On Dynkin and Klyacho idempotents in graded bialgebras

Frédéric Patras
CNRS UMR 6621
Université de Nice, Mathématiques
Parc Valrose
06108 Nice cedex 2
France
patras@math.unice.fr

Christophe Reutenauer
IRMA
7,rue rené Descartes
67084 Strasbourg
France
reutenau@math.u-strasbg.fr

1 Introduction

Let $X = \{x_1, ..., x_n, ...\}$ be an infinite alphabet. The tensor algebra on X has canonically the structure of a Lie algebra and its Lie subalgebra generated by the elements of X identifies with the free Lie algebra on X. The structure of the tensor algebra and of the free Lie algebra are closely related to certain permutation statistics, as emphasized e.g. in [8] and [16]. In this setting, the Dynkin and Klyachko idempotents are fundamental tools. For example, they reduce the construction of basis of the free Lie algebra to the study and counting of given words, such as Lyndon words.

The purpose of the present article is to show that these constructions, that could be thought of as intrinsically related to the combinatorics of the tensor bialgebra generalize in fact to all graded connected cocommutative bialgebras. Recall that, by the Cartier-Milnor-Moore theorem, these bialgebras are, up to isomorphism, the enveloping algebras of graded connected Lie algebras. We establish in particular a Baker-like identity and describe explicitly the kernels of the natural generalizations to these bialgebras of the Dynkin and Klyachko operators (Thm 6, Cor.7 and Th.15).

This provides new computational and conceptual tools for studying these bialgebras. A striking consequence is the following: it is a well-known property of the free Lie algebra that its bases are canonically in bijection with prime circular words; the generalized Klyachko idempotent allows to extend this property to each graded bialgebra. As an application, we construct a Klyachko basis of the free partially commutative Lie algebra that is parametrized by prime conjugation classes or, equivalently, by Lalonde's Lyndon elements in the free partially commutative monoid.

These results rely on two general ideas that seem to be interesting on their own. First, we introduce the notion of pseudo-coproducts for the endomorphisms of a graded bialgebra. It appears to be the right generalization to endomorphisms of the usual coproduct on the descent algebra [13], [10]. In particular, pseudo-coproducts are compatible in a strong sense (see Th.2) with the two natural products on the endomorphisms (the convolution and the composition products). The second key ingredient are certain remarkable and intriguing circular identities (see Cor.9). When interpreted as cyclotomic identities, they yield the properties of the generalized Klyachko idempotents. In the course of the proof, we also generalize the Klyachko congruences ([11], [16] p.198) on the major index of a permutation.

2 Pseudo-coproducts

Let A be a cocommutative bialgebra over a field $\mathbf{F}$ of characteristic 0. We denote by $\epsilon : \mathbf{F} \to A$ the unit of A, by $\eta : A \to \mathbf{F}$ the counit, by $\delta : A \to A \otimes A$ the coproduct and by $\pi : A \otimes A \to A$ the product. On $End(A)$ there exists the associative *convolution* product $*$, defined by $f * g = \pi \circ (f \otimes g) \circ \delta$, for which $\nu := \epsilon \circ \eta$ is the neutral element. Recall that an element a of A is *primitive* if $\delta(a) = a \otimes 1 + 1 \otimes a$; the set of primitive elements is denoted by $Prim(A)$; it is a Lie subalgebra of A.

It happens that certain convolution subalgebras of $End(A)$ have a coproduct Δ in such a way that they become a bialgebra. The most classical example is the *descent algebra*: A being the tensor bialgebra over an infinite dimensional vector space, the descent algebra is generated as a convolution algebra by the graded projections of A. The coproduct Δ has moreover the compatibility property

$$\Delta(f) \circ \delta = \delta \circ f \qquad (*),$$

for any element f of the subalgebra under consideration.

However this situation is rather rare. Even in the case of descent algebras of graded bialgebras (see[15]), there is not always a coproduct Δ satisfying $(*)$: see the Appendix for a counter-example. This justifies the following definition.

Definition 1 *An element f of $End(A)$ admits $F \in End(A) \otimes End(A)$ as a* pseudo-coproduct *if $F \circ \delta = \delta \circ f$. If f admits the pseudo-coproduct $f \otimes \nu + \nu \otimes f$, we say that f is* pseudo-primitive.

In general, an element of $End(A)$ may admit several pseudo-coproducts. However, this concept is very flexible, as shows the following result.

Theorem 2
- *If f, g admit the pseudo-coproducts F, G and $\alpha \in \mathbf{F}$, then $f+g, \alpha f, f * g, f \circ g$ admit respectively the pseudo-coproducts $F+G, \alpha F, F * G, F \circ G$, where the products $*$ and $\circ$ are naturally extended to $End(A) \otimes End(A)$.*
- *An element $f \in End(A)$ takes values in $Prim(A)$ if and only if it is pseudo-primitive.*

Proof. 1. Let $F = \sum_{i\in I} f_1^i \otimes f_2^i$ and $G = \sum_{j \in J} g_1^j \otimes g_2^j$. In the sequel of the article, we use the Sweedler conventions to abbreviate such expressions to $F = \sum f_1 \otimes f_2$ and $G = \sum g_1 \otimes g_2$. For example we shall write $F \otimes G = \sum f_1 \otimes f_2 \otimes g_1 \otimes g_2$ instead of $\sum_{i\in I}\sum_{j\in J} f_1^i \otimes f_2^i \otimes g_1^j \otimes g_2^j$, and so on. Then we have

$$F * G = \sum (f_1 \otimes f_2) * (g_1 \otimes g_2) = \sum (f_1 * g_1) \otimes (f_2 * g_2)$$

$$= \sum (\pi \circ (f_1 \otimes g_1) \circ \delta) \otimes (\pi \circ (f_2 \otimes g_2) \circ \delta) = \sum (\pi \otimes \pi) \circ (f_1 \otimes g_1 \otimes f_2 \otimes g_2) \circ (\delta \otimes \delta)$$

$$= \sum (\pi \otimes \pi) \circ (I \otimes T \otimes I) \circ (f_1 \otimes f_2 \otimes g_1 \otimes g_2) \circ (I \otimes T \otimes I) \circ (\delta \otimes \delta),$$

where I denotes the identity of A and $T(a \otimes b) = (b \otimes a)$. Thus

$$F * G = (\pi \otimes \pi) \circ (I \otimes T \otimes I) \circ (F \otimes G) \circ (I \otimes T \otimes I) \circ (\delta \otimes \delta).$$

Denote by $\delta^{[i]} : A \to A^{\otimes i}$ the i-th iterated coproduct on A and by $\pi^{[i]}$ the i-th fold product of A. In particular, $\delta^{[4]} = (\delta \otimes \delta) \circ \delta$. Since A is cocommutative, we have $(I \otimes T \otimes I) \circ \delta^{[4]} = \delta^{[4]}$. Thus

$$(F * G) \circ \delta = (\pi \otimes \pi) \circ (I \otimes T \otimes I) \circ (F \otimes G) \circ (I \otimes T \otimes I) \circ (\delta \otimes \delta) \circ \delta$$

$$= (\pi \otimes \pi) \circ (I \otimes T \otimes I) \circ (F \otimes G) \circ (\delta \otimes \delta) \circ \delta = (\pi \otimes \pi) \circ (I \otimes T \otimes I) \circ ((F \circ \delta) \otimes (G \circ \delta)) \circ \delta$$

$$= (\pi \otimes \pi) \circ (I \otimes T \otimes I) \circ ((\delta \circ f) \otimes (\delta \circ g)) \circ \delta,$$

since f, g have pseudo-coproducts F, G. Hence

$$(F * G) \circ \delta = (\pi \otimes \pi) \circ (I \otimes T \otimes I) \circ (\delta \otimes \delta) \circ (f \otimes g) \circ \delta = \delta \circ \pi \circ (f \otimes g) \circ \delta,$$

since δ is an algebra endomorphism of A. Finally

$$(F * G) \circ \delta = \delta \circ (f * g),$$

what was to be shown.

