Glasgow Math. J. **48** (2006) 575–582. © 2006 Glasgow Mathematical Journal Trust.
doi:10.1017/S0017089506003302. Printed in the United Kingdom

SOME HOPF ALGEBRAS OF WORDS

M. D. CROSSLEY
Department of Mathematics, University of Wales Swansea, Swansea SA2 8PP, Wales
e-mail: M.D.Crossley@Swansea.ac.uk

(Received 16 May, 2006; accepted 10 June, 2006)

Abstract. A number of integral Hopf algebras have been studied that have, as their underlying modules, the free **Z**-module generated by finite words in a certain alphabet. For example, the tensor algebra, the rings of quasisymmetric functions and of noncommutative symmetric functions, the Solomon descent algebra, the Malvenuto-Reutenauer algebra and the homology and cohomology of $\Omega\Sigma\mathbf{C}P^\infty$ are all of this type. Some of these are known to be isomorphic or dual to each other, some are known only to be rationally isomorphic, some have been stated in the literature to be isomorphic when they are only rationally isomorphic.

This paper is, in part, an attempt to find order in this chaos of word Hopf algebras. We consider three multiplications on such modules, and their dual comultiplications, and clarify which of these operations can be combined to obtain Hopf structures. We discuss when the results are isomorphic, integrally or rationally, and study the resulting structures. We are not attempting a classification of Hopf algebras of words, merely an organization of some of the Hopf algebras of this type that have been studied in the literature.

2000 *Mathematics Subject Classification.* 16W30, 57T05, 05E05, 55S10.

1. The basic set-up. 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; 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 **Z**-linear combinations of words. Of course $\mathbf{Z}WS = \mathbf{Z}\overline{WS} \oplus \mathbf{Z}$.

We shall restrict ourselves to the graded setting, and so we assume that S is given a grading in which 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 $\mathbf{Z}WS$ becomes graded and of finite type; i.e., the degree n part, $\mathbf{Z}WS_n$, of $\mathbf{Z}WS$, has finite rank. We can then form the graded dual $(\mathbf{Z}WS)^* = \bigoplus_n (\mathbf{Z}WS_n)^*$, and when we speak of duality we shall always mean this graded duality. Each $\mathbf{Z}WS_n$ has an obvious basis consisting of the words of degree n, and we give $(\mathbf{Z}WS_n)^*$ the dual basis, collating all of these to provide a basis for $(\mathbf{Z}WS)^*$. Of course, the elements of this dual basis are indexed by words, giving a **Z**-linear isomorphism between $\mathbf{Z}WS$ and $(\mathbf{Z}WS)^*$. A Hopf algebra structure consists of a multiplication on $\mathbf{Z}WS$, and a compatible comultiplication on $\mathbf{Z}WS$, the antipode being given automatically since $\mathbf{Z}WS$ is graded and connected. Moreover, a comultiplication can be considered as the dual of a multiplication on $(\mathbf{Z}WS)^*$ which, by the above isomorphism between $\mathbf{Z}WS$ and $(\mathbf{Z}WS)^*$, we can think of as a multiplication on $\mathbf{Z}WS$. Hence a Hopf structure is given by specifying two multiplications, and stating which of them is to be dualised to give the comultiplication.

2. Dramatis Personae – the operations. The first multiplication we consider is 'concatenation', which we denote by μ_C. The concatenation product is determined by

$$\mu_C(s_1 \cdots s_k \otimes t_1 \cdots t_l) = s_1 \cdots s_k t_1 \cdots t_l,$$

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 μ_C is clearly not commutative (unless $|S| = 1$), for example $\mu_C(s_1 \otimes s_2) = s_1 s_2 \neq \mu_C(s_2 \otimes s_1) = s_2 s_1$ for $s_1 \neq s_2 \in S$.

The dual of this is the 'chop' comultiplication, given by

$$\mu_C^*(s_1 \cdots s_k) = \sum_{i=0}^{k} s_1 \cdots s_i \otimes s_{i+1} \cdots s_k.$$

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

$$\mu_S(s_1 \cdots s_k \otimes t_1 \cdots t_l) = \sum_{\sigma} \sigma(s_1 \cdots s_k t_1 \cdots t_l),$$

summed over all permutations σ of $k + l$ symbols that satisfy

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

the permutation σ shuffling the letters in the word in the obvious way. (There will be $\binom{k+l}{k}$ such permutations.) This is commutative; but over $\mathbf{Z}$ it is not free commutative (i.e., $\mathbf{Z}WS$ with this product is not a polynomial algebra); we shall say more about this in Section 4.

