Noncommutative Symmetric Functions associated with a code, Lazard elimination and Witt vectors

Jean-Gabriel Luque and Jean-Yves Thibon

Abstract

The construction of Witt vectors is related to Lazard's factorisations of free monoids by means of a noncommutative analogue.

1 Introduction

Among Ernst Witt's many contributions to mathematics, one finds two apparently unrelated ideas, both published in 1937 in two consecutive issues of Crelle's journal. The first one, the ring of Witt vectors [15] (a generalisation of p-adic numbers), solves a problem in commutative algebra, whilst the second one, the introduction of the free Lie algebra [16], definitely pertains to noncommutative mathematics.
The aim of this note is to point out a close connection between both constructions, through the notion of noncommutative symmetric functions. What comes out is that the natural noncommutative analogues of the symmetric functions classically associated to the construction of universal Witt vectors can be related to another classical topic in the combinatorics of free Lie algebras: Lazard's factorisations of free monoids. This relation manifests itself when the elementary noncommutative symmetric functions are specialized by means of a code.
Our notations will be those of [9] and [5]. If S is a set of word we denote by $\underline{S} = \sum_{w\in S} w$ its characteristic series.

2 Noncommutative Witt symmetric functions

Let us first recall the construction of the universal ring $W(R)$ of Witt vectors associated to a commutative ring R. This is not Witt's original construction, but a simpler one that he found much later, and that he communicated to S. Lang, who published it as a series of exercises in his famous textbook of Algebra [7].
The ring $W(R)$ can be characterized by the following properties [3] (see also [6, 4]):

(W1) As a set, $W(R) = \{\mathbf{a} = (a_n)_{n\geq 1}\,,\, a_n \in R\}$, and for any ring homomorphism $f : R \to R'$, the map $W(f) :\ \mathbf{a} \mapsto (f(a_n))_{n\geq 1}$ is a ring homomorphism.

(W2) The maps $w_n :\ \mathbf{a} \mapsto \sum_{d|n} d a_d^{n/d}$ are ring homomorphisms $W(R) \to R$.

Operations on Witt vectors are better understood in terms of symmetric functions. Let $X = \{x_n\,,\, n \geq 1\}$ be an infinite set of commuting indeterminates (called here an *alphabet*), and following [11], define symmetric functions $q_n(X)$ by

$$\prod_{n\geq 1} \frac{1}{1-t^n q_n(X)} = \sigma_t(X) := \sum_{n\geq 1} t^n h_n(X) \tag{1}$$

where the complete homogeneous functions $h_n(X)$ are defined by $\sigma_t(X) = \prod_{n\geq 1}(1-tx_n)^{-1}$ (*cf.* [9]). The q_n's are connected to the power-sums $p_n(X) = \sum_i x_i^n$ by

$$p_n = \sum_{d|n} d q_d^{n/d} \tag{2}$$

and condition (W2) can be regarded as expressing the familiar properties of power sums

$$p_n(X+Y) = p_n(X) + p_n(Y)$$

$$p_n(XY) = p_n(X)p_n(Y)$$

where we use the λ-ring notation (an alphabet is identified with the formal sum of its elements).
Reutenauer [11] studied the symmetric functions $q_n(X)$ and made the conjecture that for $n \geq 2$, $(-q_n)$ is Schur positive. This conjecture was proved in [13], in a generalised noncommutative form. Denoting as in [5] the noncommutative complete homogeneous symmetric functions of an alphabet A by $S_n(A)$, one introduces noncommutative Witt symmetric functions $Q_n(A)$ by the identity

$$\prod_{n\geq 1}^{\rightarrow} \frac{1}{1-t^n Q_n(A)} = \sigma_t(A) := \sum_{n\geq 1} t^n S_n(A) \tag{3}$$

Then, it is proved in [13] that for $n \geq 2$, $(-Q_n)$ is a positive, multiplicity free, sum of noncommutative ribbon Schur functions R_I.

