*Journal of Mathematical Sciences, Vol. 106, No. 4, 2001*

# GENERALIZED OVERLAPPING SHUFFLE ALGEBRAS

**Michiel Hazewinkel**

UDC 512.552.4

This paper is mainly concerned with the Leibniz–Hopf algebra over the integers and its graded dual, the overlapping shuffle algebra. The Ditters conjecture states that this graded dual is a free commutative polynomial ring over the integers and it specifies a set of conjectured generators. The definition of the overlapping shuffle algebra can be generalized to apply to any suitable partial semigroup (instead of the semigroup of natural numbers). The paper continues with investigations of these generalized overlapping shuffle algebras (GOSA's).

## 1. Introduction

The Leibniz–Hopf algebra over the integers is the free associative algebra $\mathcal{Z} = \mathbf{Z}(Z_1, Z_2, \dots)$ over $\mathbf{Z}$ in countably many generators with comultiplication

$$\mu(Z_n) = \sum_{i+j=n} Z_i \otimes Z_j, \quad Z_0 = 1.$$

Its graded dual over the integers is denoted by $\mathcal{M}$ and is called the *overlapping shuffle algebra*. Over the rationals the Leibniz–Hopf algebra is isomorphic to the Hopf algebra

$$\mathcal{U} = \mathbf{Z}\langle U_1, U_2, \dots \rangle, \quad \mu(U_n) = 1 \otimes U_n + U_n \otimes 1.$$

Let $\mathcal{N}$ be the graded dual of $\mathcal{U}$ over the integers. This is the so-called *shuffle algebra*. An important theorem, for example in the theory of free Lie algebras, states that the algebra $\mathcal{N} \otimes_{\mathbf{Z}} \mathbf{Q}$ is commutative free polynomial in the Lyndon words. It is not true that $\mathcal{N}$ is free polynomial over the integers. The Ditters conjecture states that the algebra $\mathcal{M}$, on the contrary, is free polynomial commutative over the integers. This would make it a rather more beautiful version of $\mathcal{N}$. In this paper, I first discuss what I know concerning the Ditters conjecture.

The definition of the overlapping shuffle algebra can be generalized to any suitable partial semigroup. The case of the semigroup $\mathbf{N}$ of natural numbers corresponds to $\mathcal{M}$. These generalized overlapping shuffle algebras (GOSA's) seem to be most interesting objects. The second half of the paper is devoted to their definition and continues with a number of first results on these (bi-)algebras.

## 2. The Overlapping Shuffle Algebra

To begin with, let us consider the overlapping shuffle algebra. It will be denoted $\mathcal{M}$. In the notation below, it is GOSA($\mathbf{N}$), where GOSA stands for "generalized overlapping shuffle algebra," and it is probably the most important GOSA around. Understanding it will have many consequences. In particular, (a proof of) the "Differs conjecture," to be discussed below, is important for many things, e.g., the theory of noncommutative symmetrical functions [4], the combinatorics of permutations [5, 6], and the theory of noncommutative formal groups [2, 3, 15].

As an Abelian group, i.e., as a $\mathbf{Z}$-module, $\mathcal{M}$ is free with as basis all words on $\mathbf{N} = \{1, 2, \dots\}$ including the empty word. Such a word will be denoted $w = [a_1, a_2, \dots, a_n]$, $a \in \mathbf{N}$, e.g., $[1, 1, 2]$. 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 follows. Take a word of length $r$ with all its "spots" so far unfilled, $\max\{m, n\} \le r \le n + m$. Insert the symbols $a_i$ of the word $w$ into it in their original order with no two symbols going to the same spot. Do the same with the symbols $b_j$. It is permitted that a symbol from

Translated from Itogi Nauki i Tekhniki, Seriya Sovremennaya Matematika i Ee Prilozheniya. Tematicheskie Obzory. Vol. 69, Algebra–14, 1999.



1072-3374/01/1064-3168 $ 25.00 

$w$ and a symbol from $v$ go to the same spot, in which case they are to be added. All available spots are to be filled. This multiplication will be denoted simply by juxtaposition.

For example,

$$[a,b][c,d] = [a+c,b+d] + [a+c,b,d] + [a+c,d,b] + [a,b+c,d] + [c,a+d,b] + [a,c,b+d] + [c,a,b+d] + [a,b,c,d] + [a,c,b,d] + [a,c,d,b] + [c,a,b,d] + [c,a,d,b] + [c,d,a,b],$$

$$[2][1,3,5] = [3,3,5] + [3,5,5] + [1,3,7] + [2,1,3,5] + [1,2,3,5] + [1,3,2,5] + [1,3,5,2],$$

$$[1][1,1,1] = [2,1,1] + [1,2,1] + [1,1,2] + 4[1,1,1,1].$$

A good way of thinking about this multiplication is the so-called rifle shuffle from card-playing. Imagine 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 one, stick together; then their values are to be added.

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

## 3. Lyndon Words

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

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

A word is *Lyndon* if all its proper tails 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 $\mathcal{M}$).

**Theorem** (Chen–Fox–Lyndon factorization, [1,12]). *Every word $w$ in $\mathbf{N}^*$ factors uniquely into a decreasing concatenation product of Lyndon words*:

$$w = v_1 * v_2 * \cdots * v_k, \quad v_i \in \mathrm{Lyn}, \quad v_1 \ge v_2 \ge \cdots \ge v_k.$$

For example,

$$[2,3,1,3,1,4,1,3,1,1] = [2,3] * [1,3,1,4] * [1,3] * [1] * [1].$$

One efficient algorithm for finding the Chen–Fox–Lyndon factorization of a word is the block decomposition algorithm from [15].

## 4. 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 (see Secs. 9 and 10 below for more details). However, over the integers Lyn most definitely is not a free generating set for the overlapping shuffle algebra (see also Sec. 9 below).

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

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

Let ESL denote the set of words which are star powers of elementary Lyndon words. For instance, the words $[1,1,1,1]$, $[1,2,1,2]$, and $[1,2,1,4]$ are in ESL (but the first two are not Lyndon), and the words $[4]$, $[2,4]$ are not in ESL but are in Lyn.

The *Ditters conjecture* now states that the elements of ESL form a free (communicating) generating set for the overlapping shuffle algebra $\mathcal{M}$ over the integers.

Let the *weight* of a word $w = [a_1, a_2, \ldots, a_n]$ be equal to $a_1 + a_2 + \cdots + a_n$. The elements of ESL of weight $\geq 6$ are:

$[1]$;

$[1,1]$;

$[1,1,1]$, $[1,2]$;

$[1,1,1,1]$, $[1,1,2]$, $[1,3]$;

$[1,1,1,1,1]$, $[1,1,1,2]$, $[1,1,3]$, $[1,2,2]$, $[1,4]$, $[2,3]$;

$[1,1,1,1,1,1]$, $[1,1,1,1,2]$, $[1,1,1,3]$, $[1,1,2,2]$, $[1,1,4]$, $[1,2,1,2]$, $[1,2,3]$, $[1,3,2]$, $[1,5]$.

The Ditters conjecture dates from around 1972 (see [2,3]), and the publications quoted contain proofs, which, however, contain errors. The latest proof attempt that I know of is in [15], and until August 1997 I thought this proof to be correct. However, it is not. The error occurs in the second paragraph of p. 74. (There is no guarantee that the length'1 "separable products" occurring there are lexicographically smaller than the element $w_{(k)}$ under consideration at that time, and indeed if the calculations are done explicitly this turns out not to be the case; in fact one can show from low weight examples that no such "triangular proof" based on an induction with respect to some ordering of words will work directly.)

Thus, at this time the conjecture is again open (contrary to what I wrote in [9]).

The positive evidence in favor of the Ditters conjecture is rather strong though and I definitely think that the conjecture is true. I will now try to summarize this positive evidence.

**1.** The number of conjectured generators for each weight is exactly right. This can be formulated more precisely as follows. The overlapping shuffle algebra $\mathcal{M}$ is graded by the weight of words as defined above. Now consider the free commutative algebra over the integers, $\mathbf{Z}[\mathrm{ESL}]$, in the "variables" from ESL with each variable given its weight as a word and with the weight of a monomial equal to the product of the weights of its factors. The inclusion $\mathrm{ESL} \in \mathcal{M}$ induces a graded homomorphism of $\mathbf{Z}$-algebras

$$\varphi : \mathbf{Z}[\mathrm{ESL}] \to \mathcal{M}$$

and the ranks of the homogeneous parts of weight $n$ of the two algebras are equal:

$$\mathbf{Z}[\mathrm{ESL}]_n = \mathcal{M}_n.$$

This is seen as follows. First, there are just as many Lyndon words of weight $n$ as there are elements of ESL of weight $n$. The bijective correspondence is given by the assignment

$$\alpha : \mathrm{Lyn} \to \mathrm{ESL}, \quad [a_1, a_2, \ldots, a_n] \mapsto [d^{-1}a_1, d^{-1}a_2, \ldots, d^{-1}a_n]^{*d},$$

where $d = \gcd\{a_1, a_2, \ldots, a_n\}$. Second, the overlapping shuffle algebra over $\mathbf{Q}$ is isomorphic to $\mathbf{Q}[\mathrm{Lyn}]$, via the homogeneous morphism induced by the inclusion $\mathrm{Lyn} \subset \mathcal{M}$ (see below in Sec. 10).