The other assertions are easier and are left to the reader.

2. Since η is the counit of A, we have for any element a of A: $(I \otimes \nu + \nu \otimes I) \circ \delta(a) = a \otimes 1 + 1 \otimes a$. Hence $(f \otimes \nu + \nu \otimes f) \circ \delta(a) = f(a) \otimes 1 + 1 \otimes f(a)$. Therefore the image of f is contained in $Prim(A)$ if and only if $\delta \circ f = (f \otimes \nu + \nu \otimes f) \circ \delta$, what was to be shown. ■

A an application of pseudo-coproducts, we give a short proof of a result of Gelfand, Krob, Lascoux, Leclerc, Retakh, Thibon, [10] Cor.5.17. We consider the descent algebra Σ of the tensor bialgebra A on an infinite dimensional vector space V: as a subalgebra of $End(A)$ with convolution, Σ is generated by the graded projections $p_n : A \to A_n$, viewed as elements of $End(A)$. It is a bialgebra, with coproduct defined by $\Delta(p_n) = \sum_{i+j=n} p_i \otimes p_j$; cf. [13], [10].

Corollary 3 *An element f of Σ_n is primitive if and only if its image is contained in $Prim(A)$. In this case, it is quasi-idempotent, that is, $f^2 = \alpha f$ for some scalar α.*

Proof. Note that $\Delta(p_n)$, as defined above, is a pseudo-coproduct for p_n. Since pseudo-coproducts are by the theorem closed under convolution, since the p_n generate Σ as a convolution subalgebra of $End(A)$, and since Σ is a bialgebra, we deduce that for any $f \in \Sigma$, $\Delta(f)$ is a pseudo-coproduct for f.

If $f \in \Sigma_n$ is primitive, f is therefore also pseudo-primitive and the theorem shows that $Im(f) \subset Prim(A)$. Conversely, if this holds, then f has the pseudo-coproducts $f \otimes \nu + \nu \otimes f$ (by the theorem) and $\Delta(f)$ (by what has just been said). But the equation $F \circ \delta = \delta \circ f$ determines $F \in End(A) \otimes End(A)$ uniquely, by Schur-Weyl duality, since V has infinite dimension. Hence both pseudo-coproducts are equal and f is primitive.

Now, by definition of Σ, f is a linear combination of products $p_I = p_{i_1} * \ldots * p_{i_k}$, where the i_j are positive integers which add up to n. If $k > 1$, and a is in $Prim(A)_n$, we have $p_I(a) = \pi^{[k]} \circ (p_{i_1} \otimes \ldots \otimes p_{i_k}) \circ \delta^{[k]}(a) = 0$, since $\delta^{[k]}(a) = a \otimes 1 \otimes ... \otimes 1 + 1 \otimes a \otimes ... \otimes 1 + 1 \otimes 1 \otimes ... \otimes a$. Thus $f(a) = \alpha a$, where α is the coefficient of p_n in the linear combination. This concludes the proof. ∎

3 The Dynkin idempotent

Let A be a graded cocommutative Hopf algebra over the field $\mathbf{F}$ of characteristic 0, with $A_0 = \mathbf{F}$ (that is, A is connected). Define D in $End(A)$ by $D(a) = na$ if $a \in A_n$. Now define $l \in End(A)$ by

$$l(a) = S * D,$$

where S is the *antipode* of A, that is, the inverse of the identity of A in the convolution algebra.

In the classical case, A is the tensor bialgebra over an infinite dimensional vector space; equivalently the algebra of noncommutative polynomials in infinitely many variables, the latter being primitive. In this case l is the *Dynkin operator* that maps $x_1...x_n$ onto the Lie polynomial $[...[[x_1, x_2], x_3], ..., x_n]$, for any variables $x_1, ..., x_n$. The definition $l = S * D$ of the Dynkin operator is essentially due to von Waldenfels [18], see also [16], Th.1.12.

The next result is the analogue of the theorem of Dynkin [7], Specht [17], Wever [19].

Theorem 4 *If a is primitive, then $l(a) = D(a)$.*

Proof. We have $l(a) = (S * D)(a) = \pi \circ (S \otimes D) \circ \delta(a) = \pi \circ (S \otimes D)(a \otimes 1 + 1 \otimes a) = \pi(S(a) \otimes D(1) + S(1) \otimes D(a)) = D(a)$, since $D(1) = 0$ and $S(1) = 1$. ∎

Theorem 5 *The image of l is contained in $Prim(A)$.*

Proof. By Th.2, it is enough to show that l is pseudo-primitive. Note that $S \otimes S$ is a pseudo-coproduct for S. Indeed, $(S \otimes S) \circ \delta$ and $\delta \circ S$ are both anti-homomorphisms of A into $A \otimes A$, sending each $a \in Prim(A)$ onto $-a \otimes 1 - 1 \otimes a$; since A is graded cocommutative and connected, it is canonically isomorphic to the enveloping algebra of the Lie algebra of its primitive elements (Th. of Cartier-Milnor-Moore), and in particular is generated by them as an algebra, and the property follows.

Furthermore, $D = \sum_n np_n$; hence D admits the pseudo-coproduct $D \otimes I + I \otimes D$, as is easily verified. Thus by Th.2, l admits the pseudo-coproduct

$$(S\otimes S)*(D\otimes I+I\otimes D)=(S*D)\otimes(S*I)+(S*I)\otimes(S*D)=l\otimes\nu+\nu\otimes l.$$

■

The next result extends to all connected cocommutative graded bialgebras Baker's identity [1], see also [16] p.36. We denote $A_+ = \oplus_{n>0} A_n$.

Theorem 6 *For any a in A_+ and b in A, one has $l(al(b)) = [l(a), l(b)]$.*

Before giving the proof, we derive two corollaries. The first one extends a result of Cohn [3].

