Orthogonal projection onto the free Lie algebra

Gérard Duchamp

LITP/LIR, Université de Rouen, Place E. Blondel, B.P. 118, 76134 Mont Saint Aignan Cedex, France

Abstract

Duchamp, G., Orthogonal projection onto the free Lie algebra, Theoretical Computer Science 79 (1991) 227-239.

As an answer to a question of Garsia, we give a universal formula in a "normal form" for the orthogonal projection of free associative algebra onto free Lie algebra.

1. Introduction

Let X be an alphabet and k a field of characteristic zero. Denote by X^*, $L(X)$, $k\langle X\rangle$, respectively, the free monoid, the free Lie algebra and the free associative algebra over X (see Section 2, [1] and [5]).

There is a well-known projection $k\langle X\rangle \to L(X)$, called Dinkin's projection, defined by substitution of letters and linear extension from the formulas

$$x_1x_2, \ldots, x_n \to 1/n[.[[x_1, x_2], x_3], \ldots, x_n].$$

Several others have been studied since [4, 8].

Garsia asked for the "form" of the projection $k\langle X\rangle \to L(X)$ which is orthogonal for the only bilinear form $(\ |\ )_X$ making X^* an orthonormal basis of $k\langle X\rangle$. Of course, this question makes sense if and only if we know that $L(X) \oplus L(X)^{\perp} = k\langle X\rangle$ which is the case for $\mathrm{char}(k) = 0$ (see Section 4).

In this paper we answer this question and the results can be informally stated as follows:

(a) For $\mathrm{char}(k) = 0$, the orthogonal projection exists (which is not the case when $\mathrm{char}(k) = 2$, for instance).

(b) The orthogonal projection can be expressed, for each word length, by a linear combination of actions on the positions of the letters (the Pólya action), independent from the alphabet "universal formulas".

0304-3975/91/$03.50 © 1991—Elsevier Science Publishers B.V. (North-Holland)

(c) For each word length, these "universal formulas" can be computed from the projection of a single word that can be any word without repetition (the U_n of formulas (2.2)).

The first part of this paper (Sections 2, 3 and 4) is devoted to the reduction of the problem and one will see that the use of an infinite alphabet and a theorem of Ree allows us to "represent" the orthogonal projection by linear combinations of actions on the positions of the letters and these actions are independent of the alphabet X.

In a second part (Sections 5 and 6), devoted to explicit computations, we apply Gram's method to two bases: the first one makes use of an idempotent that Klyachko introduced in a "little known pioneering paper" [4], and another one (D_{l}), which we made to suit the problem. We give additional properties of the corresponding Gram matrices that are both invariant under a natural action of $\mathfrak{S}_{n-1}$.

Finally, Section 7 gives the "other term of Ree's decomposition". In fact, there is an algorithm, linear in time, to compute the explicit total decomposition of any polynomial under the form

$$\text{polynomial} = \text{Lie polynomial} + \text{linear combination of proper shuffles.}$$

2. Reduction of the problem

2.1. Graduation of $k\langle X\rangle$ by multidegrees

Let X be an alphabet, whose elements will be called letters, and X^* be the free monoid over X [5]. For each word $w \in X^*$ and $x \in X$ we will denote by $|w|_x$ the number of occurrences of the letter x in w and we will call it the *partial degree* of w in x.

Example 2.1. With $X = \{a, b, c\}$, $w = a^3ba^4c^2$ we have $|w|_a = 7$, $|w|_b = 1$ and $|w|_c = 2$.

The *multidegree* of a word $w \in X^*$ is the family (with finite support) $(|w|_x)_{x\in X} = \mu(w)$. It is an element of $\mathbb{N}^{(X)} = \{f: X \to \mathbb{N} \,|\, |\mathrm{supp}(f)| < +\infty\}$ (mappings with finite support from X to $\mathbb{N}$).

Remark 2.2. It is often convenient to handle the multidegree as a sequence, for instance, with the data of Example 2.1, $(|w|_a, |w|_b, |w|_c) = (7, 1, 2)$.

