Quasi-Symmetric Functions

Michiel Hazewinkel
CWI
POBox 94079
1090GB Amsterdam - The Netherlands
mich@cwi.nl

Abstract. Let $\mathcal{Z}$ denote the Leibniz-Hopf algebra, which also turns up as the Solomon descent algebra, and the algebra of noncommutative symmetric functions. As an algebra $\mathcal{Z} = \mathbf{Z} < Z_1, Z_2, \cdots >$, the free associative algebra over the integers in countably many indeterminates. The co-algebra structure is given by $\mu(Z_n) = \sum_{i=0}^{n} Z_i \otimes Z_{n-i}$, $Z_0 = 1$. Let $\mathcal{M}$ be the graded dual of $\mathcal{Z}$. This is the algebra of quasi-symmetric functions. The Ditters conjecture (1972), says that this algebra is a free commutative algebra over the integers. This was proved in [13]. In this paper I give an outline of the proof and discuss a number of consequences and related matters.

1 The Algebra of Quasi-Symmetric Functions

Quasi-symmetric functions have been around since at least 1972: the algebra of quasi-symmetric functions is the graded dual of the Leibniz-Hopf algebra $\mathcal{Z}$, see below in section 3. However, they were recognized as a useful and natural generalization of the symmetric functions and given their name much more recently in connection with algebraic-combinatorical questions some 15 years ago to deal with the combinatorics of P-partitions and the counting of permutations with given descent sets, [6, 7], see also [22].

Here is the definition of *quasi-symmetric functions*. Let X be a finite or 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 a power series, $f(X) \in R[[X]]$ is called *symmetric* if for any two finite sequences of indeterminates $X_1, X_2, \cdots, X_n$ and $Y_1, Y_2, \cdots, Y_n$ from X and any sequence of exponents $i_1, i_2, \cdots, i_n \in \mathbf{N}$, 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-symmetric formal power series are a generalization introduced by Gessel, [6], in connection with the combinatorics of P-partitions. This time one takes a *totally ordered* set of indeterminates, e.g. $V = \{V_1, V_2, \cdots\}$, 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-symmetric polynomial in three variables that is not symmetric.

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

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

$$M_w = \sum_{i_1<\cdots<i_n} X_{i_1}^{a_1} X_{i_2}^{a_2} \cdots X_{i_n}^{a_n} \tag{1.1}$$

defined by w. These, clearly, form a basis over the integers of $Qsym_{\mathbf{Z}}(X)$. Below we shall usualy simply write w instead of M_w.

To see how these basis elements multiply consider the following construction for obtaining new words (compositions) from two words $w=[a_1,a_2,\cdots,a_m]$ and $v=[b_1,b_2,\cdots,b_m]$. Take a 'sofar empty' word with $n+m-r$ slots where r is an integer between 0 and $\min\{m,n\}$, $0\le r\le \min\{m,n\}$.

Choose n of the available $n+m-r$ slots and place in it the natural numbers from w in their original order; choose r of the now filled places; together with the remaining $n+m-r-n=m-r$ places these form m slots; in these place the entires from v in their orginal order; finally, for those slots which have two entries, add them. The product of two words w and v is the sum (with multiplicities) of all words that can be so obtained. So, for instance

$$\begin{aligned}[a,b][c,d] = {} & [a,b,c,d]+[a,c,b,d]+[a,c,d,b]+[c,a,b,d]+[c,a,d,b]+ \\ & +[c,d,a,b]+[a+c,b,d]+[a+c,d,b]+[c,a+d,b]+ \\ & +[a,b+c,d]+[a,c,b+d]+[c,a,b+d]+[a+c,b+d]\end{aligned} \tag{1.2}$$

and [1][1][1]=6[1,1,1]+3[1,2]+3[2,1]+[3]. It is easy to see that the recipe given above gives precisely the multiplication of (the corresponding basis) quasi-symmetric functions. If $v=[b_1,b_2,\cdots,b_m]$, then the shuffles of $a_1,\cdots,a_n;b_1,\cdots,b_m$ correspond to the products of the monomials in M_w and M_v that have no X_j in common; the other terms arise when one or more of the X's in the monomials making up M_w and M_v do coincide. In example (1.2) the first six terms are the *shuffles*; the other terms are '*overlapping shuffles*'. The term shuffle comes from the familiar rifle shuffle of cardplaying; an overlapping shuffle occurs when one or more cards from each deck don't slide along each other but stick edgewise together; then their values are added.

Oviously this construction makes sense for any (not necessarily commutative) semigroup. Even for the simplest semigroup, consisting of just the identity, an interesting (Hopf) algebra arises, [11, 14].

The algebra of quasi-symmetric functions also arises in the study of multiple harmonic series (zeta-values), [13],

$$\zeta(i_1,i_2,\cdots,i_k)=\sum_{n_1>n_2>\cdots n_k\geq 1}\frac{1}{n_1^{i_1}n_2^{i_2}\cdots n_k^{i_k}} \tag{1.3}$$

For instance $\zeta(1)\zeta(2,1)=\zeta(3,1)+\zeta(2,2)+\zeta(1,2,1)+2\zeta(2,1,1)$. In [15] the algebra of quasi-symmetric functions is realized as a subalgebra of $\mathbf{Q}\langle x,y\rangle$ with a new commutative and associative multiplication that is very different from concatenation and this is used to study (algebraic) relations between zeta-values.