Corollary 7 *The kernel of l is spanned by 1 and the elements of the form $al(a)$, $a \in A$.*

Proof. By Th.6, $al(a)$ is in $Ker(l)$. For the converse, it is enough to show that the kernel is spanned by the elements $al(b) + bl(a)$, $a, b \in A$. Since A is a graded cocommutative bialgebra, we may write for any a in A_n: $\delta(a) = a \otimes 1 + 1 \otimes a + \sum(a_1 \otimes a_2 + a_2 \otimes a_1)$. Now $l = S * D$ hence $D = I * l = \pi \circ (I \otimes l) \circ \delta$; thus $na = \pi \circ (I \otimes l)(a \otimes 1 + 1 \otimes a + \sum(a_1 \otimes a_2 + a_2 \otimes a_1)) = \pi(I(a) \otimes l(1) + I(1) \otimes l(a) + \sum(I(a_1) \otimes l(a_2) + I(a_2) \otimes l(a_1))$ $= l(a) + \sum a_1 l(a_2) + a_2 l(a_1)$, which implies the result. ■

Corollary 8 *If $a_1, ..., a_n$ are homogeneous primitive elements of A, then $l(a_1...a_n) = deg(a_1)[...[[a_1, a_2], a_3], ..., a_n]$.*

When A is the tensor algebra over a vector space V and the a_is are elements of V, we recover the original definition of the Dynkin operator in the classical case, by means of left-to-right bracketing. Note the remarkable fact that the Dynkin idempotent outputs the degree of the first factor of the Lie monomial; it has to be compared to a result of [2], Th.1.5 (b).

Proof. If $n = 1$, it is Th.4 . We then have by induction, Th.4 and Th.6:

$$l(a_1...a_{n+1}) = (1/deg(a_{n+1}))l(a_1...a_n l(a_{n+1})) = (1/deg(a_{n+1}))[l(a_1...a_n), l(a_{n+1})]$$

$$= [l(a_1...a_n), a_{n+1}] = deg(a_1)[...[[a_1, a_2], a_3], ..., a_{n+1}].$$

■

Corollary 9 *If $a \in A_+$ and $b \in Prim(A)$, then $l(ab) = [l(a), b]$. In particular, $Ker(l) \cap A_+$ is a right A-submodule of A.*

We give a convolutional proof of the generalized Baker's identity.

Proof of Th.6. Recall that T is the endomorphism of $A \otimes A$ sending $a \otimes b$ onto $b \otimes a$. We have to show that $\alpha = l \circ \pi \circ (I \otimes l)$ and $\pi \circ (l \otimes l) \circ (I \otimes I - T)$ coincide on $A_+ \otimes A$.

We use several facts:

1. δ is an algebra endomorphism, so that $\delta \circ \pi = (\pi \otimes \pi) \circ (I \otimes T \otimes I) \circ (\delta \otimes \delta)$.
2. S is an anti-automorphism of A, so that $S \circ \pi = \pi \circ T \circ (S \otimes S)$ and $S \circ \nu = \nu$.
3. S sends each primitive element onto its opposite, thus $S \circ l = -l$.
4. D is a derivation of A, so that $D \circ \pi = \pi \circ (I \otimes D + D \otimes I)$ and $D \circ \nu = 0$.
5. l is pseudo-primitive, hence $\delta \circ l = (l \otimes \nu + \nu \otimes l) \circ \delta$.
6. $\pi \circ (\pi \otimes \pi) = \pi^{[4]}$.
7. Denote by T' the endomorphism of $A^{\otimes 3}$ sending $a \otimes b \otimes c$ onto $c \otimes a \otimes b$; then $(T \otimes I \otimes I) \circ (I \otimes T \otimes I) = T' \otimes I$.

We obtain

$$\alpha = (S * D) \circ \pi \circ (I \otimes l) = \pi \circ (S \otimes D) \circ \delta \circ \pi \circ (I \otimes l)$$

$$= \pi \circ (S \otimes D) \circ (\pi \otimes \pi) \circ (I \otimes T \otimes I) \circ (\delta \otimes \delta) \circ (I \otimes l)$$

$$= \pi \circ (\pi \otimes \pi) \circ (T \otimes I \otimes I) \circ (S \otimes S \otimes I \otimes D + S \otimes S \otimes D \otimes I) \circ (I \otimes T \otimes I)$$

$$\circ (I \otimes I \otimes l \otimes \nu + I \otimes I \otimes \nu \otimes l) \circ (\delta \otimes \delta)$$

$$= \pi^{[4]} \circ (T \otimes I \otimes I) \circ (I \otimes T \otimes I) \circ (S \otimes I \otimes S \otimes D + S \otimes D \otimes S \otimes I)$$

$$\circ (I \otimes I \otimes l \otimes \nu + I \otimes I \otimes \nu \otimes l) \circ (\delta \otimes \delta)$$

$$= \pi^{[4]} \circ (T' \otimes I) \circ (S \otimes I \otimes \nu \otimes (D \circ l) + S \otimes D \otimes (-l) \otimes \nu + S \otimes D \otimes \nu \otimes l) \circ (\delta \otimes \delta).$$

Now, A is a bialgebra, so that $(\nu \otimes I) \circ \delta(x) = 1 \otimes x$ for $x \in A$, and consequently, for any endomorphism f of A, $(\nu \otimes f) \circ \delta(x) = 1 \otimes f(x)$. Thus

$$\pi^{[4]} \circ (T' \circ I) \circ (S \otimes I \otimes \nu \otimes (D \circ l)) \circ (\delta \otimes \delta)(a \otimes b)$$

$$= \pi^{[4]} \circ (T' \otimes I) \circ (((S \otimes I) \circ \delta(a)) \otimes 1 \otimes (D \circ l)(b))$$

$$= \pi^{[3]} \circ (((S \otimes I) \circ \delta(a)) \otimes (D \circ l)(b))$$

$$= \pi^{[3]} \circ (S \otimes I \otimes (D \circ l)) \circ (\delta \otimes I)(a \otimes b).$$

We leave the similar computation of the 2 other terms to the reader; then

$$\alpha = \pi^{[3]}\circ(S\otimes I\otimes(D\circ l))\circ(\delta\otimes I)-\pi^{[3]}\circ(l\otimes S\otimes D)\circ(I\otimes\delta)\circ T+\pi^{[3]}\circ(S\otimes D\otimes l))\circ(\delta\otimes I)$$

$$= \pi\circ(\pi\otimes I)\circ(S\otimes I\otimes(D\circ l))\circ(\delta\otimes I)-\pi\circ(I\otimes\pi)(l\otimes S\otimes D)\circ(I\otimes\delta)\circ T$$

$$+\pi\circ(\pi\otimes I)\circ(S\otimes D\otimes l)\circ(\delta\otimes I)$$

$$= \pi\circ((\pi\circ(S\otimes I)\circ\delta)\otimes(D\circ l)-(l\otimes(\pi\circ(S\otimes D)\circ\delta))\circ T+(\pi\circ(S\otimes D)\circ\delta)\otimes l))$$

$$= \pi\circ(\nu\otimes(D\circ l)-(l\otimes l)\circ T+l\otimes l),$$

since $S*I=\nu$ and $S*D=l$. This ends the proof since ν vanishes on A_+.
■

Remark

The operator l is the analogue of the operator "left-to-right bracketing". There exists of course a symmetric version, corresponding to the "right-to left bracketing". Evidently it is given by $r = D*S$.

One can interpolate between l and r by defining $P = S^\alpha * D * S^\beta$, where α,β are two elements of the ground field with $\alpha+\beta=1$; note that the convolution power S^α is defined using the usual binomial expansion of $(1+x)^\alpha$, once S is written $S=\nu+S'$, where S' annihilates $A_0=\mathbf{F}$. Then one proves, similarly to Th.4 and Th.5, that: 1. If a is primitive, then $P(a)=D(a)$. 2. The image of P is contained in $Prim(A)$.