The *total degree*, or *length* is just the sum $\sum_{x\in X} |w|_x = |w|$. For example, we have $|a^3ba^4c^2| = 10$.

If k is a nontrivial ($1 \neq 0$) commutative ring, $k\langle X\rangle$ will denote the monoid algebra of X^* [1, 5] over k; its elements can be written uniquely as

$$P = \sum_{w\in X^*} \lambda_w w = \sum_{w\in X^*} (P|w)w.$$

$k\langle X\rangle$ is also called the free associative algebra or the algebra of noncommutative polynomials.

For every degree $\nu \in \mathbb{N}^{(X)}$ and $n \in \mathbb{N}$, one defines

$$X^{\nu} = \{w \in X^* \mid \mu(w) = \nu\}, \qquad X^{n} = \{w \in X \,||w| = n\}$$

and, denoting by $\langle R\rangle$ the submodule of $k\langle X\rangle$ spanned by R,

$$k_{\nu}(X) = \langle X^{\nu}\rangle, \qquad k_{n}(X) = \langle X^{n}\rangle.$$

Of course, one clearly has $k\langle X\rangle = \bigoplus_{\nu} k_{\nu}\langle X\rangle = \bigoplus_{n} k_{n}\langle X\rangle$.

Definition 2.3. (a) (homogeneous element) Every element of $k_{\nu}\langle X\rangle$ (resp. $k_{n}\langle X\rangle$) is said to be ***homogeneous*** of multidegree (resp. degree) ν (resp. n).

(b) (graded submodule) One says that a submodule M of $k\langle X\rangle$ is *graded* iff it is generated by its homogeneous elements, or iff $M = \bigoplus (M \cap k_{\nu}\langle X\rangle)$ (resp. $M = \bigoplus (M \cap k_{n}\langle X\rangle)$).

(c) (graded endomorphism) One says that an endomorphism $f \in \mathrm{End}(k\langle X\rangle)$ is *graded* iff, for each $\nu \in \mathbb{N}^{(X)}$, $f(k_{\nu}\langle X\rangle) \subseteq k_{\nu}\langle X\rangle$. Their set is a subalgebra of $\mathrm{End}(k\langle X\rangle)$ denoted $\mathrm{End}_{\mathrm{gr}}(k\langle X\rangle)$.

2.2. Action of the symmetric group on k⟨X⟩

Let $\sigma \in \mathfrak{S}_n$, $w = x_1x_2 \ldots x_n \in X^n$ and define (cf. [3]) the so-called Pólya action of σ on w as follows:

$$\text{if } n \neq 0, \quad (x_1x_2 \ldots x_n)\,.\,\sigma = (x_{\sigma(1)}x_{\sigma(2)} \ldots x_{\sigma(n)}),$$
$$\text{if } n = 0, \quad 1.\mathrm{Id} = 1.$$

It is straightforward that, for $\sigma, \tau \in \mathfrak{S}_n$, $w.(\sigma\tau) = (w.\sigma).\tau$ and $w.1 = w$; this action then extends by linearity to $k[\mathfrak{S}_n]$. For $P \in k\langle X\rangle$ and every family $\Gamma = (\gamma_n)_{n\in\mathbb{N}} \in \prod_{n\in\mathbb{N}} k[\mathfrak{S}_n]$, with $\gamma_n = \sum_{\sigma\in\mathfrak{S}_n} \gamma_n(\sigma)\sigma$ it is easy to check that

$$\sum_{n\in\mathbb{N}} \sum_{|w|=n} \sum_{\sigma\in\mathfrak{S}_n} (P|w)\gamma_n(\sigma)w.\sigma \tag{2.1}$$

is a polynomial (see Proposition 2.4(i)). This element will be denoted by $P.\Gamma$. The preceding formula leads to considering the direct product of the group algebras $\mathscr{A} = \prod_{n\in\mathbb{N}} k[\mathfrak{S}_n]$. Therefore (2.1) defines a natural extension to $\mathscr{A}$ of the Pólya action. Let us denote by $\rho_x(\Gamma)$ the element f of $\mathrm{End}(k\langle X\rangle)$ defined by $\rho(\Gamma)[P] = P.\Gamma$. With these constructions we have the following proposition.