It follows immediately that to prove that $\varphi$ is an isomorphism, it suffices to prove that it is surjective.

**2.** $\varphi_n : \mathbf{Z}[\mathrm{ESL}]_n \to \mathcal{M}_n$ is an isomorphism for $n \leq 10$ (by ad hoc and rather messy hand calculations).

**3.** A natural $p$-adic analogue of the Ditters conjecture is true (see Sec. 11 below).

For the next bit of evidence it is necessary to know that the overlapping shuffle algebra is naturally isomorphic to the algebra of quasi-symmetrical functions (see Sec. 5 for details).

**4.** The subalgebra of the symmetrical functions $\mathrm{Sym}_{\mathbf{Z}}(X) \subset \mathrm{Qsym}_{\mathbf{Z}}(X) = \mathcal{M}$ is in the image of $\varphi$. Indeed, it is generated by the words $[\underbrace{1,1,\dots,1}_{n}]$, which correspond to the elementary symmetrical functions. The Lyndon words $[n]$, $n = 1,2,\dots$, correspond to the power sums, and they are generators over $\mathbf{Q}$ for the symmetrical functions, but not over $\mathbf{Z}$.

**5.** Let $J_n$ be the submodule of $\mathcal{M}$ spanned by the words of length $\geq n$. This is an ideal in $\mathcal{M}$. To prove that $\varphi$ is surjective, it suffices to aprove that the composed maps

$$\varphi : \mathbf{Z}[\mathrm{ESL}] \to \mathcal{M} \to \mathcal{M}/J_n$$

are surjective for every $n$, i.e., that $\varphi$ is surjective modulo $J_n$ for every $n = 2,3,\dots$. In the appendix below this is proved for $n = 2,3,4,5$. There is some extra interest in that things go fine modulo words of length $\geq 5$, because it is at length 4 that the "second-generation" Lyndon words first appear. (A "first-generation" Lyndon word is one of the form $[1,1,\dots,1,a_{,1},a_2,\dots,a_m]$, $a_i \geq 2$; $[1,2,1,3]$ is a "second-generation" Lyndon word.)

## 5. Quasi-Symmetrical Functions

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 $X_1, X_2, \dots, X_n$ and $Y_1, Y_2, \dots, Y_n$ from $X$ and any sequence of exponents $i_1, i_2, \dots, i_n \in \mathbf{N}$, 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 [5] in connection with the combinatorics of plane partitions. This time one takes a totally *ordered* set of indeterminates, e.g. $V = \{V_1, V_2, \dots\}$, 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,

$$X_1 X_2^2 + X_2 X_3^2 + X_1 X_3^2$$

is a quasi-symmetrical polynomial in three variables that is not symmetrical.

Products and sums of quasi-symmetrical polynomials and power series are obviously again quasi-symmetrical, and thus one has, for example, the ring of quasi-symmetrical power series $\mathrm{Qsym}_{\mathbf{Z}}(X)^{\vee}$ in countably many commuting variables over the integers and its subring $\mathrm{Qsym}_{\mathbf{Z}}(X)$ of quasi-symmetrical polynomials in finite or countably many indeterminates, which are the quasi-symmetrical power series of bounded degree.

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

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

defined by $w$. These form a basis over the integers of $\mathrm{Qsym}_{\mathbf{Z}}(X)$.

**Proposition.** *The assignment $w \to M_w$ defines a homogeneous isomorphism of the overlapping shuffle algebra $\mathcal{M}$ with* $\mathrm{Qsym}_{\mathbf{Z}}(X)$.

The proof is immediate.

## 6. The Leibniz–Hopf algebra

Consider the free associative algebra in countably many (noncommuting) indeterminates over the integers:

$$\mathcal{Z} = \mathbf{Z}\langle Z_1, Z_2, \dots \rangle.$$

This ring is given a Hopf algebra structure by means of the comultiplication defined by

$$\mu(Z_n) = \sum_{\substack{i+j=n \\ i,j \in \mathbf{N} \cup \{0\}}} Z_i \otimes Z_j, \quad Z_0 = 1,$$

the augmentation

$$\varepsilon(Z_n) = 0, \quad n = 1, 2, \dots,$$

and the antipode

$$\iota(Z_n) = \sum_{i_1+i_2+\cdots+i_k=n} (-1)^k Z_{i_1} Z_{i_2} \cdots Z_{i_k},$$

where the last sum is over all sequences $(i_1, i_2, \cdots, i_k)$, $i_j \in \mathbf{N}$, that sum to $n$. This is the *Leibniz–Hopf algebra*. If each $Z_n$ is given weight $n$, the comultiplication and antipode are weight preserving. Thus the graded dual of $\mathcal{Z}$ is a graded algebra over the integers. A basis of $\mathcal{Z}$ over the integers is given by the monomials in the indeterminates. Thus a basis of the dual module is constituted by the words over $\mathbf{N}$, with the duality given by

$$\langle w, Z_v \rangle = \delta_{w,v},$$

where $\delta$ is the Kronecker symbol and $Z_v = Z_{b_1} Z_{b_2} \cdots Z_{b_m}$ for $v = [b_1, \dots, b_m]$. The multiplication on the dual is determined by

$$\langle wv, Z_u \rangle = \langle w \otimes v, \mu(Z_u) \rangle.$$

It is now a simple calculation to verify that this multiplication of words is precisely the overlapping shuffle multiplication.

Thus the overlapping shuffle algebra $\mathcal{M}$ is the graded dual over the integers of the Leibniz–Hopf algebra $\mathcal{Z}$.

## 7. The Representative Ring of the Big Witt Vectors

The maximal commutative quotient of the Leibniz–Hopf algebra is the algebra

$$\mathcal{R} = Z[X_1, X_2, \dots]$$

of polynomials in countably many commuting indeterminates over the integers with the same comultiplication. This is the representative ring of the big Witt vectors [7]:

$$\mathrm{Ring}(\mathcal{R}, A) = W(A)$$

for any ring $A$, where Ring is the category of commutative rings with unit element and $W$ is the functor of big Witt vectors.

The ring $\mathcal{R}$ plays a crucial role in the classification theory of commutative formal groups [7]. It is natural to examine the possible roles of the noncommutative lift $\mathcal{Z}$ for the classification theory of noncommutative formal groups. It is in this connection that the Ditters conjecture came up.

## 8. The Solomon Descent Algebra and the Representations of Symmetrical Groups

One of the (many) manifestations of the algebra $\mathcal{R}$ in various parts of mathematics is as the direct sum of the representation rings of the symmetrical groups:

$$\mathcal{R} = \bigoplus_n R(S_n),$$

where $R(S_n)$ is the ring of complex representations of the symmetrical group on $n$ letters $S_n$ [11]. More precisely, $\mathcal{R}$ is self-dual [7], and this representation theoretic $\mathcal{R}$ is the dual of the $\mathcal{R}$ of the previous section. The multiplication on $\mathcal{R}$, however, is (obviously) not the usual (tensor) multiplication of representations. Instead, it is defined via the natural isomorphism

$$R(S_i) \otimes R(S_j) = R(S_i \times S_j)$$

as follows:

$$\rho\sigma = \mathrm{Ind}_{S_i \times S_j}^{S_{i+j}}(\rho \otimes \sigma),$$

where Ind stands for induction. Similarly, and dually, using the same natural isomorphism, we dafine the comultiplication by restriction:

$$\mu(\tau) = \sum_{i+j=n} \mathrm{Res}_{S_i \times S_j}^{S_n}(\tau).$$

A great deal of the theory of representations of symmetrical groups, e.g., Frobenius reciprocity, is encoded in the observation that $\mathcal{R} = \bigoplus_n R(S_n)$ with multiplication and comultiplication thus defined is a Hopf algebra, and that it is self-dual [7].

The usual multiplications on the $R(S_n)$ define a second multiplication on $\mathcal{R}$ which is distributive over the first in the appropriate sense, making $\mathcal{R}$ a ring in the category of coalgebras.