Further, as already mentioned, the algebra of quasi-symmetric functions is dual to the *Leibniz-Hopf algebra*, also known as the *algebra of noncommutative symmetric functions*, see below, or, equivalently to the *Solomon descent algebra*, more precisely to the direct sum $\mathfrak{D}=\oplus_n D(S_n)$ of the Solomon descent algebras $D(S_n)$ of the symmetric groups, with a new multiplication over which the direct sum of the original multiplications is distributive. See [5, 17].

2 The Ditters Conjecture

Let the *weight* of a word $w=[a_1,\cdots,a_n]$, $a_i\in\mathbf{N}$ over the integers be $|w|=a_1+\cdots+a_n$. Then

2.1 *Theorem.* The algebra of quasi-symmetric functions over the integers is the free graded commutative polynomial algebra over $\mathbf{Z}$ with β_n generators of weight n where

$$\sum_{d|n}d\beta_d=2^n-1 \quad \text{or} \quad \beta_d=\sum_{d|n}\mu(d)(2^{n/d}-1) \tag{2.1}$$

with $\mu(d)$ the Möbius function.

For an outline of the proof of this theorem, see below. Full details are in [13]. The important part of the statement is that this holds over the *integers*, not just over the rationals.

The first statement of the Ditters conjecture dates from 1972, [2], where it was formulated as proposition 2.2. It states that the dual algebra over the integers of the Leibniz Hopf algebra, i.e. the algebra of quasi-symmetric functions, is a free commutative algebra over the integers. At that time quasi-symmetric functions had not yet been invented, nor the Solomon descent algebra.

Shortly after the publication of [2] it was remarked and acknowledged, see [3], Ch. II, §5, p. 29, that the proof of proposition 2.2, i.e. what is now called the Ditters conjecture, had gaps. Since then there have been quite a few purported proofs of the statement, published and unpublished. All have errors. For detailed remarks on the error in the proofs in [20, 21] see [14]. The latest alleged proof in [4] has at least three major errors; the worst one is more or less the same as the one in [20, 21].

The fact that his dual algebra is free polynomial over the integers is crucial for a part of the theory of noncommutative formal groups, including a noncommutative

version of p-typification, developed by Ditters and his students, see [2, 3, 21] and the references cited therein. Some remarks on these applications can be found below in sections 5 and 6.

Perhaps even more importantly, the Leibniz-Hopf algebra is precisely the same as the algebra of noncommutative symmetric functions as defined in [5] and further developed in a slew of subsequent papers. The fact that the symmetric functions constitute a free algebra in the elementary symmetric functions is rather important. Thus the fact that the algebra of quasi-symmetric functions is free over the integers is likely to be of some significance. The name 'Ditters conjecture' for the statement I coined myself a few years back. In [10], I referred to the statement as the Ditters-Scholtens theorem. This was when I still believed the proof in [20, 21] to be correct.

3 Outline of the Proof of the Ditters Conjecture

The *Leibniz Hopf algebra* over the integers is the free associative algebra $\mathcal{Z} = \mathbf{Z}\langle Z_1, Z_2, \cdots \rangle$ over $\mathbf{Z}$ in countably many generators with the comultiplication

$$\mu(Z_n) = \sum_{i+j=n} Z_i \otimes Z_j, \quad Z_0 = 1 \tag{3.1}$$

Its graded dual over the integers is denoted $\mathcal{M}$. It is not difficult to see that this dual is precisely the algebra of quasi-symmetric functions over the integers. Indeed, for any composition $c = (i_1, \cdots, i_n)$, define m_c by the dual basis formula $< m_c, Z_d > \; = \delta_{c,d}$ where $Z_d = Z_{j_1} Z_{j_2} \cdots Z_{j_m}$ for a composition $d = (j_1, \cdots, j_m)$. It is now a simple exercise to check that the m_c multiply exactly as the quasi-symmetric monomials M_c, defined above in section 1.

Over the rationals the Leibniz-Hopf algebra is isomorphic to the *Lie Hopf algebra*

$$\mathcal{U} = \mathbf{Z}\langle U_1, U_2, \cdots \rangle, \quad \mu(U_n) = 1 \otimes U_n + U_n \otimes 1 \tag{3.2}$$

For this consider the expression $1 + Z_1 t + Z_2 t^2 + Z_3 t^3 + \cdots = \exp(U_1 t + U_2 t^2 + U_3 t^3 + \cdots)$ which gives an expression for each Z_i in terms of the $U_1, \cdots, U_i$ with rational coefficients, and hence defines an algebra homomorphism $\beta: \mathcal{Z} \otimes \mathbf{Q} \to \mathcal{U} \otimes \mathbf{Q}$, which can be (rather easily) seen to be an isomorphism of Hopf algebras; see [8] for details.

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

A *proper tail* of a word $[a_1, \cdots a_n]$ is a word of the form $[a_i, \cdots a_n]$ 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 *LYN*.

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

$$w = v_1 * v_2 * \cdots * v_k, \quad v_i \in LYN, \ v_1 \geq v_2 \geq \cdots \geq v_k \tag{3.3}$$

For example: $[2,3,1,3,1,4,1,3,1,1] = [2,3]*[1,3,1,4]*[1,3]*[1]*[1]$.

Let $\mathcal{N}$ be the graded dual of $\mathcal{U}$ over the integers. This is the socalled *shuffle algebra* An important theorem, for example in the theory of free Lie algebras, states that th algebra $\mathcal{N} \otimes_{\mathbf{Z}} \mathbf{Q}$ is commutative free polynomial in the Lyndon words, see e.g. [19 It is not true that $\mathcal{N}$ is free polynomial over the integers. The Ditters conjecture state that the algebra $\mathcal{M}$, on the contrary, is free polynomial commutative over the integers This makes it a rather more beautiful version of $\mathcal{N}$, in the sense that $\mathcal{M}$ is a $\mathbf{Z}-$(form of $\mathcal{N}$ (i.e. $\mathcal{M} \otimes_{\mathbf{Z}} \mathbf{Q} \simeq \mathcal{N} \otimes_{\mathbf{Z}} \mathbf{Q}$) with the property that $\mathcal{M}$ is a free polynomia algebra while $\mathcal{N}$ is not.