3 Noncommutative symmetric functions associated to a code

Let A be an alphabet and $C \subset A^+$ a *code*, *i.e.* a minimal generating set of a free submonoid C^* in A^*. Suppose we have a decomposition of C as a disjoint union

$$C = \coprod_{n\geq 1} C_n \tag{4}$$

of possibly empty subsets C_n. In what follows, we shall assume that $C_n = C \cap A^n$, but this restriction in not necessary. In any case, we will consider that the elements of C_n have degree n.
We will denote by $l(w)$ the length of a word w..
We can now define a specialization $\mathbf{Sym}[C]$ of the algebra of noncommutative symmetric functions by setting

$$\Lambda_n[C] = (-1)^{n-1}\underline{C}_n\,. \tag{5}$$

With this choice of signs, the complete symmetric functions are then given by

$$S_n[C] = \sum_{w \in (C^*)_n} w \,, \tag{6}$$

the sum of all elements of degree n in C^*. We call C-*Witt symmetric function* the value $Q_i[C]$ of Q_i under this specialization. Let us give the first $Q_i[C]$ for three examples

Example 1 The Fibonacci prefix code $C = \{b, ab\}$.

$$\begin{aligned}
Q_1[C] &= b \\
Q_2[C] &= ab \\
Q_3[C] &= ab^2 \\
Q_4[C] &= ab^3 \\
Q_5[C] &= ab^2ab + ab^4 \\
Q_6[C] &= ab^3ab + ab^5 \\
Q_7[C] &= ab^6 + ab^2(ab)^2 + ab^4ab + ab^3ab^2
\end{aligned}$$

Example 2 The infinite prefix code $C = ba^*$.

$$\begin{aligned}
Q_1[C] &= b \\
Q_2[C] &= ba \\
Q_3[C] &= ba^2 + bab \\
Q_4[C] &= bab^2 + ba^3 + ba^2b \\
Q_5[C] &= bab^2a + bab^3 + ba^2b^2 + ba^2b^2 + ba^4 + ba^2ba \\
Q_6[C] &= ba^4b + ba^3b^2 + ba^2b^2a + bab^3a + bab^4 + ba^3ba + ba^5 + ba^2b^3
\end{aligned}$$

Example 3 The Dyck code D (for the Dyck language $\underline{D^*} = 1 + a\underline{D^*}b\underline{D^*}$.)

$$\begin{aligned}
&Q_1[D] = Q_3[D] = Q_5[D] = Q_7[D] = 0 \\
&Q_2[D] = ab \\
&Q_4[D] = aabb \\
&Q_6[D] = aaabbb + aababb + aabbab \\
&Q_8[D] = aaaabbbb + aaababbb + aabaabbb + aaabbbab + aaabbabb \\
&+aabbabab + aabababb + aababbab
\end{aligned}$$

On these examples, we remark that each Q_i is multiplicity free and is the characteristic series of a code. In the following section, we prove that it is always the case and give a characterization of these codes in terms of Lazard's factorisations.

4 Witt symmetric functions and factorization

4.1 Lazard elimination process

We recall that a factorisation of a monoid $\mathbb{M}$ is an ordered family of monoids $\mathbb{F} = (\mathbb{M}_i)_{i \in I}$ such that each element $m \in \mathbb{M}$ admits an unique decomposition

$$m = m_{i_1} \cdots m_{i_k} \tag{7}$$

where $i_1 > \cdots > i_k$ and $m_{i_1} \in \mathbb{M}_{i_1}, \ldots, m_{i_k} \in \mathbb{M}_{i_k}$. In the case of free monoids $\mathbb{M} = A^*$, this property can be stated in terms of generating series

$$\sum_{w \in A^*} w = \overleftarrow{\prod_i} \sum_{w \in \mathbb{M}_i} w \tag{8}$$

In that case, and more generally in the case of monoids which can be endowed with a graduation, a submonoid $\mathbb{M}' \subset \mathbb{M}$ can be characterized by the set of its generators $\mathbb{M}' \setminus \mathbb{M}'^2$. In the sequel, a factorisation will be denoted by the sequence of the generating sets of its components and for a factorisation $\mathbb{F} = (C_i)_{i \in I}$ of A^* (8) reads

$$\frac{1}{1 - \underline{A}} = \overleftarrow{\prod_i} \frac{1}{1 - \underline{C_i}}. \tag{9}$$

