjecture dates from around 1972. and the publications quoted proofs, which, however, contain errors.

Hazewinkel introduced the distinction between the "Ditters conjecture" (that the algebra was polynomial) and the "strong Dutters conjecture" (that it was the polynomial algebra on the ESL words) and give a complete proof of the Ditters conjecture. However, the latest result is that the strong Ditters conjecture is wrong.

QUASI-

Let X be a finite subset of an infinite set (of variables) and consider the ring of polynomials R[X] and the ring of power series R[[X]] over a commutative ring R with unit element in the commuting variables from X. A polynomial or power series $f(X) \in R[[X]]$ is called *symmetrical* if for any two finite sequences of indeterminates X_1, X_2, \ldots, X_n and Y_1, Y_2, \ldots, Y_n from X and any sequence of exponents $i_1, i_2, \ldots, i_n \in \mathbf{N}$, the coefficients in f(X) of $X_1^{i_1}X_2^{i_2}\cdots X_n^{i_n}$ and $Y_1^{i_1}Y_2^{i_2}\cdots Y_n^{i_n}$ are the same.

The quasi-symmetrical formal power series are a generalization introduced by Gessel [3] in connection with the combinatorics of plane partitions. This time one takes a totally ordered set of indeterminates, e.g. $V = \{V_1, V_2, \ldots\}$, with the ordering that of the natural numbers, and the condition is that the coefficients of $X_1^{i_1}X_2^{i_2}\cdots X_n^{i_n}$

and $Y_1^{i_1}Y_2^{i_2}\cdots Y_n^{i_n}$ are equal for all totally ordered sets of indeterminates $X_1 < X_2 < \cdots < X_n$ and $Y_1 < Y_2 < \cdots < Y_n$. Thus, for example. $X_1X_2^2 + X_2X_3^2 + X_1X_3^2$ is a quasi-symmetrical polynomial in three variables that is not symmetrical.

Products and sums of quasi-symmetrical polynomials and power series are obviosly again quasi-symmetrical, and thus one has, for example, the ringof quasi-symmetrical power series $Q_{sym_Z}(X)$ in countably many commuting variables over the integers and its subring $Q_{sym_Z}(X)$ of quasi-symmetrical polynomials in finite or countably many indeterminates, which are the quasi-symmetrical power series of bounded degree.

Given a word $w = [a_1, a_2, \ldots, a_n]$ over N, also called a *composition* in this context, consider the quasi-monomial function

$$M_w = \sum_{Y_1 < Y_2 < \dots < Y_n} Y_1^{a_1} Y_2^{a_2} \cdots Y_n^{a_n}$$

defined by w. These form a basis over the integers of $Q_{sym_Z}(X)$.

Proposition 6.1. The assignment $w \to M_w$ defines a homogeneous isomorphism of the overlapping shuffle algebra B with $Q_{sym_Z}(X)$.

The proof is immediate.

If $[s_1, s_2, \ldots, s_k]$ is identified with the quasi-symmetric function $\sum X_{i_1}^{s_1} \cdots X_{i_k}^{s_k}$, then m_o gives the product of two such functions considered as power series in the variables X_i . For example,

$$m_o([1,2] \otimes [3]) = [1,2,3] + [1,3,2] + [3,1,2] + [4,2] + [1,5]$$

$$\sum_{0 \le i < j} X_i X_j^2 \cdot \sum_{0 \le k} X_k^3 = \sum_{\substack{0 \le i < j < k \\ + \sum_{0 \le k < i < j} X_k^3 X_i X_j^2 + \sum_{0 \le i < k < j} X_i X_k^3 X_j^2} X_k^3 X_i X_j^2 + \sum_{0 \le i = k < j} X_i^4 X_j^2 X_k^3 X_i X_j^2 + \sum_{0 \le i < k < j} X_i^4 X_j^2 X_k^3 X_i X_j^3 X_j^2 X_k^3 X_j X_j^3 X_j^2 X_k^3 X_j X_j^3 X_j^3 X_j^2 X_k^3 X_j X_j^3 X_j^3$$

References

[1] M. D. Crossley, Some Hopf algebras of words, CWI Report: No. 06 (2006), 1–11.

- [2] R. Ehrenborg, On posets and Hopf algebras, Adv. Math., 119 (1996), 1–25.
- [3] I. Gessel, Multipartite P-partitions and products of skew Schur functions in Combinatorics and Algebra (Boulder, Colo., 1983), C. Greene, ed., vol 34 of Contemp. Math. AMS (1984), 289–317.
- [4] M. Hazewinkel, The Leibniz Hopf Algebra and Lyndon Words, CWI Report:AM– R9612 (1996).
- [5] M. Hazewinkel, The Algebra of Quasi-symmetric functions is free over the integers, Adv. Math., 164 (2001), 283–300
- [6] M. Hazewinkel, Symmetric functions, noncommutative symmetric functions and quasisymmetric functions, Acta Appl. Wath., 75 (2003), 55–83.
- [7] C. Malvenuto, C. Reutenauer, Duality between quisisymmetric functions and the Solomon descent algebra, J. Algebra, 177, no. 3 (1995), 967–982