Proposition 2.4. (i) *For every $\Gamma \in \mathscr{A}$, $\rho_X(\Gamma) \in \mathrm{End}_{\mathrm{gr}}(k\langle X\rangle)$.*

(ii) *ρ_X defines a k-algebra morphism: $\mathscr{A} \to \mathrm{End}_{\mathrm{gr}}(k\langle X\rangle)$ which is into iff X is infinite.*

Proof. (i) The sum (2.1) is a well defined element of $k\langle X\rangle$ because the family of polynomials

$$\left(\sum_{|w|=n} \sum_{\sigma\in\mathfrak{S}_n} (P|w)\gamma_n(\sigma)w.\sigma\right)_{n\in\mathbb{N}}$$

has finite support in $\mathbb{N}$. Now if $P \in k_{\nu}\langle X\rangle$, we have $P = \sum_{w\in S} (P|w|)w$ with $S \subseteq X^{\nu}$. Hence, for $\Gamma \in \mathscr{A}$, $P.\Gamma \in \langle\bigcup_{\sigma\in\mathfrak{S}_n} S.\sigma\rangle \subseteq \langle X^{\nu}\rangle = k_{\nu}\langle X\rangle$, which proves assertion (i).

(ii) The formula

$$P.\gamma = \sum_{|w|=n} \sum_{\sigma\in\mathfrak{S}_n} (P|w)\gamma_n(\sigma)w.\sigma \quad \text{for } P\in k_n\langle X\rangle,\ \gamma\in k[\mathfrak{S}_n]$$

defines the unique bilinear extension of $w.\sigma$ to $k_n\langle X\rangle \times k[\mathfrak{S}_n]$; we have $P.(\gamma\tau) = (P.\gamma).\tau$ by the universal property of any group algebra. It is then clear that ρ is a morphism of algebras.

Let us now examine the relation with the finiteness of X.

If X is finite, set $|X| = p$. We have $\dim(k_n\langle X\rangle) = p^n$ and $\dim(\mathrm{End}(k_n\langle X\rangle) = p^{2n}$ but $\dim(k[\mathfrak{S}_n]) = |\mathfrak{S}_n| = n!$. So, for N (large enough) such that $p^{2N} < N!$, there is $\gamma_0 \in k[\mathfrak{S}_n] - \{0\}$ such that $P.\gamma_0 = 0$ for all $P\in k_n\langle X\rangle$. Set $\Gamma_0 = (\alpha_n)_{n\in\mathbb{N}}$ with $\alpha_n = 0$ for all $n\neq N$ and $\alpha_N = \gamma_0$; then $\rho_X(\Gamma_0) = 0$ with $\Gamma_0 \neq 0$. Thus ρ_X is not into if X is finite.

If X is infinite, let $(x_j)_{j\geq 1}$ be an injective sequence in X. Define inductively U_n $(= x_1x_2\ldots x_n \in X^*)$ precisely by

$$U_0 = 1 \text{ (the empty word of } X^*\text{)}, \qquad U_{n+1} = (U_n)x_{n+1} \tag{2.2}$$

Set also $\alpha_n = \mu(U_n)$, we can now state a lemma as follows.