Factorisations of free monoids have been extensively studied and the reader can refer to [2, 14] for a survey. A simple but relevant example is a *Lazard's bisection*: considering a subalphabet $B \subset A$, one has

$$A^* = B^*((A \setminus B)B^*)^*. \tag{10}$$

The pair $(B, (A \setminus B)B^*)$ is a factorisation of A^* (cf. [14, 2], and [12] for their connection with free Lie algebras). Now, from (10) we can obtain a trisection (*i.e.* a factorisation in three submonoids) by iterating the process on the left or the right factor, and so on. Factorisations which can be generated applying only Lazard bisections on the right factors will be called *Lazard right compositions*. This is a simple particular case of a *locally finite right regular factorisation* [14]. Let A be an alphabet (possibly infinite) and $\omega : A \to \mathbb{N}\setminus 0$ a weight function. This function can be extended uniquely as a morphism $\omega : A^* \to (\mathbb{N}, +)$. We can associate a factorisation $\mathbb{F}(A, \omega)$ to this weight as follows. Let $(Z_i)_{i \in \mathbb{N}}$ and $(C_i)_{i \in \mathbb{N}}$ be two sets of codes defined by the recurrence relations

1. $Z_1 = A$
2. for each integer $i > 0, C_i = Z_i \cap \{w \in A^* | \omega(w) = i\}$.
3. for each integer $i > 0, Z_{i+1} = (Z_i \setminus C_i)C_i^*$

The sequence $\mathbb{F}(A, \omega) = (C_i)_{i \in I}$ obtained by omitting the empty elements in $(C_i)_{i \in \mathbb{N}}$ is a Lazard right composition.
Since each code $C \in A^*$ admits the length of words as weight function, we define the *length right factorisation* $\mathbb{F}(C)$ of a code C by

$$\mathbb{F}(C) = \mathbb{F}(C, l). \tag{11}$$

We can remark that a code is homogeneous if and only if $\mathbb{F}(C) = (C)$.

4.2 Computation of the C-Witt symmetric functions

The equality between formal series (3) can be rewritten as

$$\frac{1}{1 - \underline{C}} = \frac{1}{1 - Q_1} \frac{1}{1 - Q_2} \frac{1}{1 - Q_3} \cdots, \tag{12}$$

and in this section, we prove that this factorisation of series is the weight right factorisation of C^*.
In a more general setting, T. Scharf and one of the authors [13], gave a recursive algorithm for computing the $Q_n's$. We consider the algebra **Sym** of the non commutative symmetric functions which can be defined as the free associative algebra $\mathbb{Q}\langle S_1, S_2, \cdots, \rangle$ generated by an infinite sequence of non commutative variables S_n graded by the weight function $w(S_n) = n$. If $I = (i_1, \cdots, i_n)$, one defines

$$\tilde{S}^I = (-1)^n S_{i_1} \cdots S_{i_n} \tag{13}$$

The Q_i can be computed following the rules given in [13]:

1. $F_1 = -\sum_i \tilde{S}_i$,
2. $F_{n+1} = F_n + Q_n(1 - F_n)$,
3. Q_n is the term of weight n in F_n multiplied by -1.

Setting $Z_n = 1 - (1 - F_n)^{-1}$, we obtain

$$F_{n+1} = 1 - (1 - Z_{n+1})^{-1} \tag{14}$$

and

$$\begin{aligned} F_n + Q_n(1 - F_n) &= 1 - (1 - Z_n)^{-1} + Q_n(1 - Z_n)^{-1} \\ &= 1 - (1 - Q_n)(1 - Z_n)^{-1}. \end{aligned} \tag{15}$$

This implies

$$\begin{aligned} Z_{n+1} &= 1 - (1 - Z_n)(1 - Q_n)^{-1} \\ &= (Z_n - Q_n)(1 - Q_n)^{-1}. \end{aligned} \tag{16}$$

Following [13], each Q_i is multiplicity free on the $\tilde{S}_I$.

Let $C \subset A^*$ be a code. We denote $Z_i[C]$ and $F_i[C]$ the values of Z_i and F_i under the specialization $S_n = S_n[C]$. The definition of non commutative complete functions gives

$$\sigma_1[C] = \sum S_n[C] = \frac{1}{1 - \underline{C}}. \tag{17}$$

Hence, one has

$$Z_1[C] = 1 - (\sigma_1[C])^{-1} = \underline{C}, \tag{18}$$
$$Q_1[C] = S_1[C] = \underline{C_1} \text{ and} \tag{19}$$
$$Z_1[C] - Q_1[C] = \underline{C} - \underline{C_1}. \tag{20}$$

It follows that $Z_1[C]$ and $Q_1[C]$ are the characteristic series of the codes $Z_1 = C$ and $Q_1 = C_1$. By induction, for each $n > 0$ the series $Z_{n+1}[C]$ and $Q_{n+1}[C]$ are the characteristic series of $Z_{n+1} = (Z_n \setminus Q_n)Q_n^*$ and $Q_n^* = Z_n \cap A^{\leq n}$. Hence, the following statement holds.