It is straightforward to adapt the proof that $\mathcal{N} \otimes_{\mathbf{Z}} \mathbf{Q}$ is free polynomial over th rationals to a proof that $\mathcal{M} \otimes_{\mathbf{Z}} \mathbf{Q}$ is free polynomial in the Lyndon words, see [14] o [15] or [17]. (This does not follow from the isomorphism $\mathcal{M} \otimes_{\mathbf{Z}} \mathbf{Q} \simeq \mathcal{N} \otimes_{\mathbf{Z}} \mathbf{Q}$.)

A word $w = [a_1, a_2, \cdots, a_n] \in \mathbf{N}^*$ is called *elementary* if the greatest common divisc of its symbols is 1, $\gcd\{a_1, a_2, \cdots, a_n\} = 1$. A *concatenation power* of w (or *sta power*) is a word of the form $w^{*m} = w * w * \cdots * w$ (m factors). Let *ESL* denote the se of words which are star powers of elementary Lyndon words. For instance, the word [1,1,1,1], [1,2,1,2], [1,2,1,4] are in *ESL* (but the first two are not Lyndon), and th words [4], [2,4] are not in *ESL* but are in *LYN*.

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

There is a p-adic analogue of the strong Ditters conjecture, and the first step i establishing the Ditters conjecture is to prove these local versions for all prime number p.

Let us start with the formulation. A word $w = [a_1, \cdots, a_n]$ on $\mathbf{N}$ is *p-elementary* where p is a prime number, if the gcd of the $a_1, \cdots, a_n$ is not divisible by p. A p-star-power of a word is a word of the form $w = v * v * \cdots * v$ (p^r factors). The se *ESL*(p) is the set of words which are p-star-powers of p-elementary Lyndon words.

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

$$\mathcal{M} \otimes \mathbf{Z}_{(p)} = \mathbf{Z}_{(p)}[ESL(p)] \tag{3.4}$$

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

To prove this theorem two preliminary lemmas are used.

3.3 *Lemma* (cardinality of the sets $ESL(p)$). The number of elements in $ESL(p)$ of weight n is β_n, i.e. it is the same as that in LYN_n, the set of Lyndon words of weight n.

Proof. Let $w=[a_1,a_2,\cdots,a_m]$ be a Lyndon word of weight n. Let p^r be the largest power of the prime number p that divides the greatest common divisor $\gcd(a_1,\cdots,a_m)$. Now assign to w the word $v*v*\cdots*v$ (p^r factors), where $v=[p^{-r}a_1,p^{-r}a_2,\cdots,p^{-r}a_m]$. This sets up a bijective correspondence between LYN_n and $ESL(p)_n$, the set of words in $ESL(p)$ of weight n.

3.4 *Lemma.* Let $n=a_0+a_1p+\cdots+a_kp^k$, $a_i\in\{0,1,\cdots,p-1\}$ be the p-adic expansion of a natural number n. Then the multinomial coefficient

$$\binom{n}{\underbrace{p^k\cdots p^k}_{a_k\ times}\underbrace{p^{k-1}\cdots p^{k-1}}_{a_{k-1}\ times}\cdots\underbrace{1\cdots 1}_{a_0\ times}} \tag{3.5}$$

is nonzero modulo p.

Proof of the p-adic Ditters conjecture. We use the following ordering of words: length first and then lexicographic ordering on words of equal length. So e.g. $[1,1,1,1]>[1,2,1]>[1,1,2]>[4]$. Let $SL(p)$ be the set of all p-star powers of Lyndon words; i.e. words of the form $w=v^{*p^k}$, $v\in LYN$. 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 **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

$$w=v_1^{*n_1}*v_2^{*n_2}*\cdots v_m^{*n_m},\ v_i\in Lyn,\ v_1>v_2>\cdots>v_m \tag{3.6}$$

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

$$\prod_{i=1}^{k_1}v_1^{*n_{1i}}\prod_{i=1}^{k_2}v_2^{*n_{2i}}\cdots\prod_{i=1}^{k_1}v_m^{*n_{mi}} \tag{3.7}$$

where the products are overlapping shuffle products and where $n_{i1}+\cdots n_{ii_k}=n_i$, $i=1,\cdots,m$. 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 a product of multinomial coefficients:
For instance if one takes $n_{ij}=1$ for all i, j (which is what is done to prove

$\mathcal{M} \otimes \mathbf{Q} = \mathbf{Q}[Lyn])$, 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. The resulting coeeficient is then a product of expressions of the form (3.5) and hence nonzero modulo p by lemma 3.4, and, hence, invertible in $\mathbf{Z}_{(p)}$. This proves that also w can be written as a polynomial in $SL(p)$.