The dual comultiplication μ_S^* seems to have no established name, and so we call it the 'excision' coproduct, since it is given by

$$\mu_S^*(s_1 \cdots s_k) = \sum s_{i_1} \cdots s_{i_j} \otimes C(s_{i_1} \cdots s_{i_j}),$$

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

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 (more generally it could be any additive function of n; topologists might prefer to put the letter n in degree $2n$). The multiplication, μ_O, is the 'overlapping shuffle product' defined by

$$\mu_O(s_1 \cdots s_k \otimes t_1 \cdots t_l) = \sum_f f(s_1 \cdots s_k, t_1 \cdots t_l),$$

where f inserts a number of 0s into $s_1 \cdots s_k$ (as many as l), and inserts a number of 0s into $t_1 \cdots t_l$ (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, we have

$$\begin{aligned}\mu_O(12 \otimes 34) &= 1234 + 1324 + 3124 + 1342 + 3142 + 3412 \\ &\quad +154 + 136 + 46 + 424 + 442 + 316 + 352 \\ &= \mu_S(12 \otimes 34) + 154 + 136 + 46 + 424 + 442 + 316 + 352.\end{aligned}$$

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

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

terms; in this formula j counts the number of places where letters are added, and the multinomial coefficient counts which digits of the output word (of length $k+l-j$) are to be from the first word, which from the second, and which from both (where the letters are added). If $s_1 \cdots s_k$ is identified with the quasi-symmetric function $\sum x_{i_1}^{s_1} \cdots x_{i_k}^{s_k}$, then μ_O gives the product of two such functions considered as power series in the variables x_i.

This product is commutative and, indeed, is free commutative; i.e., $\mathbf{Z}WS$ with this multiplication is a polynomial algebra. This is the 'Ditters conjecture', which was stated as a proposition in a 1972 paper of Ditters [**2**], with an explicit set of generators – the 'ESL' words. Ditters himself discovered that the proof was incomplete and several attempts to patch this have been given and, in most cases, found wanting. In [**1**] we proved that the algebra was polynomial over $\mathbf{Z}/p$ (for any prime p) and, although the integral statement can be deduced from this, the details were not given in that paper. Around the same time Hazewinkel introduced the distinction between the 'Ditters conjecture' (that the algebra was polynomial) and the 'strong Ditters conjecture' (that it was the polynomial algebra on the ESL words) and gave a complete proof of the Ditters conjecture [**5**]. I am grateful to the referee for informing me that the strong Ditters conjecture is now known to be false (despite the numerous preprints circulating on the web that claim to prove it). The dual comultiplication is the 'Leibniz' coproduct, given by

$$\mu_O^*(s_1 \cdots s_k) = \sum_{i_1+j_1=s_1} \sum_{i_2+j_2=s_2} \cdots \sum_{i_k+j_k=s_k} i_1 \cdots i_k \otimes j_1 \cdots j_k,$$

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 $i_1 \cdots i_k$ is the empty word.

3. Combining these operations. With these three multiplications and three comultiplications there are, potentially, nine Hopf algebra structures. (Of course, many more structures can be obtained by composing one of the operations with an appropriate automorphism; this is not intended to be an exhaustive list.) However, not all the multiplications and comultiplications are compatible. 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.

		multiplication		
		μ_C	μ_S	μ_O
	μ_C^*	–	A	B
comultiplication	μ_S^*	A^*	–	–
	μ_O^*	B^*	–	–

As we noted earlier, the antipode is determined by the bialgebra structure. 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

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

the summation being over all words $t_1 \cdots t_n$ that admit $s_k \cdots s_1$ as a refinement. For example, $231 \mapsto -132 + 42 + 15 - 6$. This formula is due to Ehrenborg [**3**]. Dually, in B^*, the antipode is given by

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

where now the summation is over all refinements $t_1 \cdots t_n$ of $s_k \cdots s_1$.

It is straightforward to see that there is no repetition in the table.