The previous definition of the operator P, interpolating between l and r, and its properties, were obtained some time ago by Claudio Procesi and the second author, during a discussion on noncommutative symmetric functions.

4 Circular identities

In this section we establish two sets of identities which have a circular symmetry. They will be used in the next section, but they have their own interest.

Let $s=(x_1,...,x_p)$ be a sequence of elements of a field. We assume that the product $x_1x_2...x_p$ is equal to 1, and that each subproduct is different from 1. Let t be a variable. The identity we want to prove is the following:

$$\sum_{k\geq 0} t^k \sum_{p\geq i\geq 1} \frac{(x_{i+1}...x_p)^k}{(1-x_{i+1})(1-x_{i+1}x_{i+2})...(1-x_{i+1}x_{i+2}...x_{i+p-1})}$$

$$= 1+(-1)^{p-1}\frac{x_2x_3^2...x_p^{p-1}t^p}{(1-x_2...x_pt)(1-x_3...x_pt)...(1-x_pt)(1-t)},$$

where the subscripts have to be taken modulo p. For example, if $p = 3$, one has

$$\sum_{k\geq 0}[\frac{1}{(1-x_1)(1-x_1x_2)}+\frac{x_3^k}{(1-x_3)(1-x_3x_1)}+\frac{x_2^kx_3^k}{(1-x_2)(1-x_2x_3)}]t^k$$

$$=1+\frac{x_2x_3^2t^3}{(1-t)(1-x_3t)(1-x_2x_3t)}.$$

Before proving these identities, we derive the following consequence, obtained by taking the coefficient of t^k in the previous identity, where again the subscripts have to be taken modulo p.

Corollary 10 *For $k = 0, 1, ..., p - 1$,*

$$\sum_{p\geq i\geq 1}\frac{(x_{i+1}...x_p)^k}{(1-x_{i+1})(1-x_{i+1}x_{i+2})...(1-x_{i+1}x_{i+2}...x_{i+p-1})}=\delta_{0,k}.$$

Proof of the identity. Note that that after eliminating x_1, the remaining x_is are subject to no condition, except that the partial products of them have to be different from 1. The identity is then equivalent to a polynomial one. So we can assume that the $p - 1$ remaining elements and t are free commuting variables; then we may expand the fractions into series, and prove the identity. We have

$$\sum_{k\geq 0}\sum_{p\geq i\geq 1}\frac{(x_{i+1}...x_pt)^k}{(1-x_{i+1})...(1-x_{i+1}...x_p)(1-x_{i+1}...x_px_1)...(1-x_{i+1}...x_px_1...x_{i-1})}.$$

Note that $x_{i+1}...x_px_1 = (x_2...x_i)^{-1}$ and that $x_{i+1}...x_px_1...x_{i-1} = x_i^{-1}$. Thus, since $(1 - x^{-1})^{-1} = -x(1 - x)^{-1}$, the previous sum is equal to

$$\sum_{k\geq 0}\sum_{p\geq i\geq 1}\frac{(x_{i+1}...x_pt)^k(-1)^{i-1}x_2x_3^2...x_i^{i-1}}{(1-x_2...x_i)...(1-x_i)(1-x_{i+1})...(1-x_{i+1}...x_p)}$$

$$=\sum_{p\geq i\geq 1}(-1)^{i-1}\frac{x_2x_3^2...x_i^{i-1}}{(1-x_2...x_i)...(1-x_i)(1-x_{i+1})...(1-x_{i+1}...x_p)(1-x_{i+1}...x_pt)}.$$

Now we expand into formal power series in the variables $x_2, ..., x_p, t$ and obtain

$$\sum_{p\geq i\geq 1}(-1)^{i-1}\sum_{0<n_2<...<n_i,n_{i+1}\geq...\geq n_p\geq n}x_2^{n_2}...x_p^{n_p}t^n.$$

Denote by S_i the formal power series represented by the last summation, and by L_i its support. A nice fact is that the coefficients of S_i are 0 or 1. Then for $i \geq 2$, $L_i = \{m = x_2^{n_2}...x_p^{n_p}t^n | 0 < n_2 < ... < n_i, n_{i+1} \geq ... \geq n_p \geq n\}$ and $L_1 = \{m | n_2 \geq ... \geq n_p \geq n\}$.

We verify that if $i + 2 \leq j$, then $L_i \cap L_j$ is empty. Indeed, since $p > j - 1 \geq i + 1$, L_i is defined by conditions one of which is $n_{j-1} \geq n_j$ and, since $2 \leq j - 1$, L_j, among others, by the condition $n_{j-1} < n_j$.

Suppose now that $i \neq 1, p$. We verify that then for each monomial m in L_i, m is either in L_{i-1} or in L_{i+1}. Indeed, if $n_i < n_{i+1}$, then m is in L_{i+1}; if on the contrary $n_i \geq n_{i+1}$, then m is in L_{i-1}.

We verify now that for m in L_1, m is in L_2 or $m = 1$; and that if m is in L_p, then m is in L_{p-1}, except if m satisfies the condition $0 < n_2 < ... < n_p < n$. This will imply the identity in view of

$$\sum_{0<n_2<...<n_p<n} x_2^{n_2}...x_p^{n_p}t^n = \frac{x_2x_3^2...x_p^{p-1}t^p}{(1 - x_2...x_pt)(1 - x_3...x_pt)...(1 - x_pt)(1 - t)}.$$

So, let m be in L_1; then clearly m is in L_2, except if $n_2 = 0$, and then $m = 1$. Finally, let m be in L_p; if $n_p \geq n$, then $m \in L_{p-1}$; if $n_p < n$, then $0 < n_2 < ... < n_p < n$.

■

Let $s = (x_1, ..., x_p)$. For $\sigma \in S_p$, denote by $Maj_s(\sigma)$ the product

$$\prod_{i \in Des(\sigma)} x_{\sigma(1)}...x_{\sigma(i)},$$

where $Des(\sigma)$ is the *descent set* of σ, that is, the set $\{i, 1 \leq i \leq p-1, \sigma(i) > \sigma(i+1)\}$. Let also $\bar{D}(\sigma)$ the set of *circular descents* of σ, that is, the set $\{i, 1 \leq i \leq p, \sigma(i) > \sigma(i+1)\}$, with numbers taken modulo p. Let $\bar{d}(\sigma)$ denote the number of *circular descents* of σ. In other word, descents are circular descents, and p is a circular descent if and only if $\sigma(p) > \sigma(1)$. Note that if the product of the x_i is equal to 1, an hypothesis which will be assumed in what follows, then $Maj_s(\sigma)$ is also equal to the product $\prod x_{\sigma(1)}...x_{\sigma(i)}$ over all circular descents i of σ.

Lemma 11 *Let γ be the p-cycle $(p, p-1, ..., 1)$. If $x_1...x_p = 1$, then:*

1. $\bar{d}(\sigma\gamma) = \bar{d}(\sigma)$.
2. $Maj_s(\sigma\gamma) = x_{\sigma(p)}^{\bar{d}(\sigma)} Maj_s(\sigma)$.

3. $Maj_s(\sigma) = x_p Maj_{s\gamma}(\gamma^{-1}\sigma)$, *where* $s\gamma = (x_p, x_1, ..., x_{p-1})$.