Now, for a given weight n, let $w_1, w_2, \cdots w_m$ be all the words of that weight that are in $SL(p)$ but are not p-elementary. So, if $w_i = [a_{i1}, \cdots, a_{ik_i}]$, $p \mid \gcd\{a_{i1}, \cdots, a_{ii_i}\}$. Let $b_{ij} = p^{-1}a_{ij}$, $v_i = [b_{i1}, \cdots, b_{ik_i}]$. Now consider the overlapping shuffle powers v_i^p. It is easy to see that these are of the form

$$v_i^p = w_i + p(\text{something of weight } n) \tag{3.8}$$

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

$$\begin{aligned} a_{11}w_1 + \cdots + a_{1m}w_m &\equiv 0 \\ &\vdots \\ a_{m1}w_1 + \cdots + a_{mm}w_m &\equiv 0 \end{aligned} \tag{3.9}$$

where the matrix $A = (a_{ij})$ has the property $A \equiv I_m \mod p$. This means that the determinant of the matrix A is invertible in $\mathbf{Z}_{(p)}$, so that the $w_1, \cdots, w_m$ can be eliminated. This proves that the elements from $ESL(p)$ suffice to generate all of $\mathcal{M} \otimes \mathbf{Z}_{(p)}$ over $\mathbf{Z}_{(p)}$. Using lemma 3.5 above on the cardinality of $ESL(p)$, a counting argument finishes the proof. In more detail, let A be the free graded algebra over $\mathbf{Z}_{(p)}$ with β_n generators of weight n. Let γ_n be the rank of the free $\mathbf{Z}_p$ module of elements of weight n. The γ_n are of course recursively determined by the β_n, but the precise formula is not important here. The algebra $\mathbf{Z}_{(p)}[ESL(p)]$ viewed as the free commutative algebra over $\mathbf{Z}_{(p)}$ generated by the symbols from $ESL(p)$ is of course the same thing as A. By what has been proved the natural homomorphism $\mathbf{Z}_{(p)}[ESL(p)] \xrightarrow{\alpha} \mathcal{M} \otimes \mathbf{Z}_{(p)}$ that sends a symbol from $ESL(p)$ to the corresponding element from $\mathcal{M} \otimes \mathbf{Z}_{(p)}$ is surjective. Both algebras are torsion free, and after tensoring with the rationals the dimensions of their homogeneous parts of weight n are equal by the lemma above and the isomorphism between the overlapping shuffle algebra and the shuffle algebra. It follows that α is an isomorphism because surjective homomorphisms between free $\mathbf{Z}_{(p)}$ modules of equal rank are necessarily isomorphisms.

Proof of the main theorem 2.1. Using the p-adic theorem one can now prove the main theorem 2.1 as follows.

Let $\mathcal{M}_n$ be the graded part of weight n of $\mathcal{M}$. By the fact that $\mathcal{M}_n$ is a free

Abelian group and the fact that $\mathcal{N}\otimes_{\mathbf{Z}}\mathbf{Q} \simeq \mathcal{M}\otimes_{\mathbf{Z}}\mathbf{Q}$, we know that $\mathcal{M}_n$ is a free Abelian group of rank γ_n. Let G_n be defined by the short exact sequence

$$\bigoplus_{j=1}^{n-1}(\mathcal{M}_j\otimes\mathcal{M}_{n-j})\longrightarrow\mathcal{M}_n\longrightarrow G_n\longrightarrow 0 \tag{3.10}$$

where the first arrow is given by multiplication. Each G_n is a finitely generated Abelian group. Tensoring with $\mathbf{Z}_{(p)}$ (which is right exact) gives the corresponding exact sequence for $\mathcal{M}\otimes\mathbf{Z}_{(p)}$ and it follows from the p-adic version of the Ditters conjecture proved above that $G_n\otimes_{\mathbf{Z}}\mathbf{Z}_{(p)}$ is a free $\mathbf{Z}_{(p)}$ module of rank β_n for each prime number p. This implies that G_n is a free Abelian group of rank β_n and proves that the algebra of symmetric functions can be generated by a set of homogeneous elements $y_{n,1},y_{n,2},\cdots,y_{n,\beta_n}$, $n=1,2,\cdots$, giving a homogenous surjective ring homomorphism $\mathbf{Z}[Y]\xrightarrow{\alpha}\mathcal{M}$ where $\mathbf{Z}[Y]$ is the graded ring generated by symbols Y_{n,i_n}, $n=1,2,\cdots$; $i_n=1,\cdots,\beta_n$ of weight n. However, the homogenous parts of weight n of $\mathbf{Z}[Y]$ and $\mathcal{M}$ both are free Abelian groups of rank n. It follows immediately that the homogeneous components, $\alpha_n:\mathbf{Z}[Y]_n\to\mathcal{M}_n$ of α are isomorphisms and hence that α itself is an isomorphism.

4 Divided Power Sequences and Endomorphisms of $\mathcal{Z}$

Let H be a Hopf algebra with unit element $1\in H$. A *primitive element* in H is an element d such that $\mu(d)=1\otimes d + d\otimes 1$. The primitive elements in H form a Lie algebra under the commutator bracket $[d,d']=dd'-d'd$ denoted $L(H)$. Let $\mathcal{L}=L(\mathcal{Z})$.

A *divided power sequence* (of infinite length) in H (over d) is a sequence of elements

$$d_0=1,d_1=d,d_2,d_3,\cdots \text{ such that } \mu(d_n)=\sum_{i+j=n}d_i\otimes d_j \text{ for all } n=0,1,2,\cdots \tag{4.1}$$

A divided power series of length k is a sequence $d_0=1,d_1=d,d_2,d_3,\cdots,d_k$ such that (4.1) holds for all n up to and including k.

A divided power series of infinite length in H is the same thing as a homomorphism of Hopf algebras $\mathcal{Z}\to H$, the homomorphism corresponding to $1,d_1,d_2,\cdots$ being given by $Z_i\mapsto d_i$.