Lemma 2.5. *For each $n\in\mathbb{N}$ the family $(U_n\,.\,\sigma)_{\sigma\in\mathfrak{S}_n}$ is a basis of $k_{\alpha_n}\langle X\rangle$.*

Proof. It is enough to remark that the mapping $\sigma\to U_n.\sigma$ is one-to-one from $\mathfrak{S}_n$ to $(X^*)_{\alpha_n}$ which is an easy consequence of the definitions. □

Proof of Proposition 2.4 (*conclusion*). Suppose $\Gamma = (\gamma_n)_{n\in\mathbb{N}} \in \mathscr{A}$ and $\rho(\Gamma) = 0$. Then, for each $n\in\mathbb{N}$ we have $\rho(\Gamma).U_n = U_n.\Gamma = 0$; then by Lemma 2.5 we get $\gamma_n = 0$. □

3. Orthogonal projection on $L\langle X\rangle$

In this part we shall prove that the orthogonal projection $k\langle X\rangle \to L\langle X\rangle$ is well defined if k is of characteristic zero. In fact, if $k\neq\mathbb{Q}$ several difficulties can appear and we will point out some of them with three examples for $X = \{a, b\}$.

First example (*isotropy*): $X = \{a, b\}$; $k = \mathbb{C}$; $H = \mathbb{C}.(ab + \mathrm{i}ba)$. One has $\{0\}\neq H \subseteq H^\perp$ and no orthogonal projection can be defined.

Second example (*characteristic*): $X = \{a, b\}$; $k = \mathbb{Z}/2\mathbb{Z}$; $H = L_1(X) = k.[a, b]$. One has $H^\perp = H = k.(ab + ba) = k.(a \sqcup\!\sqcup b)$. There is no orthogonal projection and moreover Ree's theorem is no longer true.

Third example (*density*): Let $H = \{P\in k\langle X\rangle \mid \sum_{w\in X^*}(P|w) = 0\}$; then $H^\perp = \{0\}$.

So, from now on, we make the general assumption that $\mathrm{char}(k) = 0$. The following theorem establishes the existence of the orthogonal projection on $L\langle X\rangle$.

Theorem 3.1. *Let S be a subset of $k\langle X\rangle$ such that*

(i) $S=\bigcup_{n\in\mathbb{N}}(S\cap k_n\langle X\rangle)$ (*S is homogeneous*),

(ii) *for every* $(P, w)\in S\times X^*$, $(P|w)\in\mathbb{Q}$ (*S is rational*).

Then, if H is the subspace spanned by S, one has $H\oplus H^{\perp}=k\langle X\rangle$.

Proof. For every subset A of $k\langle X\rangle$, we will denote by $\langle A\rangle_{\mathbb{Q}}$ the set of linear combinations of elements of A with coefficients in $\mathbb{Q}$ (indeed the $\mathbb{Q}$-subspace of $k\langle X\rangle$ generated by A). Then by (ii) one has $\langle S\rangle_{\mathbb{Q}}\subseteq\langle X^*\rangle_{\mathbb{Q}}$. Now, the form $(\ |\ )_X$ is positive definite in $\langle X^*\rangle_{\mathbb{Q}}$. Set $S\cap k_n\langle X\rangle=S_n$; we then have $\langle S_n\rangle_{\mathbb{Q}}\subseteq\langle X^n\rangle_{\mathbb{Q}}$. As these spaces have finite dimensions and $(\ |\ )_X$ is positive definite, there is an orthogonal projection $\pi_n\in\mathrm{End}_{\mathbb{Q}}(\langle X^n\rangle_{\mathbb{Q}})$ on $\langle S_n\rangle_{\mathbb{Q}}$. From the definition of $(\ |\ )_X$, we have $\langle X^*\rangle_{\mathbb{Q}}=\bigoplus_{n\geq 0}^{\perp}\langle X^n\rangle_{\mathbb{Q}}$. Then we obtain an orthogonal projection in $\mathrm{End}_{\mathbb{Q}}(\langle X^*\rangle_{\mathbb{Q}})$ by the formula

$$\pi_{\mathbb{Q}}(P)=\sum_{n\geq 0}\sum_{|w|=n}(P|w)\pi_n(w)\quad\text{for } P\in\langle X^*\rangle_{\mathbb{Q}}.$$

$\pi_{\mathbb{Q}}(P)$ is obviously the projection on the $\mathbb{Q}$-subspace spanned by S, namely $\langle S\rangle_{\mathbb{Q}}$. Now $\pi_{\mathbb{Q}}$ has the following properties:

(i) $\pi_{\mathbb{Q}}^2=\pi_{\mathbb{Q}}$;

(ii) $\mathrm{Im}(\pi_{\mathbb{Q}})=\langle S\rangle_{\mathbb{Q}}$;

(iii) for every $v, w\in X^*$ $(v-\pi_{\mathbb{Q}}(v)|\pi_{\mathbb{Q}}(w))_X=0$.