Proof Note that $\bar{D}(\sigma\gamma) = \{i+1, i \in \bar{D}(\sigma)\}$, with numbers taken modulo p. Hence 1. follows. Moreover $\sigma\gamma(1) = \sigma(p)$ so that the product $\prod x_{\sigma\gamma(1)}...x_{\sigma\gamma(i)}$ over all circular descents i of $\sigma\gamma$ is equal to $x_{\sigma(p)}^{\bar{d}(\sigma)} Maj_s(\sigma)$. Hence 2. follows.

Note that i is a circular descent of $\gamma^{-1}\sigma$ if and only if either i is a circular descent of σ and $\sigma(i) \neq p$, or $\sigma(i+1) = p$ and in this case $i+1$ is a circular descent of σ. If we put $s\gamma = (y_1, ..., y_p)$, then $y_{\gamma^{-1}\sigma(i)} = x_{\sigma(i)}$. Thus the product $\prod y_{\gamma^{-1}\sigma(1)}...y_{\gamma^{-1}\sigma(i)}$ over all circular descents i of $\gamma^{-1}\sigma$ is equal to $x_p^{-1} Maj_s(\sigma)$.

■

5 The Klyachko idempotent

The bialgebra A is as in Section 3. We assume here that the field $\mathbf{F}$ of scalars (which is of characteristic 0) contains a primitive n-th root of unity ω_n for any $n \geq 1$. Denoting as before by p_n the graded projection $A \to A_n$, viewed as an element of $End(A)$, we write $p_C = p_{i_1} * ... * p_{i_l}$ for any composition $C = (i_1, ..., i_l)$, $i_j \in \mathbf{N}^*$. Define elements r_C of $End(A)$ by the formula

$$p_C = \sum_{C' \leq C} r_C, \tag{1}$$

where $C' \leq C$ means that C is *finer* than C', e.g. $(4,3) \leq (2,2,1,2)$. Following a variant of the definition by Klyachko [11] (see also [16] p.196), we define $\kappa_n \in End(A)$ by

$$\kappa_n = \frac{1}{n} \sum_{|C|=n} \omega_n^{maj(C)} r_C,$$

where $|C| = i_1 + ... + i_l$ is the *weight* of C and $maj(C) = (l-1)i_1 + (l-2)i_2 + ... + i_{l-1} = i_1 + (i_1 + i_2) + ... + (i_1 + ... + i_{l-1})$ is the *major index* of C.

Theorem 12 *The image of* κ_n *is contained in* $Prim(A)$.

Proof. We follow an elegant method of [10], which allows to consider together all elements κ_n for each n.

Let q be a variable. We work within $Endgr(A)[[q]]$, where $Endgr(A) = \oplus_n End(A_n)$ gets the convolution product. Let $\sigma(q) = \sum p_n q^n$, the generating function of all graded projections, where q is a free variable. The following infinite product,

$$\kappa(q) = \prod_{n \geq 0} \sigma(q^n),$$

in decreasing order, is well-defined in $Endgr(A)[[q]]$.

Observe that each element of $Endgr(A)[[q]]$ has a unique expression as a sum $\sum_n f_n$, where $f_n \in End(A_n)[[q]]$.

We may determine these elements f_n for the element $\kappa(q)$, using exactly the same calculations as in [10] p.277-278. One obtains

$$\kappa(q) = \sum_{n \geq 0} \frac{K_n(q)}{(q)_n},$$

with $(q)_n = (1-q)...(1-q^n)$ and $K_n(q) = \sum_{|C|=n} q^{maj(C)} r_C$.

We extend the definitions of Section 2 and say that an element s of $Endgr(A)[[q]]$ admits the pseudo-coproduct $G \in (Endgr(A) \otimes Endgr(A))[[q]]$ if $G \circ \delta = \delta \circ s$, where δ extends naturally to $A[[q]]$ and an element of $Endgr(A)[[q]]$ (resp. $(Endgr(A) \otimes Endgr(A))[[q]]$) defines naturally a linear mapping $A \rightarrow A[[q]]$ (resp. $A \otimes A \rightarrow (A \otimes A)[[q]]$). Furthermore, we say that s is *pseudo-group-like* if $s \otimes s$ is a pseudo-coproduct for s (the last tensor product is taken over $\mathbf{F}[q]$ and $Endgr(A)[[q]] \otimes_{\mathbf{F}[q]} Endgr(A)[[q]]$ is identified with $(Endgr(A) \otimes Endgr(A))[[q]]$). Then it follows from Th.2 that a product of pseudo-group-like elements is pseudo-group-like. Moreover, when written in the form $s = \sum_n f_n$, s is pseudo-group-like if and only if each f_n admits $\sum_{i+j=n} f_i \otimes f_j$ as pseudo-coproduct (so that the sequence (f_n) could be called a sequence of pseudo-divided powers...).

Since the $\sigma(q^n)$s are clearly pseudo-group-like elements, all this implies that for each n, $K_n(q)/(q)_n$ admits $\sum_{i+j=n} K_i(q)/(q)_i \otimes K_j(q)/(q)_j$ as pseudo-coproduct. Thus $K_n(q)$ has $\sum_{i+j=n} \frac{(q)_n}{(q)_i (q)_j} K_i(q) \otimes K_j(q)$ as pseudo-coproduct. For $q = \omega_n$, and $i, j \neq 0$, the polynomials $\frac{(q)_n}{(q)_i (q)_j}$ in q all vanish, which implies that $K_n(\omega_n) = n\kappa_n$ is pseudo-primitive and the theorem follows from Th.2. ■

Corollary 13 *κ_n is idempotent.*

Proof. By the previous theorem, it is enough to show that if a is primitive, then $\kappa_n(a) = a$; we may even assume that a is homogeneous of degree n.

We follow here the same way as [8] p.336. Since $p_C(a) = (p_{i_1} * ... * p_{i_k})(a) = 0$ as soon as C has length $k = l(C) > 1$, we obtain from Eq.(1) that $r_C(a) = (-1)^{l(C)-1}a$, for each composition C of weight n. Thus we obtain

$$n\kappa_n(a) = \sum_{|C|=n} \omega_n^{maj(C)}(-1)^{l(C)-1}a.$$

By classical bijection between compositions of n and subsets of $\{1, ..., n-1\}$, sending $C = (i_1, ..., i_l)$ onto $S = \{i_1, i_1 + i_2, ..., i_1 + ... i_{l-1}\}$, with the property that $maj(C) = maj(S)$ (= sum of the elements in S) and $l(C) - 1 = |S|$, we obtain

$$n\kappa_n(a) = (\sum_{S \subset \{1,...,n-1\}} \omega_n^{maj(S)}(-1)^{|S|})a$$

$$= (\sum_{1 \leq i_1 < ... < i_r \leq n-1} \omega_n^{i_1 + ... + i_r}(-1)^r)a = (\prod_{1 \leq i \leq n-1} (1 - \omega_n^i))a$$

$$= (\prod_{1 \leq i \leq n-1} (x - \omega_n^i)|_{x=1})a = ((1 + x + ... + x^{n-1}|_{x=1})a = na,$$

since ω_n is a primitive n-th root of unity. ∎

The original definition by Klyachko of κ_n gives its action on any word; equivalently, on a product of homogeneous Lie polynomials of degree 1. We extend this formula, by giving the action of κ_n on a product of arbitrary homogeneous primitive elements in a general graded connected cocommutative bialgebra. For this, we evaluate the element $\kappa(q)(a_1 ... a_p)$, with the previous notations, where $a_1, ..., a_p$ are homogeneous primitive elements of respective degree $d_1, ..., d_p$, with $d_1 + ... + d_p = n$. It follows from the definition of the convolution that it is a linear combination of permutations of the product $a_1 ... a_p$.