Examples of primitive elements in $\mathcal{Z}$ are the 'power sums'

$$p_n=\sum_{i_1+\cdots+i_k=n}(-1)^{n+k}i_1Z_{i_1}Z_{i_2}\cdots Z_{i_k} \tag{4.2}$$

Because of the Hopf algebra isomorphism $\mathcal{Z}\otimes_{\mathbf{Z}}\mathbf{Q}\simeq\mathcal{U}\otimes_{\mathbf{Z}}\mathbf{Q}$, $\mathcal{L}\otimes_{\mathbf{Z}}\mathbf{Q}$ is the free Hopf algebra on countably many generators over the rationals. And in fact the p_n of (4.2) above form a free generating set.

It is definitely not true that $\mathcal{L}$ is a free Lie algebra over $\mathbf{Z}$; it is a much m complicated object that is still imperfectly understood.

It is an immediate consequence of theorem 2.1 that

4.1 *Theorem.* Every primitive element of $\mathcal{Z}$ extends to an (infinite length) divi power series. More generally, every finite length divided power series can be exten to an infinite length one.

To see this we use the construction of certain free co-algebras. Let B be a graded module over the integers $\mathbf{Z}$(or over any ring R) whose homogenous summa are of finite rank, and let B^* be its graded dual. The *free graded cofree algebra* c the integers, CoF(B), determined by B is the graded dual of the free associa graded algebra, $\mathrm{Fr}(B^*)$, over the integers generated by B^*. It can be characterizec a universal property that is dual to that of free associative algebras as follows (tho that is not important here). It comes with a canonical map $\pi:\mathrm{CoF}(B)\to B$, the gra dual of the canonical map $B^*\to \mathrm{Fr}(B^*)$, and satisfies the following property: every graded map of a graded coalgebra C to the module B, $C\xrightarrow{\varphi} B$, there unique morphism of graded coalgebras $C\xrightarrow{\psi}\mathrm{CoF}(B)$ such that $\pi\psi=\varphi$.

The cofree coalgebra CoF(B) can be explicitly described as follows. Take tensor module

$$T(B)=\mathbf{Z}\oplus B\oplus B^{\otimes 2}\oplus B^{\otimes 3}\oplus\cdots \qquad (1$$

There are natural isomorphisms $\varphi_{i,j}: B^{\otimes i}\otimes B^{\otimes j}\longrightarrow B^{\otimes(i+j)}$; $i,j=0,1,2,\cdots$ .U these, the comultiplication on $T(B)$ is defined by

$$\mu(b_1\otimes b_2\otimes\cdots\otimes b_n)=\sum_{i=0}^{n}\varphi_{i,n-i}^{-1}(b_1\otimes b_2\otimes\cdots\otimes b_n) \qquad (1$$

The cofree coalgebra CoF(B) has a unique group like element, viz $1\in\mathbf{Z}$ (which i dual of the augmentation of $\mathrm{Fr}(B^*)$). The *primitives* of CoF(B), are the elemen $B\subset T(B)$. In CoF(B) every primitive element b can be extended to a divided p sequence of infinite length. Indeed one such sequence is

$$b,\ b\otimes b,\ b\otimes b\otimes b,\ \cdots$$

It is also true that any divided power sequence of length n can be extended to o length infinity. This follows easily by induction because if $\delta_1,\delta_2,\cdots,\delta_n$ and $\delta_1,\delta_2,\cdot$ are two different divided power sequences that agree up to degree $n-1$, the difference of the last terms, $\delta_n-\delta_n'$, is a primitive.

The free cocommutative graded coalgebra, CCoF(B), over B, is the subcoal of CoF(B) of symmetric tensors. It is the graded dual of the commutative free al generated by B^* as the maximal commutative quotient of $\mathrm{Fr}(B^*)$.

Now as the graded dual of the free graded algebra $\mathcal{M}$, $\mathcal{Z}$ is cofree graded and theorem 4.1 follows by the remarks above. (Note that the elements of (4.5) are symmetric tensors.)

4.2 *Corollary.* The set of Hopf algebra endomorphisms of $\mathcal{Z}$ is very large being in bijective correspondence with the set of all infinite sequences $q_1, q_2, q_3, \cdots, q_i \in \mathcal{L}$.

See also section 5 below for more on the Hopf algebra endomorphisms of $\mathcal{Z}$.

Remark. The free commutative coalgebra over B, which satisfies the same universal property for not necessarily graded coalgebras and morphisms is not CoF(B), but a certain recursive completion; see [12] for details.

5 Formal Groups I: Curves and Classification

An n-dimensional *formal group* over a commutative ring A with unit element is an n-tuple

$$F_i(X,Y) \in A[[X_1, X_2, \cdots X_n; Y_1, Y_2, \cdots, Y_n]] = A[[X;Y]], \quad i = 1, \cdots, n \tag{5.1}$$

of formal power series in $2n$ (commuting) variables $X_1, X_2, \cdots X_n; Y_1, Y_2, \cdots Y_n$ such that

$$F_i(X,Y) \equiv X_i + Y_i \text{ mod(degree 2)}, \; F(X, F(Y,Z)) = F(F(X,Y),Z) \tag{5.2}$$

in $A[[X;Y;Z]]$. I.e. a formal group is given by a co-associative comultiplication $R(F) \to R(F) \hat{\otimes} R(F)$, where $R(F) = A[[X]]$ and $\hat{\otimes}$ is the completed tensor product of power series rings, for which $\varepsilon: R(F) \to A$, $X_i \mapsto 0$, $i = 1, \cdots, n$ is a co-unit. The existence of an antipode is then automatic. $R(F)$ is called the *contravariant bi-algebra* of the formal group. Its continuous linear dual

$$U(F) = \mathrm{Hom}_A(R(F), A) \tag{5.3}$$

is a Hopf algebra in the usual sense of the word and is called the *covariant bi-algebra* of the formal group. A formal group is the algebraic counterpart of (the infinitesimal part) of an (analytic) Lie group near the identity. Their interest lies in the fact that they can be considered over any commutative ring with unit element. The theory of formal groups has many applications (in number theory, in algebraic topology, in algebraic geometry, ...); see [8] for some of them.