THEOREM 1. *These four Hopf structures are, integrally, distinct – no two are isomorphic as Hopf algebras.*

Proof. Since μ_C is not commutative, a Hopf algebra with this product cannot be isomorphic to a Hopf algebra with μ_S or μ_O as product. Similarly, μ_S is not polynomial (see Section 4 below), so a μ_S Hopf algebra cannot be isomorphic to a μ_O one. Similarly with the coproduct – μ_S^* is not copolynomial and so a Hopf algebra with this comultiplication could not be isomorphic to one with μ_O^* as comultiplication. □

Duality is, of course, given by reflection in the main diagonal in the table, so that in fact we have only two Hopf algebras up to duality: A and B. The algebra A is what Hazewinkel [**5**] 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. The rationalization $A^* \otimes \mathbf{Q}$ is referred to as the 'concatenation Hopf algebra' $\mathbf{Q}\langle T \rangle$ in [**6**]. The algebra B, denoted $\mathcal{M}$ by Hazewinkel, is more familiar as the ring of quasi-symmetric functions with the outer coproduct, as defined by [**6**]. It is known to topologists as the cohomology of $\Omega\Sigma\mathbf{C}P^\infty$, and the dual algebra B^*, referred to by Hazewinkel as the 'Leibniz-Hopf algebra' is isomorphic to the Solomon Descent algebra [**6**, **9**], and is the ring of 'noncommutative symmetric functions' of [**4**], and the integral lift of the algebra F of [**1**].

Rationally, any (graded, connected) Hopf algebra with commutative multiplication will be a polynomial algebra, by the Hopf-Borel theorem, 7.11 of [**8**]. Hence the obstruction to an integral isomorphism between A and B used in the proof of Theorem 1 vanishes rationally and, indeed, A and B are rationally isomorphic as Hopf algebras.

THEOREM 2. *The Hopf algebras $A \otimes \mathbf{Q}$ and $B \otimes \mathbf{Q}$ are isomorphic. The Hopf algebras $A \otimes \mathbf{Q}$ and $A^* \otimes \mathbf{Q}$ are not isomorphic.*

Proof. The first statement is Theorem 2.1 of **[6]**. For the second statement we can use the same argument as for Theorem 1 – μ_S is commutative but μ_C is not. □

The rational isomorphism between A and B can be generalized as follows.

THEOREM 3. *Let H_1 be a Hopf algebra whose underlying module is $\mathbf{Q}WS$; i.e., $\mathbf{Q} \otimes \mathbf{Z}WS$, where S is countable. Concretely, assume S is the set $\mathbf{N}$ of positive integers (or some finite subset $\{1, \dots, n\}$) and, without loss of generality, that degree is a non-decreasing function; i.e., $\deg(m) < \deg(n)$ implies $m < n$. Note that it need not be strictly increasing – there may be several letters in a given degree.*

If H_1 has product μ_C and any cocommutative coproduct, then $H_1 \cong H_2$, where H_2 is the Hopf algebra with underlying module $\mathbf{Q}WS$, product μ_C and coproduct μ_S^*.

In other words, any two countable cocommutative concatenation Hopf algebras over $\mathbf{Q}$ that are isomorphic as modules will be isomorphic as Hopf algebras.

Proof. We construct an algebra homomorphism $f : H_2 \to H_1$ by specifying $f(n)$ for each $n \in \mathbf{N}$. Since H_2 is, as an algebra, the free associative algebra on $\mathbf{N}$, this determines f completely. We shall ensure that f is a Hopf algebra homomorphism by arranging that $f(n)$ is primitive for each n, and we ensure that f is an isomorphism by arranging that $f(n)$ is congruent to n modulo $1, \dots, n-1$.

To do this, for each $n \geq 1$, let $D_n \subset H_1$ be the subalgebra generated by the elements $1, \dots, n$ of S. Clearly the dimensions of D_n and D_{n-1} are identical in degrees lower than the degree of n, and in that degree they differ by exactly 1. By degree considerations, D_n and D_{n-1} are sub Hopf algebras whose duals will be commutative. By the Hopf-Borel theorem D_n^* and D_{n-1}^* must then be polynomial algebras and, by the dimension argument above, we see that $\dim QD_n^* = 1 + \dim QD_{n-1}^*$ in the degree of n, where Q denotes the module of indecomposables. Dually, the dimension of the primitives in this degree in D_n must exceed that in D_{n-1} by one. Hence there is a primitive in D_n (and so in H_1) in the degree of n, which involves the generator n; i.e., cannot be expressed in terms of $1, \dots, n-1$. Multiplying this primitive by a scalar, if necessary, we obtain a primitive which is equal to n modulo words in $1, \dots, n-1$. We define $f(n)$ to be this primitive. □

In this theorem one hypothesis is that the Hopf algebras are isomorphic as algebras and another implies, by the Hopf-Borel theorem, that they will be isomorphic as coalgebras. Hence the import of the theorem is the *Hopf algebra* isomorphism. What is striking is that in this proof it is the Hopf-Borel theorem which is persuaded to yield this Hopf algebra isomorphism.