Let us denote by π_k the unique extension of $\pi_{\mathbb{Q}}$ to $k\langle X\rangle$ (uniquely defined by $\pi_k(w)=\pi_{\mathbb{Q}}(w)$ for every word $w\in X^*$). Now, for all words v, $w\in X^*$ we have

(*) $\pi_k^2(w)=\pi_k(\pi_{\mathbb{Q}}(w))={}^1\ \pi_{\mathbb{Q}}^2(w)=\pi_{\mathbb{Q}}(w)=\pi_k(w)$,

(**) $\pi_k(w)\in\langle S\rangle_{\mathbb{Q}}$, and

(***) $(v-\pi_k(v)|\pi_k(w))_X=0$.

From (*) one gets that $\pi_k^2=\pi_k$; (**) implies that we have $\mathrm{Im}(\pi_k)\subseteq H$. Remark also that $\langle\pi_k(X^n)\rangle_{\mathbb{Q}}=\langle\pi_{\mathbb{Q}}(X^n)\rangle_{\mathbb{Q}}=\mathrm{Im}(\pi_n)=\langle S_n\rangle_{\mathbb{Q}}$ so that $S\subseteq\mathrm{Im}(\pi_k)$. Finally $\mathrm{Im}(\pi_k)=H$. (***) implies, by bilinear extension, that $(P-\pi_k(P)|\pi_k(Q))_X=0$ for every $P, Q\in k\langle X\rangle$. In conclusion π_k is, in $\mathrm{End}_k(k\langle X\rangle)$, the orthogonal projection on H. □

Corollary 3.2. *We have* $L(X)\oplus^{\perp}L(X)^{\perp}=k\langle X\rangle$.

Proof. It is an easy consequence of the theorem when one remarks that $L_n(X)=L(X)\cap k_n\langle X\rangle$ is generated by the Lie monomials:

$$\delta(x_1x_2\ldots x_n)=[.[[x_1,x_2],x_3],\ldots,x_n]=\sum_{\sigma\in\mathfrak{S}_n}c(\sigma)x_{\sigma(1)}x_{\sigma(2)}\ldots x_{\sigma(n)}\qquad(3.1)$$

where $c(\sigma)\in\{-1,1,0\}$. □

Notation. In the sequel, the orthogonal projection on $L(X)$ will be denoted by π_X.

[1] This equality holds because $\pi_{\mathbb{Q}}(w)\in\langle X^*\rangle_{\mathbb{Q}}$.

4. Alphabetic substitutions

By the universal properties of the free associative algebras [5, p. 16], any mapping $f: X \to Y$ extends uniquely as a k-algebra morphism $s_f: k\langle X\rangle \to k\langle Y\rangle$. Such a morphism is called an *alphabetic substitution.* The set of these substitutions will be denoted $\mathcal{S}(X;\, Y)$ (or $\mathcal{S}(X)$ if $X = Y$). The orthogonal projection on $L(X)$ has a remarkable behavior in connection with alphabetic substitutions which is intimately related to the existence of "universal generating systems" such as (3.1). We point this out as follows (Theorem 4.1(iv) and (v)).