So, let w be some permutation of $a_1 ... a_p$ (by a usual abuse, we consider w simultaneously as a formal word and as an element of A). Let $w = u_1 ... u_l$ be the factorisation of w in maximal increasing words, for the natural order $a_1 < ... < a_p$. Let C be the composition $(deg(u_1), ..., deg(u_l))$.

Lemma 14 *The coefficient of w in $\kappa(q)(a_1 ... a_p)$ is* $\frac{q^{maj(C)}}{\prod_{w=uv, u \neq 1}(1 - q^{deg(u)})}$.

Corollary 15 *The coefficient of w in $\kappa_n(a_1 ... a_p)$ is*

$$\frac{\omega_n^{maj(C)}}{\prod_{w=uv, u, v \neq 1}(1 - \omega_n^{deg(u)})} = \frac{1}{n} \prod (1 - \omega_n^i)\omega_n^{maj(C)},$$

where the second product is over all i such that w has no nontrivial proper left factor of degree i.

As an example, let $n=4$ and let a_1, b_1, c_2 be primitive elements of degree equal to their subscript. Then by the corollary (with $i=\omega_4$)

$$4\kappa_4(a_1b_1c_2) = i^0(1-i^3)a_1b_1c_2 + i^3(1-i^2)a_1c_2b_1 + i^1(1-i^3)b_1a_1c_2$$

$$+i^3(1-i^2)b_1c_2a_1 + i^2(1-i^1)c_2a_1b_1 + i^5(1-i)c_2b_1a_1$$

$$= (1+i)a_1b_1c_2 - 2ia_1c_2b_1 + (i-1)b_1a_1c_2 - 2ib_1c_2a_1 - (1-i)c_2a_1b_1 + (i+1)c_2b_1a_1$$

$$= (1+i)[a_1,[b_1,c_2]] + (1-i)[[a_1,c_2],b_1].$$

Proof of the corollary. We have $(q)_n\kappa(q)(a_1...a_p) = K_n(q)(a_1...a_p)$ and $n\kappa_n = K_n(\omega_n)$. Since $(q)_n/\prod_{w=uv,u\neq 1}(1-q^{deg(u)}) = \prod(1-q^i)$, with the i as above, and since $n=\prod_{1\leq j\leq n-1}(1-\omega_n^j)$, the corollary follows. ∎

Proof of the lemma. One has

$$\kappa(q) = (... * \sigma(q^3) * \sigma(q^2) * \sigma(q) * \sigma(1))$$

$$= \prod_{m\geq 0}(\sum_{i\geq 0} q^{im}p_i)$$

$$= \sum_{i_1,...,i_r\geq 1, m_1>...>m_r\geq 0} q^{i_1m_1+...+i_rm_r} p_{i_1} * ... * p_{i_r}.$$

Recall that $p_{i_1} * ... * p_{i_r}$ is equal to $\pi^{[r]}\circ(p_{i_1}\otimes ... \otimes p_{i_r})\circ\delta^{[r]}$. Applied to $a_1...a_p$, this term gives the sum of all $v_1...v_r$, for all possible increasing non trivial complementary subwords (that is, subsequences, if $a_1...a_p$ is viewed as a sequence) $v_1,...,v_r$ of $a_1...a_p$, of respective degree $i_1,...,i_r$. Thus, the coefficient of w in $\kappa(q)(a_1...a_p)$ is equal to the sum

$$\sum_{w=v_1...v_r}\sum_{m_1>...>m_r\geq 0} q^{m_1deg(v_1)+...+m_rdeg(v_r)},$$

where the first sum is subject to the condition that the v_j are nontrivial increasing words. Putting $d_j = deg(v_j)$, the second sum is equal classically to

$$\frac{q^{(r-1)d_1+...+d_{r-1}}}{(1-q^{d_1})...(1-q^{d_1+...+d_r})}.$$

Note that the v_j must necessarily be factors of the u_j, so that composition $(d_1,...,d_r)$ is finer than $C=(deg(u_1),...,deg(u_l))$; thus, the searched coefficient is equal to

$$\sum_{E\geq D\geq C}\frac{q^{maj(D)}}{(1-q^{d_1})...(1-q^{d_1+...+d_r})}$$

where E is the composition determined by the degrees of the letters of w. We must show that this is equal to $\frac{q^{maj(C)}}{\prod_{w=uv,u\neq 1}(1-q^{deg(u)})}$.

Equivalently, multiplying by $\prod_{w=uv,u\neq 1}(1-q^{deg(u)})$ and replacing compositions by subsets of $\{1,...,n-1\}$ (with S corresponding to C and U to E) that

$$\sum_{S\subset T\subset U}(q^{maj(T)}\prod_{i\in U-T}(1-q^i))=q^{maj(S)}.$$

By inclusion-exclusion, this is equivalent to

$$\sum_{S\subset T\subset U}(-1)^{|T|-|S|}q^{maj(T)}=\prod_{i\in S}q^i\prod_{j\in U-S}(1-q^j),$$

which is easily shown to be true. ∎

Theorem 16 *The kernel of the restriction of κ_n to A_n is spanned by the elements of the form $ab-\omega_n^{deg(b)}ba$, $a,b\in A$.*

Proof.

1. Let $a_1,...,a_p$ be homogeneous primitive elements whose degrees add up to n. Using Corollary 14, we evaluate $\kappa_n(a_1...a_p)$ and then $\kappa_n(a_pa_1...a_{p-1})=\kappa_n(b_1...b_p)$, with $b_1=a_p$, $b_2=a_1$,...,$b_p=a_{p-1}$.

Let w be as before Lemma 13; in the first expression of Corollary 14, the numerator is $Maj_s(\sigma)$, if we put $w=a_{\sigma(1)}...a_{\sigma(p)}$, $\sigma\in S_p$, $s=(x_1,...,x_p)=(\omega_n^{deg(a_1)},...,\omega_n^{deg(a_p)})$, with the notations of Section 4.

If $a_1,...,a_p$ are replaced by $b_1,...,b_p$, then $w=b_{\gamma^{-1}\sigma(1)}...b_{\gamma^{-1}\sigma(p)}$, with $\gamma=(p,p-1,...,1)$. Thus this numerator, for the same w, is replaced by $Maj_{s\gamma}(\gamma^{-1}\sigma)$, since $s\gamma=(x_p,x_1,...,x_{p-1})$. The latter is equal by Lemma 10 to $x_p^{-1}Maj_s(\sigma)$. Observe that the denominator is unchanged.