The Solomon descent algebras $D(S_n)$ [16] were invented as noncommutative analogues of the rings of characters of the symmetrical groups (and, more generally, Coxeter groups). These can also be "direct summed" to a larger object

$$\mathcal{D} = \bigoplus_n D(S_n)$$

with a new multiplication over which the direct sum of the original multiplications is distributive. It turns out that $\mathcal{D}$ is naturally isomorphic to the Leibniz–Hopf algebra $\mathcal{Z}$ ([13]; see also [4]) and $\mathcal{R} = \bigoplus_n R(S_n)$ is the commutative quotient of $\mathcal{D}$ in the same way that $\mathcal{R} = \mathbf{Z}[X_1, X_2, \dots]$ is the commutative quotient of $\mathcal{Z}$.

The dual of $\mathcal{Z}$ is the overlapping shuffle algebra $\mathcal{M}$ which is the algebra of quasi-symmetrical functions $\mathrm{Qsym}_{\mathbf{Z}}(X)$ which contains the algebra of symmetrical functions, $\mathrm{Sym}_{\mathbf{Z}}(X)$, which is the dual of $\mathcal{R}$; thus everything fits perfectly, in the sense that the dual of the quotient situation $\mathcal{Z} \to \mathcal{R}$ is the inclusion situation $\mathrm{Sym}_{\mathbf{Z}}(X) \subset \mathrm{Qsym}_{\mathbf{Z}}(X)$.

## 9. The Shuffle Algebra

There is a second Hopf algebra structure on the free associative algebra in countably many indeterminates over $\mathbf{Z}$, i.e., a second way to make the ring $\mathbf{Z}\langle Z_1, Z_2, \dots\rangle$ into a Hopf algebra. This structure is actually rather better known and it plays a most important role in the theory of free Lie algebras and related matters. In order to avoid notational confusion, let

$$\mathcal{U} = \mathbf{Z}\langle U_1, U_2, \dots\rangle$$

be another copy of the free associative algebra in countably many variables over $\mathbf{Z}$, and let the comultiplication be defined by

$$\mu(U_n) = 1 \otimes U_n + U_n \otimes 1.$$

Let $\mathcal{N}$ be the graded dual algebra of $\mathcal{U}$. This is the *shuffle algebra*. The shuffle multiplication is the same as the overlapping shuffle multiplication except that overlaps are not allowed. Thus, for example,

$$[a,b] \times_{\mathrm{sh}} [c,d] = [a,b,c,d] + [a,c,b,d] + [a,c,d,b] + [c,a,b,d] + [c,a,d,b] + [c,d,a,b]$$

and

$$[1] \times_{\mathrm{sh}} [1] = 2[1,1], \quad [1] \times_{\mathrm{sh}} [1] \times_{\mathrm{sh}} [1] = 6[1,1,1].$$

A well known theorem says that over the rationals the shuffle algebra is free polynomial. More precisely, let $\mathbf{Q}[\mathrm{Lyn}]$ be the free commutative polynomial ring over the set Lyn of Lyndon words; then (see, e.g., [14]) the following statement holds.

**Theorem** (shuffle-algebra structure theorem). $\mathcal{N} \otimes \mathbf{Q} = \mathbf{Q}[\mathrm{Lyn}]$.

Note that nothing like this is true over the integers. Indeed, by the second examples of the shuffle multiplication above $\mathcal{N} \otimes \mathbf{Z}/(2)$ has nilpotents and therefore $\mathcal{N}$ cannot be a free algebra over $\mathbf{Z}$. From this point of view, if, as seems likely, the Ditters conjecture is true, the overlapping shuffle algebra $\mathcal{M}$ is a rather nicer "version" of $\mathcal{N}$. Here the word "version" refers to the fact that over the rational numbers, $\mathbf{Q}$, $\mathcal{M}$ and $\mathcal{N}$ become isomorphic (see Sec. 10 below).

The proof of the shuffle-algebra structure theorem is a straightforward application of the following theorem concerning shuffle products in connection with the Chen–Fox–Lyndon factorization.

**Theorem.** *Let $w \in \mathbf{N}^*$ be a word on the natural numbers, and let $w = v_1 * v_2 * \cdots * v_m$ be its Chen–Fox–Lyndon factorization. Then all words that occur with nonzero coefficient in the shuffle product $v_1 \times_{\mathrm{sh}} v_2 \times_{\mathrm{sh}} \cdots \times_{\mathrm{sh}} v_m$ are lexicographically less than or equal to $w$ and $w$ occurs with nonzero integer coefficient in this product.*

Given this result, the proof of the shuffle-algebra theorem proceeds as follows. Order all words lexicographically. Consider some nonempty word $w$. With induction. [1] being the smallest nonempty word, we can assume that all words lexicographically smaller than $w$ have been written as polynomials in the elements of Lyn. Take the Chen–Fox–Lyndon factorization $w = v_1 * v_2 * \cdots * v_m$ of $w$ and consider, using the Chen–Fox–Lyndon factorization theorem,

$$v_1 \times_{\mathrm{sh}} v_2 \times_{\mathrm{sh}} \cdots \times_{\mathrm{sh}} v_m = aw + (\text{remainder}) .$$

By that theorem, the coefficient $a$ is nonzero and all the words in (remainder) are lexicographically smaller than $w$ and hence $\in \mathbf{Q}[\mathrm{Lyn}]$. It follows that also $w \in \mathbf{Q}[\mathrm{Lyn}]$. This proves generation, i.e., surjectivity of the natural map $\mathbf{Q}[\mathrm{Lyn}] \to \mathcal{N}$. Injectivity follows by counting. The map is homogeneous, both algebras are graded and $\dim_{\mathbf{Q}}(\mathbf{Q}[\mathrm{Lyn}]_n) = \dim_{\mathbf{Q}}(\mathcal{N}_n)$ (see, e.g., [14, 15] for details).

## 10. The Overlapping Shuffle Algebra over the Rationals

As was already stated, the overlapping shuffle algebra and the shuffle algebra become isomorphic over the rationals. Given that the shuffle algebra over the rationals is free polynomial there are of course very many possible algebra homomorphisms. There is a particularly nice one which comes from a Hopf algebra isomorphism between $\mathcal{Z} \otimes \mathbf{Q}$ and $\mathcal{U} \otimes \mathbf{Q}$ as follows.

Consider the expression

$$1 + Z_1 t + Z_2 t^2 + Z_3 t^3 + \cdots = \exp(U_1 t + U_2 t^2 + U_3 t^3 + \cdots).$$

This gives an expression for each $Z_i$ in terms of $U_1, \ldots, U_i$ and hence defines an algebra homomorphism

$$\beta : \mathcal{Z} \otimes \mathbf{Q} \to \mathcal{U} \otimes \mathbf{Q}.$$

**Theorem.** *The algebra homomorphism $\beta$ is an isomorphism of Hopf algebras and hence its dual defines an isomorphism of algebras $\beta^* : \mathcal{N} \otimes \mathbf{Q} \to \mathcal{M} \otimes \mathbf{Q}$.*

For details, see, e.g., [8]. This proves of course that $\mathcal{M} \otimes \mathbf{Q}$ is free polynomial and gives a set of generators which is, however, neither the set Lyn nor the set ESL.

It is also not difficult to adapt the proof that $\mathcal{N} \otimes \mathbf{Q}$ is free polynomial on Lyn to a proof that $\mathcal{M} \otimes \mathbf{Q}$ is free polynomial on Lyn. The only modification needed is to change a bit the ordering on words that is used. The ordering that works here is the following:

$$w \succ v \iff \begin{cases} \mathrm{length}(w) > \mathrm{length}(v) & \text{or} \\ \mathrm{length}(w) = \mathrm{length}(v) & \text{and} \quad w \geq v \quad (\text{lexicographically}). \end{cases}$$

I know of no proof at the moment to show that $\mathcal{M} \otimes \mathbf{Q}$ is free polynomial (over $\mathbf{Q}$) on ESL.

## 11. A $p$-adic Analogue of the Ditters Conjecture

There is a $p$-adic analogue of the Ditters conjecture, which, surprisingly, can be proved by a fairly straightforward modification of the argument which is used to prove the shuffle-algebra structure theorem. Surprising, because I do not believe that this is the right way to get at the Ditters conjecture itself.

Let us start with the formulation. A word $w = [a_1, \dots, a_n]$ on $\mathbf{N}$ is *$p$-elementary*, where $p$ is a prime number, if the gcd of $a_1, \dots, a_n$ is not divisible by $p$. A $p$-star-power of a word is a word of the form

$$w = \underbrace{v * \cdots * v}_{p \text{ factors}}.$$

The set $\mathrm{ESL}(p)$ is the set of words which are $p$-star-powers of $p$-elementary Lyndon words.