Theorem 4.1. *Let X, Y be alphabets. Then we have the following statements.*

(i) *The elements of $\mathcal{S}(X;\, Y)$ are $\mathcal{A}$-linear i.e., for every $P \in k\langle X\rangle$, $\Gamma \in \mathcal{A}$, $s \in \mathcal{S}(X;\, Y)$, we have $s(P.\Gamma) = s(P).\Gamma$.*

(ii) *If X is infinite, for every $f \in \mathrm{End}_{\mathrm{gr}}(k\langle X\rangle)$, f commutes with $\mathcal{S}(X)$ $\Leftrightarrow$ $f \in \rho_X(\mathcal{A})$.*

(iii) *For every $s \in \mathcal{S}(X;\, Y)$, $s(L(X)) \subseteq L(Y)$ (the restriction to these subspaces will be denoted by s_L).*

(iv) *One has the following commuting diagram:*

$$\begin{tikzcd} k\langle X\rangle \arrow[r, "\pi_X"] \arrow[d, "s"'] & L(X) \arrow[d, "s_L"] \\ k\langle Y\rangle \arrow[r, "\pi_Y"] & L(Y) \end{tikzcd} \tag{4.1}$$

(v) *There is a unique $\Gamma_L \in \mathcal{A}$ such that, for every alphabet A, $\pi_A = \rho_A(\Gamma_L)$.*

Proof. (i) follows from a straightforward computation with formula (2.1).

(ii) As in Theorem 3.1, we make use of an injection $\mathbb{N}^* \to X$ and keep the notations U_n and α_n. If $f \in \mathrm{End}_{\mathrm{gr}}(k\langle X\rangle)$ one has, for every n, $f(U_n) \in k_{\alpha_n}\langle X\rangle$; hence, as $(U_n.\sigma)_{\sigma\in\mathfrak{S}_n}$ is a basis of $k_{\alpha_n}\langle X\rangle$, we can write

$$f(U_n) = \sum_{\sigma\in\mathfrak{S}_n} \lambda(\sigma, n)\, U_n.\sigma. \tag{4.2}$$

Define $\Gamma_f = (\gamma_n)_{n\in\mathbb{N}}$ with $\gamma_n = \sum_{\sigma\in\mathfrak{S}_n} \lambda(\sigma, n)\sigma$ and $\varphi_f = \rho_x(\Gamma_f)$. Expression (4.2) implies that, for every $n \in \mathbb{N}$, $f(U_n) = U_n.\Gamma_f$. If, moreover, f commutes with $\mathcal{S}(X)$ we have $f = \varphi_f$ from the following lemma.

Lemma 4.2. *If $f, g \in \mathrm{End}(k\langle X\rangle)$ commute with $\mathcal{S}(X)$ and coincide on the words U_n, then $f = g$.*

Proof. We only have to show that

$$f(w) = g(w) \quad \text{for every word } w, \tag{4.3}$$

which is straightforward for $w = 1$ as $1 = U_0$. Now let $w = y_1 y_2 \ldots y_n$. The substitution defined by $s(x_i) = y_i$ for $1 \leq i \leq n$ and $s(x) = x$ otherwise is such that $s.U_n = w$. Then $f(w) = f(s.U_n) = s.f(U_n) = s.(g(U_n)) = g(s.U_n) = g(w)$. □

Proof of Theorem 4.1 (*conclusion*). We now know that $f \in \rho_X(\mathscr{A})$. The converse in (ii) is an easy consequence of (i) with $X = Y$.

(iii) Consider $s \in \mathscr{S}(X;\, Y)$. Then s, being a k-algebra morphism $k\langle X\rangle \to k\langle Y\rangle$ is also a morphism for the Lie structures. Hence $s(X) \subseteq Y$ implies $s(L(X)) \subseteq L(Y)$.