Thus the coefficient of w in $\kappa_n(a_pa_1...a_{p-1})$ is equal to that of w in $\kappa_n(a_1...a_p)$ multiplied by $\omega_n^{-deg(a_p)}$. Thus $a_1...a_p-\omega_n^{deg(a_p)}a_pa_1...a_{p-1}$ is in the kernel of κ_n. This implies that the elements described in the theorem are in this kernel, for each primitive element b; but since primitive elements generate A, these elements are in the kernel, without restriction on b.

2. We now show that $x-\kappa_n(x)$ is a linear combination of elements as in the statement, for any x in A_n. This will imply the reverse inclusion of the statement and imply the theorem. It is enough to show this for $x=a_1...a_p$, where the a_is are homogeneous primitive elements. For this, it is enough to show that $x-\kappa_n(x)$ is a linear combination of elements of the form $a_{\sigma(1)}...a_{\sigma(p)}-x_{\sigma(p)}a_{\sigma\gamma(1)}...a_{\sigma\gamma(p)}$, $\sigma\in S_p$, with the same notations as above.

By Corollary 14, the coefficient of $a_{\sigma(1)}...a_{\sigma(p)}$ in $\kappa_n(a_1...a_p)$ is $Maj_s(\sigma)/H_s(\sigma)$, where $H_s(\sigma) = \prod_{1\leq i\leq p-1}(1 - x_{\sigma(1)}...x_{\sigma(i)})$.

We deduce from linear algebra that an element $u = \sum_{\sigma\in S_p} u_\sigma \sigma$ of the symmetric group algebra is in the subspace E spanned by the elements $\sigma - x_{\sigma(p)}\sigma\gamma$ if and only if for any σ the sum

$$\sum_{0\leq i\leq p-1} (x_{\sigma(p-i+1)}x_{\sigma(p-i+2)}...x_{\sigma(p)})^{-1}u_{\sigma\gamma^i}$$

vanishes. Even, it suffices to verify this in two cases: (i) σ is the identity of S_p; (ii) σ is not a power of γ.

Let $u_\sigma = 1 - Maj_s(\sigma)/H_s(\sigma)$ if σ is the identity, and $u_\sigma = -Maj_s(\sigma)/H_s(\sigma)$ otherwise. Lemma 10 shows that

$$Maj_s(\sigma\gamma^i) = (x_{\sigma(p-i+1)}x_{\sigma(p-i+2)}...x_{\sigma(p)})^{\bar{d}(\sigma)}Maj_s(\sigma).$$

Thus, in case (i):

$$\sum_{0\leq i\leq p-1} (x_{\sigma(p-i+1)}...x_{\sigma(p)})^{-1}u_{\sigma\gamma^i} = \sum_{0\leq i\leq p-1} (x_{p-i+1}...x_p)^{-1}u_{\sigma\gamma^i}$$

$$= 1 - \sum_{0\leq i\leq p-1} (x_{p-i+1}...x_p)^{-1}Maj_s(\gamma^i)/H_s(\gamma^i)$$

$$= 1 - \sum_{0\leq i\leq p-1} (x_{p-i+1}...x_p)^{-1}(x_{p-i+1}...x_p)^{\bar{d}(id)}Maj_s(id)/H_s(\gamma^i)$$

$$= 1 - \sum_{0\leq i\leq p-1} 1/H_s(\gamma^i) = 0$$

by Corollary 9 with $k = 0$, since $\bar{d}(id) = 1$. Similarly, in case (ii):

$$\sum_{0\leq i\leq p-1} (x_{\sigma(p-i+1)}...x_{\sigma(p)})^{-1}u_{\sigma\gamma^i}$$

$$= -Maj_s(\sigma)\sum_{0\leq i\leq p-1} (x_{\sigma(p-i+1)}...x_{\sigma(p)})^{\bar{d}(\sigma)-1}/H_s(\sigma\gamma^i).$$

This vanishes by Corollary 9: indeed, σ is not a power of γ, so that $2 \leq \bar{d}(\sigma) \leq p - 1$.

All this implies that u lies in E, and it follows that $x - \kappa_n(x)$ is of the indicated form.

■

6 Applications

In a free monoid, two words u, v are called *conjugate* if for some words x, y one has $u = xy, v = yx$. Conjugation is an equivalence relation, whose classes are called *circular words*. For example, the conjugation class of $aabab$ is the circular word $\{aabab, ababa, babaa, abaab, baaba\}$. A circular word is *prime* if none of its representants is a proper power; for example, the previous circular word is prime, and the circular word $\{abab, baba\}$ is not prime. Note that it is customary, in Combinatorics on Words, to say "primitive word" instead of "prime word"; this could be misleading, since "primitive" applies here to a property of elements of a bialgebra.

It is a well-known fact that the homogeneous bases of free Lie algebras (in particular the Hall bases) are in bijection with prime circular words; this fact was apparently first observed by Meier-Wunderli [14]. This property is also a consequence of the fact that in the classical case, the kernel of the Klyachko idempotent is spanned by the elements

$$uv - \omega_n^{deg(v)} vu, \tag{2}$$

u, v, homogeneous, $deg(uv) = n$; the latter fact was noted in an equivalent form by Garsia, [8] Th.4.3, who observed that the collection of Lie polynomials $\kappa_n(l)$, l Lyndon word of length n, is a basis of the free Lie algebra. In other words, the free Lie algebra is as vector space canonically isomorphic, via the Klyachko operator, with the quotient of the tensor algebra by the subspace spanned by the elements of the form (2).

Theorem 15 extends this result to an arbitrary graded bialgebra A.

An interesting particular case is when A is a free partially commutative algebra, or equivalently, since A is naturally a bialgebra, when $Prim(A)$ is a free partially commutative Lie algebra, see [5]. Then it has been shown by Lalonde that bases of $Prim(A)$ are in bijection with conjugation classes of prime elements of the corresponding free partially commutative monoid M, see [12]. Recall that M is generated by a set X, with relations of the form $xy = yx$; an element of M is *prime* if it cannot be properly written as a product of two commuting elements in M (this extends the definition of a prime word when M is a free monoid). A *conjugation class* is an equivalence class of M for the equivalence relation $\sim$ *generated* by the relations $uv \sim vu$, $u, v \in M$ (unlike the case of the free monoid, these relations do not form a transitive relation, in general). A conjugation class is called *prime* if its elements are all prime; equivalently, if it contains a prime element, as is easily verified (or deduced from the proof below).

So one expects that if we choose a set L of representatives of the prime conjugation classes of M (for example the set of *Lyndon elements*), see [12], then one has the following result.

Corollary 17 *The set $\kappa_{deg(l)}(l)$, $l \in L$, is a basis of the free partially commutative Lie algebra.*

*P*roof. We know by [12] that this set has the desired number of elements in each graded component. So it is enough to show that they span $Prim(A)$. But M spans A. Note that by Theorem 15, $\kappa_n(uv) = \omega_n^{deg(v)} \kappa_n(vu)$. This implies that if m, m' are conjugate, then $\kappa_n(m)$ and $\kappa_n(m')$ differ multiplicatively by a nonzero constant. Moreover, it shows that if m is not prime, then $\kappa_n(m) = 0$. Hence the set $\kappa_{deg(l)}(l)$ spans the same set as $\kappa_{deg(m)}(m)$, $m \in M$, that is, it spans $\kappa_n(A) = Prim(A)$. ■

The previous result implies that the set $\kappa_{deg(l)}(l)$, $l \in L$, is linearly independant. Hence, if $\kappa_n(m) = 0$, m cannot be prime.