**Theorem** ($p$-adic analogue of the Ditters conjecture).

$$\mathcal{M} \otimes \mathbf{Z}_{(p)} = \mathbf{Z}_{(p)}[\mathrm{ESL}(p)],$$

*i.e., $\mathcal{M} \otimes \mathbf{Z}_{(p)}$ is the free commutative algebra on $\mathrm{ESL}(p)$ over $\mathbf{Z}_{(p)}$.*

To prove this, we first need some information on binomial and multinomial coefficients. Extend the usual definition of the binomial coefficients in the standard way:

$$\binom{n}{m} = 0 \quad \text{if } m > n, \qquad \binom{n}{0} = 1 \quad \text{if } n \geq 0.$$

**Proposition.** *Consider the $p$-adic expansion of two natural numbers $m$ and $n$*

$$n = a_0 + a_1 p + \cdots + a_k p^k, \quad m = b_0 + b_1 p + \cdots + b_k p^k, \quad a_i, b_i \in \{0, 1, \dots, p-1\}.$$

*The value of the binomial coefficient modulo $p$ is equal to*

$$\binom{n}{m} \equiv \binom{a_0}{b_0}\binom{a_1}{b_1} \cdots \binom{a_n}{b_n}.$$

*In particular, if $b_i \leq a_i$ for all $i$, this binomial coefficient is nonzero modulo $p$.*

**Corollary.** *The multinomial coefficient*

$$\binom{n}{\underbrace{p^k \cdots p^k}_{a_k \text{ times}} \underbrace{p^{k-1} \cdots p^{k-1}}_{a_{k-1} \text{ times}} \cdots \underbrace{1 \cdots 1}_{a_0 \text{ times}}}$$

*is nonzero modulo $p$.*

**Proof of the proposition.** For $0 \leq n \leq p-1$ things are clear. Now let $n \geq p$, write down the $p$-adic expansion of $n$ and $m$ as in the formulation of the proposition and let

$$n_1 = a_0 + a_1 p + \cdots + a_{k-1} p^{k-1}, \qquad m_1 = b_0 + b_1 p + \cdots + b_{k-1} p^{k-1}.$$

We have

$$(x+y)^n = (x+y)^{a_k p^k} (x+y)^{n_1} \equiv \left(x^{p^k} + y^{p^k}\right)^{a_k} (x+y)^{n_1}.$$

Writing things out gives

$$(x+y)^n = \left\{ \binom{a_k}{0} \left(x^{p^k}\right)^{a_k} \left(y^{p^k}\right)^0 + \cdots + \binom{a_k}{i} \left(x^{p^k}\right)^{a_k - i} \left(y^{p^k}\right)^i + \cdots + \left(x^{p^k}\right)^0 \left(y^{p^k}\right)^{a_k} \right\}$$
$$\times \left\{ \binom{n_1}{0} x^{n_1} y^0 + \cdots + \binom{n_1}{i} x^{n_1 - i} y^i + \cdots + \binom{n_1}{0} x^0 y^{n_1} \right\}.$$

It follows that

$$\binom{n}{m} \equiv \binom{a_k}{b_k}\binom{n_1}{m_1},$$

and with induction the desired result follows.

**Proof of the $p$-adic Ditters conjecture.** We use the same ordering of words as at the end of Sec. 10 above, i.e., length first and then lexicographic ordering on words of equal length. Let $SL(p)$ be the set of all $p$-star powers of Lyndon words, i.e., words of the form

$$w = v^{*p^k}, \quad v \in \mathrm{Lyn}.$$

The first step is to prove that all words can be written as polynomials in the elements of $SL(p)$. Let $w$ be a word over $\mathbf{N}$. With induction we can assume that all smaller words can be written as polynomials in $SL(p)$, and by induction on weight that all nontrivial products can be so written. Let

$$w = v_1^{*n_1} * v_2^{*n_2} * \cdots * v_m^{*n_m}, \quad v_i \in \mathrm{Lyn}, v_1 > v_2 > \cdots > v_m$$

be its Chen–Fox–Lyndon factorization. Consider products of the form

$$\prod_{i=1}^{k_1} v_1^{*n_{1i}} \prod_{i=1}^{k_2} v_2^{*n_{2i}} \cdots \prod_{i=1}^{k_m} v_m^{*n_{mi}},$$

where the products are overlapping shuffle products and $n_{i1} + \cdots + n_{ii_k} = n_i$, $i = 1, \ldots, m$. The largest word occurring in such a product (in the ordering we are using) will be the word $w$, independent of how the various star-powers are broken up. However, the coefficient of $w$ will depend on how the star-powers of the $v_j$ are broken up. Indeed, the coefficient will be the product of multinomial coefficients

$$\binom{n_1}{n_{11} \cdots n_{1k_1}} \binom{n_2}{n_{21} \cdots n_{2k_2}} \cdots \binom{n_m}{n_{m1} \cdots n_{mk_m}}.$$

For instance, if one takes $n_{ij} = 1$ $\forall i, j$ (which is what is done to prove $\mathcal{M} \otimes \mathbf{Q} = \mathbf{Q}[\mathrm{Lyn}]$ (see Sec. 10 above), the coefficient is $n_1! n_2! \cdots n_m!$, and if one takes the other extreme, $k_1 = k_2 = \cdots = k_m = 1$, the coefficient is 1. Here, for our present purposes, we break up each $n_j$ according to its $p$-adic expansion, i.e., if $n = a_0 + a_1 p + \cdots + a_k p^k$, $a_i \in \{0, 1, \ldots, p-1\}$, then it is partitioned (broken up) into

$$\underbrace{p^k, p^k, \ldots, p^k}_{a_k \text{ parts}}, \underbrace{p^{k-1}, p^{k-1}, \ldots, p^{k-1}}_{a_{k-1} \text{ parts}}, \ldots, \underbrace{p, \ldots, p}_{a_1 \text{ parts}}, \underbrace{1, \ldots, 1}_{a_0 \text{ parts}}.$$

The corollary above says that in this case the coefficient is nonzero modulo $p$, i.e., it is an invertible element of $\mathbf{Z}_{(p)}$. This proves that also $w$ can be written as a polynomial in $SL(p)$.

Now for a given weight $n$, let $w_1, w_2, \ldots, w_m$ be all the words of that weight that are in $SL(p)$ but are not $p$-elementary. So, if $w_1 = [a_{i1}, \ldots, a_{ik_i}]$, $p | \gcd\{a_{i1}, \ldots, a_{ii_k}\}$. Let

$$b_{ij} = p^{-1} a_{ij}, \quad v_i = [b_{i1}, \ldots, b_{ik_i}].$$

Now consider the overlapping shuffle powers $v_i^p$. It is easy to see that these are of the form

$$v_i^p = w_i + p(\text{something of weight } n).$$

By what has been proved, each of these somethings of weight $n$ can be written as polynomials in $SL(p)$. Do so. Now calculate modulo nontrivial products and the elements of $\mathrm{ESL}(p)$. The result will be the following $n$ congruence relations:

$$a_{11} w_1 + \cdots + a_{1n} w_n \equiv 0, \quad \ldots, \quad a_{n1} w_1 + \cdots + a_{nn} w_n \equiv 0,$$

where the matrix $A = (a_{ij})$ has the property $A \equiv i_n \mod p$. This implies that the determinant of the matrix $A$ is invertible in $\mathbf{Z}_{(p)}$, so that $w_1, \ldots, w_n$ can be eliminated. This proves that the elements from $\mathrm{ESL}(p)$ suffice to generate all of $\mathcal{M} \otimes \mathbf{Z}_{(p)}$ over $\mathbf{Z}_{(p)}$. The same counting argument used before finishes the proof.

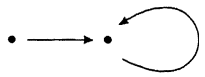

Fig. 1

**Remark.** There is no predicting (that I can see) which $w$'s will show up in these congruence relations. A priori, larger ones, smaller ones (lexicographically) and also the same ones can show up. And they do. This is where the proof attempt from [15] breaks down. All one knows in that case is that the rows in the matrix $A$ break up into several classes corresponding to different primes $p$, and these rows are "unit rows" modulo that $p$. That is not enough, as the matrix

$$A = \begin{pmatrix} 3 & 2 \\ 6 & 4 \end{pmatrix}$$

for the prime 2 for the first row and the prime 3 for the second one shows. Explicit examples for low weights give matrices $A$ that are invertible over the rationals but not necessarily over the integers, showing that more relations in $\mathcal{M}$ need to be used.