A *curve* $\gamma(t) = (\gamma_1(t), \cdots, \gamma_n(t))$ in a formal group is an n-tuple of formal power series in one variable t with coefficients in A without constant terms. Two curves can be multiplied by the formula $\gamma(t)\delta(t) = F(\gamma(t), \delta(t))$ and this turns the set of curves into a group, denoted $\mathcal{C}(F;A)$. There are natural subgroups, $\mathcal{C}^m(F;A)$ consisting of

the curves that are congruent zero modulo (degree m), and the group of curves is complete with respect to the topology defined by these subgroups.

There are a number of obvious operators defined on the group of curves: the homothety operators $\langle a\rangle$ and Verschiebungs operators $\mathbf{V}_n$ defined by

$$\mathbf{V}_m\gamma(t)=\gamma(t^m),\quad m=1,2,\cdots;\quad \langle a\rangle\gamma(t)=\gamma(at),\quad a\in A \tag{5.4}$$

For commutative formal groups there are in addition the socalled *Frobenius operators*, which are defined as follows. For a curve $\gamma(t)$ consider the expression

$$\gamma(x_1t^{1/m})\gamma(x_2t^{1/m})\cdots\gamma(x_mt^{1/m}) \tag{5.6}$$

with coefficients in $A[x_1,\cdots,x_m]$ where the x_i are additional (commuting) indeterminates. Because the formal group is commutative, the coefficients in (5.6) are symmetric polynomials in the x_i which can therefore be written in terms of the elementary symmetric functions $e_1,\cdots,e_m$. Do so, and now substitute $e_1=\cdots=e_{m-1}=0$, $e_m=(-1)^{m-1}$. The result is a an n-tuple of power series in t, not just $t^{1/m}$, and this is by definition the curve $\mathbf{f}_m\gamma(t)$. Combining all these operators turns the commutative group into module over a quite large ring denoted Cart(A) and as such the groups of curves are classifying for commutative formal groups.

The functorial group (with operators; i.e. module) $\mathcal{C}(F;A)$ is also representable. The representing object is the infinite dimensional formal group W of the Witt vectors of which the covariant bi-algebra $U(W)$ is the *Witt vector Hopf algebra*

$$\mathbf{Z}[X_1,X_2,\cdots],\quad \mu(X_n)=\sum_{i+j=n}X_i\otimes X_j,\quad \varepsilon(X_n)=0 \tag{5.7}$$

where $X_0=1$, the commutative analogue of the Leibniz Hopf algebra. It also turns out that the Hopf algebra endomorphisms over A of $U(W)$ identify with Cart(A). For all this see [8].

Now let's turn to not necessarily commutative formal groups. For these the definition of Frobenius operators as above for the commutative case does not work. It is clear (from the commutative case) that if the group of curves is to contain a great deal of information on the formal group from which it comes, then that group should have a large collection of operators defined on it. As we shall see, the freeness of the dual $\mathcal{M}$ of the Leibniz Hopf algebra $\mathcal{Z}$ implies that there is indeed a very large number of functorial operators on curves including a large number of 'Frobenius type' ones.

To do this we first reinterprete the notion of curves in a formal group F in terms of its covariant bi-algebra. A curve $\gamma(t)\in\mathcal{C}(F;A)$ is simply a continuous algebra homomorphism $R(F)=A[[X]]\to A[[t]]$, the components of $\gamma(t)$ being the images of the X_i. Taking continuous linear duals we find a co-algebra homomorphism $CF_A\to U(F)$, where CF_A is the co-algebra

$$CF_A = A \oplus AX_1 \oplus AX_2 \oplus \cdots$$
$$\mu(X_n) = \sum_{i+j=n} X_i \otimes X_j, \quad X_0 = 1; \quad \varepsilon(X_i) = 0, \ i \neq 0, \ \varepsilon(X_0) = 1 \tag{5.8}$$

Now consider the images of the X_i (which completely determine the co-algebra morphism). This gives a sequence of elements

$$d_0 = 1, d_1, d_2, \cdots, \ d_i \in U(F) \ \text{ with the property } \ \mu(d_n) = \sum_{i+j=n} d_i \otimes d_j \tag{5.9}$$

i.e. a divided power series in the Hopf algebra $U(F)$. Thus a curve in a formal group F is the same thing as a divided power series in its covariant Hopf algebra. Let $\mathcal{Z}_A = \mathcal{Z} \otimes_{\mathbf{Z}} A$. Then it immediately follows that

$$\mathrm{Hopf}_A(\mathcal{Z}_A, U(F)) = \mathcal{C}(F; A), \quad \alpha \mapsto (1, \alpha(Z_1), \alpha(Z_2), \cdots) \tag{5.10}$$

Now the graded linear dual of $\mathcal{Z}$ is a free polynomial algebra; it follows that the (non-graded) dual of $\mathcal{Z}_A$ is a power series algebra and so (5.10) says that also in the noncommutative case the functor of curves is representable by a formal group; as it is in the commutative case. Writing a divided power series $d_0 = 1, d_1, d_2, \cdots$ as a power series $1 + d_1 t + d_2 t^2 + \cdots$ with coefficients in the (as a rule noncommutative) covariant bialgebra $U(F)$, multiplication of curves corresponds to multiplication of power series. All this is well known and already in [2], see also [8].