(iv) We define a bilinear product ш (shuffle [6, 7]) on $k\langle X\rangle$ by induction on words with the following formulas:

$$\begin{cases} w \sqcup\!\sqcup\, 1_{X^*} = 1_{X^*} \sqcup\!\sqcup\, w = w \\ vx \sqcup\!\sqcup\, wy = (vx \sqcup\!\sqcup\, w)y + (v \sqcup\!\sqcup\, wy)x. \end{cases} \tag{4.4}$$

Denote by S_X the subspace generated by the proper shuffles, that is to say, the elements $v \sqcup\!\sqcup\, w$ with $v \neq 1$ and $w \neq 1$. Ree [7] has shown that $L\langle X\rangle^{\perp} = S_X$. Formulas (4.4) prove that if $s \in \mathscr{S}(X;\, Y)$, we have $s(u \sqcup\!\sqcup\, v) = s(u) \sqcup\!\sqcup\, s(v)$, whence $s(S_x) \subseteq S_Y$ (as $v \neq 1 \Rightarrow s(v) \neq 1$). This shows the claim.

(v) The same formulas (4.4) show that $\mu(v \sqcup\!\sqcup\, w) = \mu(v) + \mu(w)$ and hence that S_X is a graded subspace of $k\langle X\rangle$. $L\langle X\rangle$ and $L\langle X\rangle^{\perp} = S_X$ being graded, one has $\Pi_X \in \mathrm{End}_{\mathrm{gr}}(k\langle X\rangle)$. If, moreover, X is infinite, (iv) implies that Π_X commutes with $\mathscr{S}(X)$ and hence $\Pi_X = \rho(\Gamma_X)$ for a $\Gamma_X \in \mathscr{A}$.

Remark first that if Y is another infinite alphabet, $\Gamma_X = \Gamma_Y$ since, if we choose injections $j \to x_j$ and $j \to y_j$, we can define the corresponding words U_n and V_n as in (2.2) and also a substitution $s \in \mathscr{S}(X;\, Y)$ such that $s(U_n) = V_n$ for all n. Hence,

$$V_n.\Gamma_Y = \Pi_Y(V_n) = \Pi_Y(s(U_n)) = s(\Pi_X(U_n)) = s(U_n.\Gamma_X)$$

$$= s(U_n).\Gamma_X = V_n.\Gamma_X \quad \text{for all } n \in \mathbb{N}$$

Lemma 4.2 shows that $\rho_Y(\Gamma_Y) = \rho_Y(\Gamma_X)$ and then $\Gamma_Y = \Gamma_X$ as Y is infinite and then ρ_Y is injective by Proposition 2.4. Thus Γ_L must be the common value of Γ_X for any infinite X. This proves also the uniqueness of Γ_L.

Finally let A be any finite alphabet and X be an infinite auxiliary alphabet. Take any surjection $s \in \mathscr{S}(X;\, Y)$ (such elements exist, being defined from any surjection $X \to A$). If $Q \in k\langle A\rangle$ we can write $Q = s(P)$ for some $P \in k\langle X\rangle$. Then: $\pi_A(Q) = \Pi_A(s(P)) =$ (by (iv)) $s(\Pi_X(P)) = s(P.\Gamma_L) = s(P).\Gamma_L = Q.\Gamma_L$. □

5. A "universal" formula for the orthogonal projection

Theorem 4.1 proves that the orthogonal projections can be expressed by Γ_L i.e. "universal formulas" (independent of the alphabet) computed from any infinite alphabet. Moreover, one only needs to know the family of Lie polynomials $\Pi_X(U_n)$. For any sequence defined as above, the following proposition shows how to compute them.

Proposition 5.1. *Let X be an infinite alphabet and $j \to x_j$ an injection $\mathbb{N}^* \to X$. We keep the definitions of U_n and α_n as previously. Let $\mathscr{P} = (P_i)_{1 \leq i \leq m}$ be any basis of $L_{\alpha_n}\langle X\rangle$,* *then* $\langle P_i|P_j\rangle_{1\leq i,j\leq m}$ *is invertible and the orthogonal projection of* U_n *on* $L(X)$ *is* $\Pi_X(U_n)=\sum_{1\leq i\leq m}\lambda_iP_i$ *where the family* $(\lambda_i)_{1\leq i\leq m}$ *satisfies*

$$\begin{pmatrix} P_1.P_1 & P_1.P_2 & \cdots & P_1.P_m \\ P_2.P_1 & P_2.P_2 & \cdots & P_2.P_m \\ \vdots & \vdots & & \vdots \\ P_m.P_1 & P_m.P_2 & \cdots & P_m.P_m \end{pmatrix}^{-1} \begin{pmatrix} P_1.U_n \\ P_2.U_n \\ \vdots \\ P_m.U_n \end{pmatrix} = \begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \vdots \\ \lambda_m \end{pmatrix} \tag{5.1}$$