4. The shuffle algebra. Thanks to the Ditters conjecture the commutative algebra B is fairly well understood. It is natural to then ask about the algebra structure of A. This is commutative, but not free. For example, any word, when multiplied by itself p times, becomes 0 modulo p. Hence the mod p reduction $A \otimes \mathbf{Z}/p$ has zero divisors, and if this is not free, then A itself cannot be. As this trick shows, the mod p reductions of A turn out to be rather more amenable than A itself.

The Hopf-Borel theorem says that, over a field of characteristic p, every commutative Hopf algebra is a product of monogenic Hopf algebras and that the truncation in each factor must occur at height a power of p. Since, in $A \otimes \mathbf{Z}/p$, every word has p-th power zero, it follows that the p-th power map is trivial (since the words form a basis), and so all factors are truncated at height p. Consequently we have the following result.

THEOREM 4. *$A \otimes \mathbf{Z}/p$ is a tensor product of truncated polynomial algebras of the form $\mathbf{Z}/p[x]/(x^p)$. In particular, $A \otimes \mathbf{Z}/2$ is an exterior algebra.*

The degrees of the generators can be worked out, since we know the Poincaré series of $A \otimes \mathbf{Z}/p$ (it being equal to that of A). Alternatively, noting that for any field k the algebras

$$k[x] \qquad \text{and} \qquad \bigotimes_{n\geq 0} k[y_n]/\left(y_n^p\right),$$

have the same Poincaré series if $|y_n| = p^n|x|$, we see that the Poincaré series of the indecomposables of $A \otimes \mathbf{Z}/p$, $PQ_{A,p}(t)$, can be derived from that of a polynomial algebra C that has the same Poincaré series as A. Concretely:

$$PQ_{A,p}(t) = PQ_C(t) + PQ_C(t^p) + PQ_C(t^{p^2}) + PQ_C(t^{p^3}) + \cdots,$$

where $PQ_C(t)$ denotes the Poincaré series of the indecomposables in the polynomial algebra C.

To be more specific, let us henceforth assume that S is the set $\mathbf{N}$ of non-negative integers, with the element $n \in S$ having degree n. Then for C we could take the Hopf algebra B and, using the first few terms of $PQ_B(t)$ given in [**1**], we see that, when $p = 2$, the number of generators (i.e. the dimension of the module of indecomposables) in each degree in $A \otimes \mathbf{Z}/2$ is given by the following table.

Degree :	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
No. gens. :	1	2	2	5	6	11	18	35	56	105	186	346	630	1179	2182

At the time of writing, Neil Sloane's online handbook of integer sequences had no information on this sequence.

Thus, thanks to the Hopf-Borel theorem, we are able to clarify the algebra structure of $A \otimes \mathbf{Z}/p$ quite satisfactorily (and, of course, $A \otimes \mathbf{Q}$ is isomorphic to the polynomial algebra $B \otimes \mathbf{Q}$). However, the integral structure is much more intricate. Of course, an integral generating set must contain, in each degree, at least as many elements as a generating set for $A \otimes \mathbf{Z}/p$, whatever p is, and so this gives a lower bound on the number of generators for A. In low degrees, these bounds are as follows.

Degree :	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
No. gens. $\geq$	1	2	3	5	7	11	19	35	59	105	187	346	631	1179	2188

Direct calculations show that these lower bounds are not accurate in general; the exact number of generators in degrees 1 to 7 is as follows.

Degree :	1	2	3	4	5	6	7
No. gens. :	1	2	3	5	8	13	21

https://doi.org/10.1017/S0017089506003302 Published online by Cambridge University Press

However, the tempting conclusion that the number of generators is given by the Fibonacci sequence is false: the preceding table shows that there are at least 35 generators in degree 8.