The next bit is new and is only the beginning of something that needs to be explored in great detail and much deeper. Take an additional set of commuting indeterminates $x_1, x_2, \cdots$ (which also commute with the Z_j) and consider the ordered product

$$(1 + x_1 Z_1 t + x_1^2 Z_2 t^2 + x_1^3 Z_3 t^3 + \cdots) \ \cdots \ (1 + x_n Z_1 t + x_n^2 Z_2 t^2 + x_n^3 Z_3 t^3 \cdots) \ \cdots \tag{5.11}$$

5.1 *Proposition.* The expression (5.11) is equal to

$$1 + \sum_w M_w(x_1, x_2, \cdots) Z_w t^{|w|} \tag{5.12}$$

where the sum is over all nonempty words $w = [a_1, a_2, \cdots, a_k]$, $a_i \in \{1, 2, \cdots\}$ over the natural numbers, $|w| = a_1 + \cdots + a_k$ is the weight of w and $Z_w = Z_{a_1} Z_{a_2} \cdots Z_{a_k}$, and $M_w(x_1, x_2, \cdots)$ is the quasi-symmetric function defined by the word w (see (1.4) above.

The proof is straightforward.

Now take any algebra homomorphism φ: $\mathcal{M} \to A$. This gives a new divided power series in $\mathcal{Z}$, viz

$$d_0 = 1, d_1, d_2, \cdots, \; d_j = \sum_{|w|=j} \varphi(M_w) Z_w \qquad (5.$$

and hence a Hopf algebra endomorphism of $\mathcal{Z}_A$ given by $Z_j \mapsto d_j$, and, by representability of $\mathcal{C}(F;A)$ by $\mathcal{Z}_A$, functorial operations on the groups of cur Because $\mathcal{M}$ is free polynomial there are very many such operations. An alge homomorphism from $\mathcal{M}$ to $\mathbf{Z}$ is a certain kind of element in the completion $\hat{\mathcal{Z}}$ o For suitable divided power series (not all yield convergent series), w $g = 1 + d_1 + d_2 + d_3 + \cdots \in \hat{\mathcal{Z}}$. Then g is group-like: $\mu(g) = g \otimes g$ and hence quali Indeed, we then have $\langle g, ab\rangle = \langle \mu(g), a \otimes b\rangle = \langle g, a\rangle\langle g, b\rangle$. This brings us bac divided power series again (which is of little use if one does not already know there are very many of them).

In addition there are all kind of 'Frobenius like' operations (and of course stil Verschiebung and homothety operations). These 'Frobenius like' operations are de as follows. In (5.11) replace t by $t^{1/m}$. Instead of (5.12) one then finds the s expression but with $t^{|w|/m}$ instead of $t^{|w|}$. Now take a homorphism φ that is zero o the free polynomial generators of weight not a multiple of m. Then the resulting s will be in t instead of just $t^{1/m}$ (easy to see) and we obtain a new divided power s and new operations. Again, because $\mathcal{M}$ is free graded, there are very many of the

It remains to be investigated what one can do with all these operations instance, in the context of p-typification (see the section below). And also wha be said about the collection of Hopf endomorphisms of $\mathcal{Z}$. This set is a noncommu group (each endomorphism corresponds uniquely to a divided power series in these can be multiplied); in addition there is composition of endomorphisms an is both left and right distributive over the multiplication. Thus we have a kind o whose underlying group is noncommutative.

The same point of view can be taken in the commutative case. Her endomorphisms of $U(\mathbb{W})$ form the ring Cart($\mathbf{Z}$) which has an explicit descripti terms of Frobenius, Verschiebung, and homothety operators, see [8]. It will be inter to sort out how the endomorphisms that come from algebra homomorphisms fro graded dual of $U(\mathbb{W})$ to $\mathbf{Z}$ fit in. Note that the graded dual of $U(\mathbb{W})$ is the alge symmetric functions. (The Witt vector Hopf algebra is selfdual.)

6 Formal Groups II: p-typification

For the moment, till the last paragraph in this section, all formal groups v commutative. One tool that is of considerable usefulness in the study of comm formal groups is p-typification. In a sense they can be treated 'one prime at a For instance two commutative formal groups over the the integers are isomor and only of they are isomorphic over the localizations $\mathbf{Z}_{(p)}$, the ring of all r numbers with denominators prime to p, for all prime numbers p. Let me descri some of p-typification theory in the commutative case.

For the moment, let F be a formal group over an integral domain A; let $Q(A)$ be its quotient field. Then there exist a unique n-tuple of power series $f(X) \in Q(A)[[X]]$, $f(X) \equiv X$ mod (degree 2), such that $F(X,Y) = f^{-1}(f(X) + f(Y))$, called the logarithm of F. (i.e. over the ring of fractions F is (strictly) isomorphic to the additive formal group). Such a formal group is p-typical if its logarithm is of the form

$$f(X) = \sum_{i=0}^{\infty} m_i X^{p^i} \tag{6.1}$$

where X^{p^i} is short for the column vector with entries $X_j^{p^i}$ and the m_i are matrices with coefficients in the field of fractions. Over a $\mathbf{Z}_{(p)}$-algebra every formal group is isomorphic to a p-typical one. The notion can also be defined for formals groups over rings that are not necessarily integral domains and the same result holds.