## 12. Generalized Overlapping Shuffle Algebras

Let $S$ be a partial semigroup, i.e., a set with a partially defined multiplication function

$$S \times S \to S$$

that is associative. This last requirement means that if $s_1s_2$ and $s_2s_3$ are both defined, then so are $(s_1s_2)s_3$ and $s_1(s_2s_3)$ and these two are then equal, and also if $s_2s_3$ and $s_1(s_2s_3)$ are defined, then $s_1s_2$ is defined (and $(s_1s_2)s_3 = s_1(s_2s_3)$), and if $s_1s_2$ and $(s_1s_2)s_3$ are defined, then $s_2s_3$ is defined (and $(s_1s_2)s_3 = s_1(s_2s_3)$). For instance the set of morphisms of a category is a partial semigroup in this sense.

The generalized overlapping shuffle algebra defined by a partial semigroup over $\mathbf{Z}$ (or, more generally, over a commutative ring $R$ with unit element) is defined as follows. As a free Abelian group it has as basis all words on the set $S$. The product is basically the overlapping shuffle product (taking account the order of the factors) and with only those overlaps allowed for which the product is defined. This is an associative algebra with unit element (represented by the empty word). This algebra will be denoted GOSA($S$). For instance, let $S$ be the partial semigroup depicted in Fig. 1, i.e.,

$$S = \{s_1,\ s_2;\ s_2s_1 = s_1,\ s_2s_2 = s_2,\ \text{no other products defined}\}.$$

Then, for example

$$[s_1][s_2] = [s_1, s_2] + [s_2, s_1], \quad [s_2][s_1] = [s_2] + [s_2, s_1] + [s_1, s_2]$$

and

$$[s_2][s_2, s_1] = 2[s_2, s_1] + 2[s_2, s_2, s_1] + [s_2, s_1, s_2], \qquad [s_2, s_1][s_2] = [s_2, s_1] + 2[s_2, s_2, s_1] + [s_2, s_1, s_2].$$

In particular, this particular GOSA is not commutative. Indeed, GOSA($S$) is commutative if and only if $S$ is commutative.

If the multiplication on $S$ is nowhere defined one obtains the shuffle algebra, $\mathrm{Sh}_{\mathbf{Z}}(S)$ over the set $S$. For the case of the semigroup $\mathbf{N}$ of natural numbers with addition the result is the overlapping shuffle algebra we have been examining in the previous sections, i.e., GOSA($\mathbf{N}$) = $\mathcal{M}$. Some other special GOSA's will be discussed in some detail below.

## 13. GOSA's as Duals of Hopf Algebras

Again let $S$ be a partial semigroup. We now need one mild extra finiteness condition:

$$\forall s \in S \quad \#\{(t,u) \in S \times S : tu = s\} < \infty.$$

This holds, for instance, for all finite semigroups and for (partially) ordered semigroups such as the natural numbers; it does not hold for any infinite group, for instance, the group of integers.

Define $\mathcal{Z}(S)$ as the free associative algebra over the integers in the (noncommuting) variables $Z_s$, $s \in S$, i.e., as the algebra $\mathcal{Z}(S) = \mathbf{Z}\langle Z_s : s \in S\rangle$, and define the comultiplication and counit by

$$\mu(Z_s) = 1 \otimes Z_s + \sum_{ut=s} Z_u \otimes Z_t + Z_s \otimes 1 \quad \text{and} \quad \varepsilon(Z_s) = 0.$$

This defines the bialgebra $\mathcal{Z}(S)$, and its graded dual is GOSA($S$) (where, if $S$ is not finite, increasing weights need to used for the $Z_s$).

It is certainly not the case that these bialgebras can always be given the structure of a Hopf algebra, i.e., that they always admit an antipode. An example is

$$S = \{e,\ s_1,\ s_2;\ s_1^2 = s_2,\ s_1 s_2 = s_2 s_1 = s_2^2 = s_2\}$$

and with $e$ a unit element. A simple calculation shows that there cannot be an antipode in this case. Another example is the multiplicative group bialgebra

$$\mathbf{Z}[X], \quad \mu(x) = 1 \otimes X + X \otimes X + X \otimes 1,$$

but in this case, there is an antipode if $Z[X]$ is completed to the power-series ring $\mathbf{Z}[[X]]$, which makes this one a sort of trivial counterexample.

**Proposition.** *Let $S$ be a partial semigroup without unit element with a partial order on it such that $pq > p$ for all $q$ and such that for all $s \in S$*

$$\#L(s) < \infty, \qquad \text{where} \quad L(s) = \{t \in S : t < s\}.$$

*Then the bialgebra $\mathcal{Z}(S)$ has an antipode.*

The proof is straightforward, starting with the minimal elements, i.e., those for which $L(s) = \varnothing$. This is by no means the most general statement that can be proved concerning antipodes for the bialgebras $\mathcal{Z}(S)$.

For any ring $R$ with unit element and semigroup $S$, let

$$M_S(R) = \left\{1 + \sum a_s s : s \in S,\ a_s \in R\right\}$$

be the semigroup of "1-units" of $R[S]$, where $R[S]$ is the semigroup algebra of $S$ over $R$ (without, however, identifying the unit element of $S$ (if it has one) with the unit of $R[S]$). Then the semigroup valued functor $R \mapsto M_S(R)$ is represented by $\mathcal{Z}(S)$.

**Remark.** There are some obvious variants of the construction of the $\mathcal{Z}(S)$ as given above, for instance the following two.

Again let the underlying algebra be the free associative algebra in $Z_s$, $s \in S$. But now, define the comultiplication by

$$\mu(Z_s) = \sum_{ut=s} Z_u \otimes Z_t.$$

Denote this "bialgebra" by $\mathcal{Z}_0(S)$. The word bialgebra is in quotes because it is not always the case that there is a corresponding counit.

For $S$ a matrix partial semigroup such as the one depicted in Fig. 2 (which is, of course, the $3 \times 3$ case), $\mathcal{Z}_0(S)$ does have a natural counit, viz.

$$\varepsilon(Z_{ij}) = \delta_{ij}$$

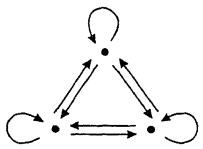

Fig. 2

and the resulting bialgebra is the matrix-function bialgebra of matrix comultiplication. The construction $\mathcal{Z}(S)$ itself also gives this matrix-function bialgebra but "shifted" (see Sec. 15 below). This construction is perhaps less appropriate here because the "pure shuffle" part of the multiplication in the dual comes from $1 \otimes Z$ and $Z \otimes 1$ parts of the comultiplication.

A third variant is as follows. Let now $M$ be a partial monoid, i.e, there is a twosided unit element $e$. The underlying algebra is now $\mathbf{Z}\Big\langle Z_m : m \in M \setminus \{e\}\Big\rangle$, and $Z_e$ is identified with 1. The comultiplication formula is the same as above, i.e.,

$$\mu(Z_s) = \sum_{ut=s} Z_u \otimes Z_t$$

and there is a counit given by

$$\varepsilon(Z_m) = 0 \quad \forall m \in M \setminus \{e\}.$$

Denote the result of this construction by $\mathcal{Z}_{00}(M)$. Clearly $\mathcal{Z}(S) = \mathcal{Z}_{00}(S \cup \{e\})$, where $S \cup \{e\}$ is the partial monoid obtained by adding a new (artificial) twosided unit element $e$. There are corresponding "GOSA's: $\mathrm{GOSA}_0$ and $\mathrm{GOSA}_{00}$.

## 14. The Simplest GOSA

Possibly the simplest partial semigroup is the one-element $S = \{s; s^2 = s\}$. Let us see what the corresponding GOSA looks like, i.e., $\mathrm{GOSA}(\{s\})$. The dual is the ring of polynomials in one variable $\mathbf{Z}[X]$ with comultiplication $X \mapsto 1 \otimes X + X \otimes X + 1 \otimes X$, i.e., the multiplicative (formal) group. The possible words on $\{s\}$ are strings of $n$ $s$'s and are conveniently coded by some symbol as $\langle n \rangle$. The multiplication on $\mathrm{GOSA}(\{s\})$ is given by the explicit formula

$$\langle n \rangle \langle m \rangle = \sum_{i=0}^{\min\{m,n\}} \left( \frac{(n+m-i)!}{(n-i)!(m-i)!i!} \right) \langle n+m-i \rangle.$$

Let $P = P_{\mathrm{finite}}(\mathbf{N} \cup \{0\})$ be the set of all finite subsets of the set of the nonnegative integers. For each $n \in \mathbf{N} \cup \{0\}$ write down its dyadic expansion

$$n = a_0 + a_1 2 + a_2 2^2 + \cdots + a_k 2^k, \quad a_i \in \{0, 1\},$$

and define

$$\xi(n) = \{i : a_i \neq 0\} \in P.$$

Give $P$ a semigroup structure by means of the union operation.