5. The dual Steenrod algebra revisited. As noted in [**1**], for each prime p, the algebra $B^* \otimes \mathbf{Z}/p$ has a particularly important quotient $\mathcal{A}_p$, the mod p Steenrod algebra (to be precise, for p odd, this is the Bockstein-free part of the Steenrod algebra, but we will use the term Steenrod algebra in both cases). Consequently, the dual Steenrod algebra is a sub Hopf algebra of $B \otimes \mathbf{Z}/p$, which leads to one quick proof of the fact that the dual Steenrod algebra is polynomial, a result originally due to Milnor [**7**]. We can describe the inclusion $\mathcal{A}_p^* \hookrightarrow B \otimes \mathbf{Z}/p$ quite explicitly as follows, where we assume that we have fixed a prime p.

The inclusion $\mathcal{A}_p^* \hookrightarrow B \otimes \mathbf{Z}/p$ is determined by the images of the generators ξ_n of the dual Steenrod algebra, and ξ_n is mapped to the element $\tilde{\xi}_n = p^{n-1}p^{n-2}\cdots p1$ in $B \otimes \mathbf{Z}/p$. Note that

$$\tilde{\xi}_n^{p^m} = p^{m+n-1}p^{m+n-2}\cdots p^{m+1}p^m;$$

hence, applying the coproduct to $\tilde{\xi}_n$, we get

$$\mu_C^*(\tilde{\xi}_n) = \mu_C^*(p^{n-1}p^{n-2}\cdots p1) = \sum_{i=0}^{n} p^{n-1}\cdots p^i \otimes p^{i-1}\cdots 1 = \sum_{i=0}^{n} \tilde{\xi}_{n-i}^{p^i} \otimes \tilde{\xi}_i.$$

So far it has not been possible to establish whether or not these elements $\tilde{\xi}_n$ are indecomposable in $B \otimes \mathbf{Z}/p$.

The completely explicit description of both product and coproduct in B now offers yet another approach to Steenrod algebra calculations. In this context the Adem relations form a statement of when a given word, or linear combination of words, belongs to the dual Steenrod algebra. For example, using the formulas above for conjugation, we see that, for $p = 5$,

$$\chi(\xi_2) = \chi(51) = 6 + 15.$$

The Adem relations then tell us, for example, that 6 on its own is not an element of the dual Steenrod algebra and nor (consequently) is 15. Thus, in order to express $\chi(\xi_2)$ as a polynomial in the ξ_ns, we need to find some elements which multiply to produce $6 + 15$. The obvious example is 1.5, which multiplies to $6 + 15 + 51$. Hence $\xi_1.\xi_1^5 = \chi(\xi_2) + \xi_2$; i.e., $\chi(\xi_2) = -\xi_2 + \xi_1^6$.

ACKNOWLEDGEMENT. Much of the work in this paper was carried out while the author was a visitor at the Institut Mittag-Leffler, and I would like to thank this insitute for the opportunity to enjoy such an excellent working environment. Thanks also go to Andy Baker and Manfred Schocker for some useful discussions, and to the referee for updating me on the status of the strong Ditters conjecture.

REFERENCES

1. M. D. Crossley, The Steenrod algebra and other copolynomial Hopf algebras, *Bull. London Math. Soc.* **32** (2000), 609–614.

2. E. J. Ditters, Curves and formal (co)groups, *Invent. Math.* **17** (1972), 1–20.

3. R. Ehrenborg, On posets and Hopf algebras, *Adv. Math.* **119** (1996), 1–25.

4. I. M Gelfand, D. Krob, A. Lascoux, B. Leclerc, V. S. Retakh and J.-Y. Thibon, Noncommutative symmetric functions, *Adv. Math.* **112** (1995), 218–348.

5. M. Hazewinkel, The algebra of quasi-symmetric functions is free over the integers, *Adv. Math.* **164** (2001), 283–300.

6. C. Malvenuto and C. Reutenauer, Duality between quasi-symmetric functions and the Solomon descent algebra, *J. Algebra* **177** (1995), 967–982.

7. J. Milnor, The Steenrod algebra and its dual, *Ann. of Math.* **67** (1958), 150–171.

8. J. Milnor and J. Moore, On the structure of Hopf algebras, *Ann. of Math.* **81** (1965), 211–264.

9. L. Solomon, A Mackey formula in the group ring of a Coxeter group, *J. Algebra* **41** (1976), 255–268.