A curve $\gamma(t)$ in a commutative formal group over an integral domain (not necessarily p-typical) is a p-typical curve if $f(\gamma(t))$ is of the form

$$f(\gamma(t)) = \sum a_i t^{p^i} \tag{6.2}$$

for suitable vectors a_i. This is equivalent to the property that $\mathbf{f}_q \gamma(t) = 0$ for all Frobenius operators $\mathbf{f}_q$, q a prime different from p. For formal groups and curves over arbitrary rings A, this property is the definition. These are, therefore, see (6.2), very economical curves (to borrow a term from [21]), depending on few parameters. They also suffice to describe all curves in the sense that every curve is a unique shifted (= apply a Verschiebung operator) product (= sum in the present commutative case) of p-typical curves. See [8] for much more.

Now let F be a not necessarily commutative formal group. The question arises whether there is a suitable generalization of all this in that case. Whether there still exist a suitable substitute for Frobenius operators in the noncommutative case is unclear at best. So something else has to be found. This provided much of the orginal motivation for the study of $\mathcal{Z}$ and its graded dual $\mathcal{M}$. A quite elaborate (and complicated) theory has been developed, starting with [3} and, so far, finishing with [21], The principal tool is theorem 4.3 on the possibility of extending any finite length curve (= finite length divided power series) in $\mathcal{Z}$ to an infinite length one.

7 The MPR Hopf algebra

The Hopf algebra $\mathcal{Z}$ (i.e. the Leibniz Hopf algebra = algebra of noncommutative symmetric functions = Solomon descent algebra) is a magnificent object. And so is its dual, the algebra of quasi-symmetric functions $\mathcal{M}$. Both deserve still far more study than the already considerable attention they have had. They have one blemish compared to their (co)commutative analogues, the Witt vector Hopf algebra (= Hopf algebra of symmetric functions) $\mathcal{X} = \mathbf{Z}[X_1, X_2, \cdots] = U(\mathcal{W})$, which is selfdual.

There exists, however, a selfdual noncocommutative, noncommutative Hopf algebra $\mathcal{R}$, invented by Malvenuto, Poirier and Reutenauer, see [17, 18], that contains $\mathcal{Z}$ and covers $\mathcal{M}$; both in a very natural way. This is a possibly even more beautiful and rewarding object and has so far been little studied.

References.

1. K T Chen, R H Fox, R C Lyndon, *Free differential calculus IV*, Ann. Math. **68** (1958), 81-95.
2. E J Ditters, *Curves and formal (co)groups*, Inv. Math. **17** (1972), 1-20.
3. E J Ditters, *Groupes formels*, Notes d'un cours, Université de Paris XI, Orsay, 1974. Chapître II, §5, p. 29.
4. E J Ditters, A C J Scholtens, *Free polynomial generators for the Hopf algebra QSym of quasisymmetric functions*, J. pure and applied Algebra, **144** (1999), 213-227.
5. Israel M Gelfand, Daniel Krob, Alain Lascoux, Bernard Leclerc, Vladimir S Retakh, Jean-Yves-Thibon, *Noncommutative symmetric functions*, Adv. Math. **112** (1995), 218-348.
6. Ira M Gessel, *Multipartite P-partitions and inner product of skew Schur functions*. In: Comtemporary Mathematics **34**, Amer. Math. Soc., 1984, 289-301.
7. Ira M Gessel, Christophe Reutenauer, *Counting permutations with given cycle-structure and descent set*, J. Combinatorial Theory, Series A: **64** (1993), 189-215.
8. Michiel Hazewinkel, *Formal groups and applications*, Academic Press, 1978.
9. Michiel Hazewinkel, *The Leibniz-Hopf algebra and Lyndon words*, preprint, CWI,, 1996.
10. Michiel Hazewinkel, *Leibniz-Hopf algebra*, In: Encyclopaedia of Mathematics, Supplement volume I, KAP, 1997, 349-350.
11. Michiel Hazewinkel, *The simplest generalized overlapping shuffle algebra*, Preprint, CWI, Amsterdam, 1997.
12. Michiel Hazewinkel, *Cofree co-algebras and recursiveness*, Preprint, CWI, Amsterdam, 1999.
13. Michiel Hazewinkel, *The algebra of quasi-symmetric functions is free over the integers*, Prepint, CWI, Amsterdam, March 1999. Submitted Inventiones Math.
14. Michiel Hazewinkel, *Generalized overlapping shuffle algebras*. In: Proceedings Pontryagin memorial conference, Moscow 1998, to appear 2000.
15. M E Hoffman, *The algebra of multiple harmonic series*, J. of Algebra **194** (1997), 477-495.
16. M Lothaire (ed.), *Combinatorics on words*, Addison-Wesley, 1983.
17. C Malvenuto, Chr Reutenauer, *Duality between quasi-symmetric functions and the Solomon descent algebra*, J. of Algebra **177** (1994), 967-982.
18 S Poirier, Chr Reutenauer, *Algèbres de Hopf de tableaux*, Ann. Sc. Math. Québec **19** (1995), 79-90.
19. Chr Reutenauer, *Free Lie algebras*, Oxford University Press, 1993.
20. A C J Scholtens, *On the graded dual of the noncommutative universal Leibniz Hopf algebra Z*, Preprint, Math. Sem. Free Univ. of Amsterdam, 1994.
21. A C J Scholtens, *S-typical curves in non-commutative Hopf algebras*, thesis, Free University of Amsterdam, 1996.
22. R P Stanley, *On the number of reduced decompositions of elements of Coxeter groups*, Eur. J. Combinatorics **5** (1984), 359-372.
23. Moss E. Sweedler, *Hopf algebras*, Benjamin, 1969, 336pp.