We may deduce from this a curious property of conjugation in M: suppose that one has a closed chain $m = m_0, m_1, ..., m_k = m$ of elements, such that at each stage $m_i = u_i v_i$, $m_{i+1} = v_i u_i$ for some nontrivial elements u_i, v_i of M. Then, with $n = deg(m)$, $\kappa_n(m_i) = \kappa_n(u_i v_i) = \omega_n^{deg(v_i)} \kappa_n(v_i u_i) = \omega_n^{deg(v_i)} \kappa_n(m_{i+1})$, which implies that $\kappa_n(m) = \kappa_n(m_0) = \omega_n^d \kappa_n(m_k) = \omega_n^d \kappa_n(m)$, with $d = \sum deg(v_i)$. So, if m is prime, $\kappa_n(m)$ is nonzero and n must divide d.

The previous property is also a consequence of [4] and [6]: indeed, we have $v_i m_i = m_{i+1} v_i$, so that $v_{k-1} ... v_0 m_0 = m_k v_{k-1} ... v_0$. Hence m commutes with $v_{k-1} ... v_0$. Moreover, it follows from the relations $m_i = u_i v_i$ that the variables appearing in $v_{k-1} ... v_0$ lie in the set Y of variables appearing in m. Let N be the submonoid of M generated by Y. Then, since m is prime, the centralizer in N of m is, as submonoid, generated by m itself (see [4], [6]); this implies that n divides d.

7 Appendix

We show here the existence of a graded bialgebra A whose descent algebra has no coproduct satifying the compatibility property $(*)$ of Section 1.

We use results and calculations, known for the case where A is the tensor algebra over an infinite vector space (see [9], [16] chapter 9, [15]), but which extend without difficulty in the general case. For any partition λ, denote by A^λ the subspace of A spanned by the elements $(a_1, ..., a_p) :=$

$(1/p!) \sum_{\sigma \in S_p} a_{\sigma(1)} \ldots a_{\sigma(p)}$, where each a_i is a homogeneous primitive element of degree λ_i, and $\lambda = (\lambda_1, \ldots, \lambda_p)$. Then A is the direct sum of all the subspaces A^λ (a consequence of the theorem of Poincaré-Birkhoff-Witt). The projector onto $A^{(n)}$, parallely to the other subspaces, is the n-th eulerian idempotent e_n, ; it is an element of the descent algebra Σ of the bialgebra A.

Now let $A = \mathbf{F}\langle x, y \rangle$, the bialgebra of noncommutative polynomials, with the variable x of degree 1 and y of degree 2.

We verify that one has the equality $f = g$, where $f = (e_3, [e_1, [e_1, e_2]])$ and $g = ([e_1, e_3], [e_1, e_2])$ (caution: Lie brackets and products are taken in the convolution algebra). Let $z = [x, y]$. Note that, since A^1, A^2, A^3 are all of dimension 1, spanned respectively by x, y, z, $A^{(3,2,1,1)}$ is of dimension 1, spanned by (x, x, y, z).

By Lemma 9.25 in [16], one has $(e_3 * e_1 * e_1 * e_2)((x, x, y, z)) = 2zxxy$ and similarly for the other convolution products of e_3, e_2, e_1, e_1, e_2. Thus $f((x, x, y, z)) = 2(z, [x, [x, y]])$. Similarly $(e_1 * e_3 * e_1 * e_2)((x, x, y, z)) = 2xzxy$, and $g((x, x, y, z)) = 2([x, z], [x, y])$. The latter is equal to $2(z, [x, [x, y]])$, and we conclude that f, g coincide on $A^{(3,2,1,1)}$. By the same result, they annihilate both each element of the form $(a_1, \ldots, a_p)$, with the notations above, when λ is not equal to $(3, 2, 1, 1)$. Thus $f = g$.

Suppose now that the descent algebra Σ of A has a coproduct Δ satisfying $(*)$. Then the e_n are primitive for Δ. We apply Δ to the equality $2f = 2g$ and take its restriction to $A_4 \otimes A_3$; we obtain $[e_1, [e_1, e_2]] \otimes e_3 = [e_1, e_3] \otimes [e_1, e_2]$. Apply this to $(x, x, y) \otimes z$: by the same Lemma, we obtain $2[x, [x, y]] \otimes z = 0$, a contradiction.

References

[1] H.F.Baker, Alternants and continuous groups, Proc. London Math. Soc. 3, 1905, 24-47.

[2] D. Blessenohl, H.Laue, On the descending Loewy series of Solomon's descent algebra, J. Algebra, 180, 1996, 698-724.

[3] P.M.Cohn, Integral modules, Lie rings and free groups, Ph.D. Thesis, Univ. of Cambridge, 1951.

[4] R.Cori, Y. Métivier, Recognizable subsets of some partially abelian monoids, Theor. Comput. Sci. 35, 1985, 179-189.

[5] G.Duchamp, D.Krob, The free partially commutative Lie algebra: bases and ranks. Adv. Math. 95, 1992, 92-126.

[6] C.Duboc, Some properties of commutation in free partially commutative monoids, Inform. Process. Letters 20, 1985, 1-4.

[7] E.B.Dynkin, Calculation of the coefficients in the Campbell-Hausdorff formula, Dokl. Akad. Nauk SSSR 57, 1947, 323-326.

[8] A.Garsia, Combinatorics of the free Lie algebra and the symmetric group, in: Analysis, et cetera, 309-382, Academic Press, Boston, MA, 1990.

[9] A.Garsia, C.Reutenauer, A decomposition of Solomon's descent algebra, Adv. Math. 77, 1989, 189-262.

[10] I.M.Gelfand, D.Krob, A.Lascoux, B.Leclerc, V.Retakh, J.-Y.Thibon, Noncommutative symmetric functions, Adv. Math. 112, 1995, 218-348.

[11] A.A.Klyachko, Lie elements in the tensor algebra, Sib. Mat. ZH. (translation) 15, 1974, 1296-1304.

[12] P.Lalonde, Lyndon heaps: an analogue of Lyndon words in free partially commutative monoids, Discrete Math. 145, 1995, 171-189.

[13] C.Malvenuto, C.Reutenauer, Duality between quasi-symmetric functions and the Solomon descent algebra, J. Algebra 177 ,1995, 967-982

[14] H.Meier-Wunderli, Note on a basis of P. Hall for the higher commutators in free groups. Comment. Math. Helv. 26, 1952, 1-5.

[15] F.Patras, L'algèbre des descentes d'une bigèbre graduée, J. Algebra 170, 1994, 547-566

[16] C.Reutenauer, Free Lie Algebras, Oxford University Press, 1993.

[17] W.Specht, Die linearen Beziehungen zwischen höheren Kommutatoren, Mat. Z. 51, 1948, 367-376.

[18] W.von Waldenfels, Zur Charakterisierung Liescher Elemente in freien Algebren, Arch. Mat. 17, 1966, 44-48.

[19] F.Wever, Über Invarianten in Lieschen Ringen, Mat. Annalen 120, 1949, 563-580.