**Theorem.** *The map $\langle n \rangle \mapsto \xi(n) \in P$ defines an isomorphism*

$$\xi : \mathrm{GOSA}(\{s\}) \otimes \mathbf{Z}/(2) \to \mathbf{Z}/(2)[P],$$

*where the target is the semigroup algebra of the semigroup $P$ over $\mathbf{Z}/(2)$.*

For details, see [10].

## 15. Matrix-Function Algebras

Consider the partial semigroup of $n^2$ elements defined as follows

$$M_n = \left\{ s_{ij} : i,j \in \{1,\dots,n\};\ s_{ij}s_{jk} = s_{ik},\ \text{other products undefined} \right\}$$

(the "matrix-product semigroup" so to speak). This can be seen as the partial semigroup of morphisms of a finite category; the case $n = 3$ is depicted above in Sec. 13. The corresponding bialgebra $\mathcal{Z}(M_n)$ is the "matrix-function bialgebra" in the sense that for any ring with unit element $R$, $\mathrm{Ring}(\mathcal{Z}(M_m), R)$ is the semigroup of $n \times n$-matrices with coefficients in $R$ under matrix multiplication. For $\alpha \in \mathrm{Ring}(\mathcal{Z}(M_n), R)$, the corresponding matrix is $A = (a_{ij})$, $a_{ij} = \alpha(Z_{ij}) + \delta_{ij}$. There is of course a corresponding "coaddition" $\sigma(Z_{ij}) = 1 \otimes Z_{ij} + Z_{ij} \otimes 1 - \delta_{ij}$ (and corresponding "cozero") making $\mathcal{Z}(M_n)$ a coring object in the category of rings. There are many "functorial" sub-matrix-rings represented by similar $\mathcal{Z}(S)$'s.

## 16. GOSA($\mathbf{N}^*$)

Another particularly interesting class of GOSA's to investigate (it seems to me) are the

$$\mathcal{G}_n = \mathrm{GOSA}(A^* \setminus \{e\}) = \mathrm{GOSA}_{00}(A^*),$$

where $A$ is an alphabet of $n$ letters, $A^*$ is the free monoid of all words over that alphabet, and $e$ stands for the empty word. The basis of this GOSA consists of all strings of words $s = [w_1, w_2, \dots, w_n]$, i.e., sentences, including the empty sentence, which serves as the unit element. Let the alphabet $A$ consist of the letters

$$A = \{y_1, y_2, y_3, \dots\} \quad \text{(finite or countable)}.$$

The length of a sentence $s$ is the sum of the lengths of the words making up that sentence. The signature of a sentence is the string $(i_1, i_2, \dots, i_k)$ of nonnegative integers, where $i_j$ is the total number of times that $y_j$ occurs in the words making up the sentence $s$. For instance,

$$\mathrm{sig}[y_1y_2, y_1, y_4y_1] = (3,1,0,1).$$

If the sentences $s_1, s_2$ have signatures $\sigma_1, \sigma_2$, then the product $s_1s_2 \in \mathcal{G}$ is the sum of basis elements which all have signature $\sigma_1 + \sigma_2$, where signatures are added componentwise.

The GOSA's $\mathcal{G}$ are highly noncommutative, and a first question might be whether they are freely generated by certain (perhaps partially commuting) generators. This is not the case. The first obstruction occurs at length 3. For signature $(1,1,1)$ one needs, modulo products of sentences of lower lengths, at least 7 generators; for instance

$$[y_1, y_2y_3],\ [y_1, y_3y_2],\ [y_2, y_1y_3],\ [y_3, y_1y_2],\ [y_1, y_2, y_3],\ [y_1, y_3, y_2],\ [y_2, y_1, y_3]$$

and then there is one relation which comes from

$$[y_1][y_2, y_3] - [y_2, y_3][y_1] + (S_3) = 0,$$

where $+(S_3)$ means "apply the nonidentity permutations from $S_3$ to the expression on the left and add all these to that expression."

Quite generally, for any three words $u, v, w \in A^*$ one has the relation

$$[u][v * w] - [v * w][u] + [v][w * u] - [w * u][v] + [w][u * v] - [u * v][w] = 0,$$

or, equivalently,

$$[u][v, w] - [v, w][u] + (S_3) = 0.$$

There are also longer length relations like

$$[y_1][y_2, y_3, y_4] - [y_2, y_3, y_4][y_1] + (C_4) = 0,$$

where $C_4$ is the cyclic group of the four permutations (1), (1234), (13)(24), (1432), and their natural generalizations for five or more $y$'s. Further there are relations such as

$$[y_1, y_2][y_3y_4] - [y_3y_4][y_1, y_2] + (A_4) = 0,$$

where $A_4$ is the alternating group on four letters. Up to and including length 4, these kinds of quadratic relations are the only ones that are needed, and one is tempted to speculate that this might be generally the case.

## 17. The Malvenuto–Reutenauer Hopf Algebra

The Leibniz–Hopf algebra $\mathcal{Z}$ of noncommutative symmetrical functions is a noncommutative generalization of the Hopf algebra of symmetrical functions. The latter one is self-dual, which $\mathcal{Z}$ cannot be, being cocommutative on the one hand and (maximally) noncommutative on the other. There exists, however, a noncommutative and noncocommutative generalization of the algebra of symmetrical functions over the integers which is self-dual. This very nice object is due to Malvenuto and Reutenauer [13]. This is a much more symmetrical animal, which has $\mathcal{M}$ as a natural quotient (and $\mathcal{Z}$ as a natural subobject), and I would suggest that the business of noncommutative symmetrical functions should perhaps be redone in this context rather than over the nonselfdual generalization $\mathcal{Z}$ of the algebra of symmetrical functions.

## Appendix. Generation mod length $n$

Let $J_n$ be the subspace of $\mathcal{M}$ spanned by all the words of length $n$ (where the length of a word $[a_1, a_2, \ldots, a_n]$ is, of course, $n$). This is an ideal in $\mathcal{M}$. If $\mathcal{M}$ is seen as the algebra of quasi-symmetrical functions, and hence as a subalgebra of the power series in $X_1, X_2, \ldots$, calculating modulo $J_n$ is exactly the same as calculating modulo $X_{n+1}, X_{n+2}, \ldots$.

Because a word of weight $n$ has length $\leq n$, to prove surjectivity of the map $\varphi : \mathbf{Z}[\mathrm{ESL}] \to \mathcal{M}$, it suffices to prove that it is surjective modulo $J_n$ for each $n$. This is entirely analogous to the case of the symmetrical functions, where to prove that a symmetrical polynomial of degree $n$ is a polynomial in the elementary symmetrical functions it suffices to work with the first $n$ elementary symmetrical functions only.

It is useful to have some terminology. We shall say that an element of $\mathcal{M}$ is AM$n$ (where $n = 2, 3, 4$, or 5 for the cases considered here) if it is in the image of $\varphi$ modulo the ideal $J_n$. (Here "AM" stands for "available modulo.")

Below there are the detailed proofs that $\varphi : \mathbf{Z}[\mathrm{ESL}] \to \mathcal{M}$ is surjective modulo $J_n$ for $n \leq 5$. These range from immediate (for $n = 2$) to rather quite messy (for $n = 5$).

**A1. Generation modulo $J_2$.** The only words of length $\leq 2$ are the words $[n]$ which correspond to the power sums

$$X_1^n + X_2^n + \cdots \in \mathrm{Qsym}_{\mathbf{Z}}(X) = \mathcal{M}.$$

These are polynomials over $\mathbf{Z}$ in the elementary symmetrical functions which, in turn, correspond to the words

$$\underbrace{[1, 1, \ldots, 1]}_{n} \in \mathrm{ESL}.$$

**A2. Generation modulo $J_3$.** Because of the above we need only consider words of length 2. Now

$$[a][b] = [a + b] + [a, b] + [b, a]$$

with induction (on weight) we can assume that all products are AM 3. Thus, it suffices to show that $[a, b]$ is AM 3 for $a \leq b$, indeed for $a < b$ because $[a, a]$ is symmetrical and hence AM$n$ for all $n$. Now $[1, n]$ is a generator (i.e., an element of ESL), and

$$[a - 1][1, b] \equiv [a, b] + [1, a + b - 1] \mod J_3,$$

and we are done. Actually, it is not difficult to show that the algebra $\mathcal{M}/J_3$ is isomorphic to the algebra over $\mathbf{Z}$ generated by the three elements $[1]$, $[1, 1]$, and $[1, 2]$ modulo the single relation

$$[1, 2]^2 \equiv [1][1, 1][1, 2] - [1][1, 1]^2.$$

Here there is a significant difference between $\mathrm{Qsym}_{\mathbf{Z}}(X)$ and $\mathrm{Sym}_{\mathbf{Z}}(X)$. In the latter case $\mathrm{Sym}_{\mathbf{Z}}(X)/J_n$ is free polynomial in $n$ generators for every $n$.