Proposition 1 *Let C be a code. Each C-Witt symmetric function $Q_i[C]$ is the characteristic series of a code Q_i and the sequence $(Q_i)_{i\in I}$ obtained by deleting the empty set from $(Q_1, Q_2, \ldots, Q_n, \ldots)$ is the length right factorisation of C^*.*

Example 4 The sequence $(a, Q_1[ba^*], Q_2[ba^*], \ldots)$ is a factorisation of A^*. The same method is applicable to compute homogeneous factorisations of non-homogeneous alphabets. For example, considering the alphabet $A = \mathbb{N} \setminus 0$ with the weight $\omega = id$, one finds

$$
\begin{aligned}
&Q_1[A] = 1\\
&Q_2[A] = 2\\
&Q_3[A] = 21 + 3\\
&Q_4[A] = 211 + 31 + 4\\
&Q_5[A] = 2111 + 212 + 311 + 32 + 41 + 5\\
&Q_6[A] = 21111 + 51 + 2112 + 6 + 3111 + 312 + 42 + 411
\end{aligned}
$$

It is easy to see that this can be obtained from example 2 by the morphism $ba^n \to n + 1$.

One has the following decomposition

Corollary 2 *Let $w \in Q$, then either $w \in C$ either there exist $w_1, w_2 \in Q$ verifying $w = w_1 w_2$ with $\omega(w_2) < \omega(w_1) < \omega(w)$. Furthermore, if $w_1 \notin C$ then $w_1 = w_1' w_1''$ with $w_1', w_1'' \in Q$ and $\omega(w_1'') \leq \omega(w_2)$*

This follows from the standard bracketing process of regular factorisations, which is described in [14].

4.3 Non-commutative elementary symmetric functions and Lazard elimination

The link between Lazard elimination and non-commutative Witt symmetric functions can be better understood in terms of elementary symmetric functions. The generating function of non-commutative elementary symmetric function is

$$\lambda_t = \sum_{k \leq 0} \Lambda_k t^k. \tag{21}$$

These fonctions are related to non-commutative complete functions by

$$\sigma_t = \frac{1}{\lambda_{-t}} = \frac{1}{1 - \Lambda_1 t + \Lambda_2 t^2 - \cdots + (-1)^n \Lambda_n t^n + \cdots}. \tag{22}$$

If we set $\tilde{\Lambda}_n = (-1)^{n+1} \Lambda_n$, the series $\sigma_1(X)$ can be considered as the characteristic series of the free monoid $\mathbf{\Lambda}^* = \{\tilde{\Lambda}_1, \tilde{\Lambda}_2, \ldots, \tilde{\Lambda}_n\}^*$. We endow this monoid with the weight function defined by $\omega(\tilde{\Lambda}_n) = n$. Then,

Theorem 3 *One has*

$$\mathbb{F}(\mathbf{\Lambda}, \omega) = (Q_1[\mathbf{\Lambda}], Q_2[\mathbf{\Lambda}], \ldots) = (Q_1, Q_2, \ldots) \tag{23}$$

This provides a simple algorithm to compute the decomposition of the non-commutative symmetric Witt functions in the basis of elementary symmetric functions. Let us gives the computation of the first Q_i's,