**A3. Generation modulo $J_4$.** Because of A2 we need only prove that all words of length 3 are AM 4. (This, however, will still involve more detailed consideration of words of smaller length.) Now

$$[1][a-1,b,c] \equiv [a,b,c] + [a-1,b+1,c] + [a-1,b,c+1],$$

where $\equiv$ now, of course, denotes congruence modulo $J_4$. Thus, with induction on weight and with induction on the first symbol in the words of length 3, it suffices to prove that the words of length 3 that start with a 1 are AM 4. This leaves three cases:

(1) $[1,a,b]$, $a,b>1$;
(2) $[1,1,b]$, $b \geq 1$;
(3) $[1,a,1]$, $a>1$.

The first two cases involve generators. Therefore, it remains to deal with the last one. Now

$$[1][1,a] = [2,a] + [1,a+1] + 2[1,1,a] + [1,a,1].$$

If $a$ is odd, then $[2,a]$ is in ESL; also $[1,a+1],[1,1,a] \in$ ESL. Therefore, it only remains to show that words of the form $[2,2b]$ are AM 4, where we can assume $b \geq 2$ because $[2,2]$ is symmetrical. Now

$$[1,b]^2 \equiv [2,2b] + 2[1,b+1,b] + 2[1,1,2b] + 2[2,b,b] \quad \text{and} \quad [2,b,b] \equiv [1,1,1][1,b-1,b-1].$$

This concludes this proof.

**A4. Generation modulo $J_5$.** Here, of course, $\equiv$ will denote congruence modulo $J_5$. Because of A3 it suffices to deal with words of length 4 precisely. Again, by induction on weight we can assume that all sums of nontrivial products are AM 5. The calculations involve taking care of a fair number of different cases.

**Step 1.** Words of the form $[a,b,c,d]$, $a,b,c,d \geq 2$, are AM 5.

Indeed, $[a,b,c,d] \equiv [1,1,1,1][a-1,b-1,c-1,d-1]$.

**Step 2.** Words of the form $[2,2b,2c]$, $b,c \geq 2$, are AM 5.

To see this, calculate

$$\begin{aligned}[1,b,c]^2 \equiv\ & [2,2b,2c] + 2[1,b+1,c+b,c] + 2[2,b,b+c,c] + 2[2,2b,c,c] \\ & + 2[2,2b,c,c] + 2[1,b+1,b,2c] + 2[1,1,2b,2c].\end{aligned}$$

Now all terms on the right hand side, except $[2,2b,2c]$, are generators or are AM 5 by Step 1.

**Step 3.** Words of the form $[2,2b]$ are AM 5.

If $b=1$, this is symmetrical and hence AM $n$ for all $n$; therefore, we can assume $b \geq 2$. Now calculate

$$[1,b]^2 = [2,2b] + 2[1,b+1,b] + 2[1,1,2b] + 2[2,b,b] + 4[1,1,b,b] + 2[1,b,1,b].$$

The only troublesome term is $[2,b,b]$. But if $b=2$ this is symmetrical; if $b$ is odd, this is a generator and if $b \geq 4$ and even, this is AM 5 by Step 2.

**Step 4.** Words of the form $[1,a,1,c]$ are AM 5.

If $c \geq a > 1$, these words are generators, i.e., in ESL. If $1 < c < a$, calculate

$$\begin{aligned}[1,a][1,c] = & [2,a+c] + [2,a,c] + [2,c,a] + [1,a+1,c] + [1,c+1,a] + 2[1,1,a+c] \\ & + [1,a,1,c] + 2[1,1,a,c] + 2[1,1,c,a] + [1,c,1,a].\end{aligned}$$

Now $[2,a+c]$ is either a generator or is AM 5 by Step 3. All the other terms on the right hand side, except the desired term $[1,a,1,c]$, are generators except possibly $[2,a,c]$ and $[2,c,a]$. If at least one of the $a,c$ is odd, these are generators, and if both are even these two terms are AM 5 by Step 2.

**Step 5.** Words of the form $[a,1,b,c]$, $a,b,c \geq 2$, are AM 5.

To see this, calculate

$$[a-1][1,1,b,c] \equiv [a,1,b,c] + [1,a,b,c] + [1,1,a+b-1,c] + [1,1,b,a+c-1]$$

and note that all the terms on the right, except the desired one, are generators.

**Step 6.** Words of the form $[2,2,c]$, $c \geq 2$, are AM 5.

If $c$ is odd this is a generator, and if $c = 2$, this is symmetrical. Thus we can assume that $c = 2b$, $b \geq 2$. As in Step 2, calculate

$$\begin{aligned}[1,1,b]^2 \equiv\ & [2,2,2b] + 2[1,2,b+1,b] + 2[2,1,b+1,b] + 2[2,2,b,b] \\ & + 2[2,1,1,2b] + 2[1,2,1,2b] + 2[1,1,2,2b].\end{aligned}$$

The first term on the right is the desired one, the second is a generator, the third is AM 5 by Step 5, the fourth is AM 5 by Step 1 and the last two are generators. It remains to deal with $[2,1,1,2b]$. We have

$$[1][1,1,1,2b] \equiv [2,1,1,2b] + [1,2,1,2b] + [1,1,2,2b] + [1,1,1,2b+1],$$

and all the terms on the right, except the desired one, are generators.

**Step 7.** Words of the form $[1,a,b,1]$, $a \geq 2$, $b \geq 3$, are AM 5.

To see this, calculate

$$[1][1,a,b] = [2,a,b] + [1,a+1,b] + [1,a,b+1] + 2[1,1,a,b] + [1,a,1,b] + [1,a,b,1].$$

The last term on the right is the desired one; the next to last term is a generator if $b \geq a$ and is AM 5 otherwise by Step 4 because $b \geq 3$. Except for $[2,a,b]$ the other terms on the right are generators. If one of the $a,b$ is odd, this term is a generator; if both are even and $a \geq 4$ this term is AM 5 by Step 2, and if both are even and $a = 2$ this term is AM 5 by Step 6.

**Step 8.** Words of the form $[a,b,1,c]$, $a,b,c \geq 2$, are AM 5.

This time calculate

$$\begin{aligned}[a-1,b-1][1,1,1,c] \equiv\ & [a,b,1,c] + [a,1,b,c] + [1,a,b,c] \\ & + [a,1,1,b+c-1] + [1,a,1,b+c-1] + [1,1,a,b+c-1].\end{aligned}$$

The first term on the right is the desired one, the second is AM 5 by Step 5, the third is a generator, and so is the sixth and last. Further, $b+c-1 \geq 3$. Therefore, if $a = 2$ the fifth term is a generator, and if $a \geq 3$ it is AM 5 by Step 4. It remains to deal with the fourth term. For this one consider

$$\begin{aligned}[a-1][1,1,1,b+c-1] \equiv\ & [a,1,1,b+c-1] + [1,a,1,b+c-1] \\ & + [1,1,a,b+c-1] + [1,1,1,a+b+c-1].\end{aligned}$$

The second term is again either a generator or AM 5 by Step 4, and the third and fourth are generators. Therefore, $[a,1,1,b+c-1]$ is also AM 5 and we are finished with this step.

**Step 9.** Words of the form $[a,b,c,1]$, $a,b,c \geq 2$, are AM 5.

To see this consider

$$[a-1,b-1,c-1][1,1,1,1] \equiv [a,b,c,1] + [a,b,1,c] + [a,1,b,c] + [1,a,b,c]$$

and, noting that $[1,a,b,c]$ is a generator, use Steps 7 and 8.

**Step 10.** Words of the form $[1,a,1,c]$, $a,c \geq 2$, are AM 5.

This completes the result of Step 4. However Step 4 in its original form was used for Step 8, which, in turn, will be used here. If $a, c \geq 3$ this is Step 4, and if $a \leq c$ this is a generator. Thus only the cases $[1, a, 1, 2]$, $a \geq 3$, remain. Now

$$[1][1, a-1, 1, 2] \equiv [2, a-1, 1, 2] + [1, a, 1, 2] + [1, a-1, 2, 2] + [1, a-1, 1, 3].$$

The first term on the right is AM 5 by Step 8; the second is the desired one; the third is a generator; the fourth is a generator if $a \leq 4$ and is AM 5 by Step 4 if $a \geq 4$.

**Step 11.** Words of the form $[1, a, b, 1]$, $a, b \geq 2$, are AM 5.

This completes the result of Step 7. Using Step 7 it only remains to deal with $[1, a, 2, 1]$, $a \geq 2$. To do this, consider

$$[1][1, a-1, 2, 1] \equiv [2, a-1, 2, 1] + [1, a, 2, 1] + [1, a-1, 3, 1] + [1, a-1, 2, 2].$$

First let $a \geq 3$. Then the first term is AM 5 by Step 9; the second is the desired one; the third is AM 5 by Step 7; the fourth is a generator. That takes care of this subcase. For $a = 2$, consider

$$[1][1, 2, 2] = [2, 2, 2] + [1, 3, 2] + [1, 2, 3] + 2[1, 1, 2, 2] + [1, 2, 1, 2] + [1, 2, 2, 1].$$

The last term on the right is the desired one, the first is symmetrical, and all the others are generators, taking care of this subcase.

**Step 12.** Words of the form $[3, b, c]$, $b, c \geq 3$, are AM 5.

For this case consider

$$\begin{aligned}[1,1,1][2, b-1, c-1] \equiv\ & [3, b, c] + [1, 3, b, c-1] + [3, 1, b, c-1] + [3, b, 1, c-1] + [3, b, c-1, 1] \\ & + [3, 1, b-1, c] + [1, 3, b-1, c] + [1, 2, b, c] + [3, b-1, 1, c] + [3, b-1, c, 1] \\ & + [2, b, c, 1] + [2, b, 1, c] + [2, 1, b, c]\end{aligned}$$

and note that all the terms on the right, except the desired one, are AM 5 by Steps 7–9.

**Step 13.** Words of the form $[1, 1, a, 1]$, $a \geq 5$, are AM 5.

To see this, consider

$$[2][1, 1, a-2, 1] \equiv [3, 1, a-2, 1] + [1, 3, a-2, 1] + [1, 1, a, 1] + [1, 1, a-2, 3]$$

and

$$\begin{aligned}[1,1][2, 1, a-3, 1] \equiv\ & [3, 2, a-3, 1] + [3, 1, a-2, 1] + [3, 1, a-3, 2] \\ & + [2, 2, a-2, 1] + [2, 2, a-3, 2] + [2, 1, a-2, 2], \\ [1,1][1, 2, a-3, 1] \equiv\ & [2, 3, a-3, 1] + [2, 2, a-2, 1] + [2, 2, a-3, 2] \\ & + [1, 3, a-2, 1] + [1, 3, a-3, 2] + [1, 2, a-2, 2], \\ [1,1][1, 1, a-3, 2] \equiv\ & [2, 2, a-3, 2] + [2, 1, a-2, 2] + [2, 1, a-3, 3] \\ & + [1, 2, a-2, 2] + [1, 2, a-3, 3] + [1, 1, a-2, 3].\end{aligned}$$

Combining these and using Steps 1, 7, 8, and 9 gives the desired result.

**Step 14.** Words of the form $[1, 1, a, 1]$, $a \geq 2$, are AM 5.

For $a \geq 5$, this is Step 13. Therefore, let $a \leq 4$. Consider

$$[1][1, 1, a] = [2, 1, a] + [1, 2, a] + [1, 1, a+1] + 3[1, 1, 1, a] + [1, 1, a, 1]$$

and

$$[2][1, a] = [3, a] + [1, 2+a] + [2, 1, a] + [1, 2, a] + [1, a, 2].$$

For the values of $a$ under consideration, the first term on the right in the second equation is AM 5, and the second, fourth, and fifth are generators. Thus, $[2, 1, a]$ is AM 5 for $a \leq 4$. Using this the first equation in this step gives that $[1, 1, a, 1]$ is AM 5 also for these values of $a$ and hence for all values of $a$.

**Step 15.** Words of the form $[2,1,a]$, $a \geq 2$, are AM 5.

This now follows from Step 14, using the first equation of Step 14.

**Step 16.** Words of the form $[2,a,1]$, $a \geq 2$, are AM 5.

For this, consider

$$[2][1,a] = [3,a] + [1,a+2] + [2,1,a] + [1,2,a] + [1,a,2]$$

and

$$[1][2,a] = [3,a] + [2,a+1] + [1,2,a] + [2,1,a] + [2,a,1].$$

The first equation of these two gives that $[3,a]$ is AM 5, and then the second, using also Step 3, gives the desired result.

**Step 17.** Words of the form $[1,a,1,1]$, $a \geq 2$, are AM 5.

Consider

$$\begin{aligned}[1,1][1,a] = {} & [2,a+1] + [2,1,a] + [2,a,1] + [1,2,a] + [1,a+1,1] + 2[1,1,a+1] \\ & + 3[1,1,1,a] + 2[1,1,a,1] + [1,a,1,1].\end{aligned}$$

Using Steps 3, 14, 15, and 16 the desired result follows if we can show that $[1,a+1,1]$ is AM 5. This follows directly from

$$[1][1,a+1] = [2,a+1] + [1,a+2] + 2[1,1,a+1] + [1,a+1,1]$$

and Step 3.

**Step 18.** All words of length 4 are AM 5.

This is done by induction on the first element of a word $[a,b,c,d]$ using the formula

$$[1][a-1,b,c,d] \equiv [a,b,c,d] + [a-1,b+1,c,d] + [a-1,b,c+1,d] + [a-1,b,c,d+1].$$

Thus it only remains to deal with all words of the form $[1,a,b,c]$. If $a,b,c \geq 2$, this is a generator. If precisely one of the $a,b,c$ is equal to 1, we have one of the cases

$$[1,1,b,c], \quad b,c \geq 2; \qquad [1,a,1,c], \quad a,c \geq 2; \qquad [1,a,b,1], \quad a,b \geq 2.$$

The first of these is a generator; the second and third are taken care of by Steps 10 and 11 respectively. If precisely 2 of the $a,b,c$ are equal to 1, we have one of the cases

$$[1,1,1,c], \quad c \geq 2; \qquad [1,1,b,1], \quad b \geq 2; \qquad [1,a,1,1], \quad a \geq 2.$$

The first of these is a generator, and the second and third are taken care of by Steps 14 and 17.

This concludes the proof that the conjectured generators suffice modulo length 5.

## REFERENCES


1. K. T. Chen, R. H. Fox, and R. C. Lyndon, "Free differential calculus, IV," *Ann. Math.*, **68**, 81–95 (1958).
2. E. J. Ditters, "Curves and formal (co)groups," *Inv. Math.*, **17**, 1–20 (1972).
3. E. J. Ditters, "Croupes formels," *Lect. Notes*, Université de Paris XI, Orsay (1974).
4. I. M. Gelfand, D. Krob, A. Lascoux, B. Leclerc, V. S. Retakh, and J.-Y. Thibon, "Noncommutative symmetrical functions," *Adv. Math.*, **112**, 218–348 (1995).
5. I. M. Gessel, "Multipartite $P$-partitions and inner product of skew Schur functions," In: *Contemporary Mathematics*, Vol. 34, AMS (1984), pp. 289–301.
6. I. M. Gessel and C. Reutenauer, "Counting permutations with given cycle-structure and descent set," *J. Combinatorial Theory, Series A*, **64**, 189–215 (1993).
7. M. Hazewinkel, *Formal Groups and Applications*, Academic Press (1978).
8. M. Hazewinkel, *The Leibniz–Hopf algebra and Lyndon words*, preprint, CWI (1996).

9. M. Hazewinkel, "Leibniz–Hopf algebra," In: M. Hazewinkel (ed.), *Encyclopaedia of Mathematics, Supplement* 1, KAP (1997), pp. 349–350.
10. M. Hazewinkel, *The simplest generalized overlapping shuffle algebra*, preprint, CWI (1998).
11. D. Knutson, *$\lambda$-Rings and the Representation Theory of the Symmetrical Group*, Springer (1973).
12. M. Lothaire (ed.), *Combinatorics on Words*, Addison-Wesley (1983).
13. C. Malvenuto and C. Reutenauer, "Duality between quasi-symmetrical functions and the Solomon descent algebra," *J. Algebra,* **177**, 967–982 (1994).
14. C. Reutenauer, *Free Lie Algebras*, Oxford University Press (1993).
15. A. C. J. Scholtens, *S-typical curves in noncommutative Hopf algebras*, Thesis. Free Univ. of Amsterdam (1996).
16. L. Solomon, "A Mackey formula in the group ring of a Coxeter group," *J. Algebra,* **41**, 255–268 (1976).