$$\begin{aligned}
&Q_1 = \Lambda_1\\
&Q_2 = -\Lambda_2\\
&Q_3 = -\Lambda_2\Lambda_1 + \Lambda_3\\
&Q_4 = -\Lambda_2\Lambda_1\Lambda_1 + \Lambda_3\Lambda_1 - \Lambda_4\\
&Q_5 = -\Lambda_2\Lambda_1^3 + \Lambda_2\Lambda_1\Lambda_2 + \Lambda_3\Lambda_1\Lambda_1 - \Lambda_3\Lambda_2 - \Lambda_4\Lambda_1 + \Lambda_5\\
&Q_6 = -\Lambda_2\Lambda_1^4 + \Lambda_5\Lambda_1 + \Lambda_2\Lambda_1\Lambda_1\Lambda_2 - \Lambda_6 + \Lambda_3\Lambda_1^3 - \Lambda_3\Lambda_1\Lambda_2 + \Lambda_4\Lambda_2 - \Lambda_4\Lambda_1\Lambda_1\\
&Q_7 = -\Lambda_3\Lambda_1^2\Lambda_2 + \Lambda_3\Lambda_4 - \Lambda_3\Lambda_1\Lambda_2\Lambda_1 + \Lambda_3\Lambda_1\Lambda_3 + \Lambda_3\Lambda_2^2 - \Lambda_4\Lambda_1^3 + \Lambda_4\Lambda_1\Lambda_2 - \Lambda_4\Lambda_3\\
&+\Lambda_4\Lambda_2\Lambda_1 + \Lambda_5\Lambda_1^2 - \Lambda_5\Lambda_2 - \Lambda_6\Lambda_1 + \Lambda_7 - \Lambda_2\Lambda_1^5 + \Lambda_2\Lambda_1^3\Lambda_2 + \Lambda_2\Lambda_1^2\Lambda_2\Lambda_1\\
&-\Lambda_2\Lambda_1^2\Lambda_3 - \Lambda_2\Lambda_1\Lambda_2^2
\end{aligned}$$

(compare to examples 2 and 4).
The decomposition of the elementary functions in the basis of the $Q_I = Q_{i_1}\cdots Q_{i_n}$ is obtained by inspection of the series

$$\frac{1}{\sigma_t} = \lambda_{-t} = 1 - \sum_n \tilde{\Lambda}_n t^n = \overleftarrow{\prod_i}(1 - Q_i t^i). \tag{24}$$

One gets

$$\tilde{\Lambda}_n = \sum_k (-1)^k \sum_{\substack{i_1 > \cdots > i_k\\ i_1 + \cdots + i_k = n}} Q_{i_1}\cdots Q_{i_k} \tag{25}$$

References

[1] F. Bassino, M.-P. Béal, D. Perrin, *Length distributions and regular sequences, in Codes, Systems ans Graphical Models* , IMA Volumes in Mathematics and its Applications, Springer-Verlag, p. 415-437, 2001

[2] J. Berstel et D. Perrin, *Theory of Codes*, Academic Press, New-York, 1985.

[3] P. Cartier, *Groupes formels associés aux anneaux de Witt généralisés*, C.R. Acad. Sci. Paris **265** (1967), 49-52.

[4] J. Dieudonné, *Schur functions and group representations*, Astérisque **87-88** (1983), 7-19.

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

[6] M. Hazewinkel, *Formal Groups and Applications*, Academic Press, New York, 1978.

[7] S. Lang, *Algebra.* Addison-Wesley Publishing Co., Inc., Reading, Mass. 1965 xvii+508 pp

[8] M. Lazard, *Groupes, anneaux de Lie et problème de Burnside*, Istituto Matematico dell'UNiversità di Roma, 1960.

[9] I.G. Macdonald, *Symmetric functions and Hall polynomials*, Oxford Math. Monographs, Oxford, 1979; 2nd ed. 1995.

[10] N. Metropolis, G.-C. Rota, *Witt vectors and the algebra of necklaces*, Adv. Math. **50** (1983), 95-125.

[11] C. Reutenauer, *On symmetric functions related to Witt vectors and the free Lie algebra*, Adv. Math. **110** (1995), 234-246.

[12] C. Reutenauer, *Free Lie Algebras* (Oxford University Press, New-York, 1993).

[13] T. Scharf and J.-Y. Thibon, *On Witt vectors and symmetric functions*, Algebra Colloq. **3** (1996), no. 3, 231–238.

[14] G. Viennot, *Algèbres de Lie libres et monoïdes libres*, Thèse de Doctorat d'Etat, Université Paris VII, 1974.

[15] E. Witt, *Zyklische Körper und Algebren der Charakteristik p vom Grade p^m* , J. Reine Angew. Math. **176** (1937), 126-140.

[16] E. Witt, *Treue Darstellung Liescher Ringe*, J. Reine Angew. Math. **177** (1937), 152-160.