Proof. If we set $\Gamma_L=(\pi_n)_{n\in\mathbb{N}}$ we have $\Pi_X(U_n)=U_n.\Gamma_L=U_n.\pi_n=\sum_{\sigma\in\mathfrak{S}_n}\pi_n(\sigma)U_n.\sigma$ and hence $\Pi_X(U_n)\in k_{\alpha_n}\langle X\rangle$. This is precisely the orthogonal projection of U_n on $L_{\alpha_n}(X)$. It is well known that $L_{\alpha_n}(X)$ has a basis with rational coordinates relative to X^* (any Lyndon or Hall basis as in [5] will do) and hence an orthogonal basis with rational coordinates (because the Gram–Schmitt process is done within $\langle X^*\rangle_{\mathbb{Q}}\subseteq k\langle X\rangle$ where the form $(\ |\ )_X$ is positive definite). Let $\mathscr{B}$ be such a rational orthogonal basis and let $\mathscr{M}$ be the change matrix from $\mathscr{B}$ to $\mathscr{P}$; the matrix of inner products (the so-called Gram matrix) $(P_i|P_j)_{1\leq i,j\leq m}$ is then $M={}^t\mathscr{M}\Delta\mathscr{M}$, where Δ is the diagonal matrix of inner products of $\mathscr{B}$. This shows that M is invertible. As $\Pi_X(U_n)\in k_{\alpha_n}\langle X\rangle$, we can write $\Pi_X(U_n)=\sum_{1\leq i\leq m}\lambda_iP_i$ and this polynomial can be characterized as the solution of the linear system

$$\left\langle\left(U_n-\left(\sum_{1\leq i\leq m}\lambda_iP_i\right)\right)\middle|P_j\right\rangle=0 \quad \text{for } 1\leq j\leq m \tag{5.2}$$

whose matrix of coefficients is M, and hence (5.2) has a unique solution expressed by (5.1). □

6. Working up with some particular bases of $k\langle X\rangle$

6.1. Klyachko's basis

In his paper "Lie elements in tensor algebra", Klyachko [4] introduces an idempotent of $k[\mathfrak{S}_n]$ defined by

$$\kappa_n=\frac{1}{n}\sum_{\sigma\in\mathfrak{S}_n}\varepsilon^{\mathrm{maj}(\sigma)}\sigma \tag{6.1}$$

where ε is any primitive nth root of unity (it is assumed that k has one) and $\mathrm{maj}(\sigma)=\sum_{\sigma(i)>\sigma(i+1)}i$ (the "major index").

Let X be a totally ordered alphabet; X^* is then totally ordered with the lexicographic order. Call any word $x_1x_2\ldots x_n$ which is strictly less than all its circular rearrangements a *Lyndon word* [5, 6]; that is,

$$x_1x_2\ldots x_n<x_{i+1}x_{i+2}\ldots x_nx_1x_2\ldots x_i \quad \text{for all } 1\leq i\leq n-1.$$

Denote by $L(n)$ the set of Lyndon words of length n (results about Lyndon words can be found in [5]). Garsia [3] shows that $(w\kappa_n)_{w\in L(n)}$ is a basis of $L_n\langle X\rangle = L\langle X\rangle \cap k_n\langle X\rangle$ (κ_n as in (6.1)).

Here, to get the projection of U_n, we just have to consider the letters $x_1, x_2, \ldots, x_n$ of a supposed infinite alphabet $X = \{x_i\}_{i\in\mathbb{N}^*}$. If we order them by $x_1 < x_2 < \cdots < x_n < \cdots$, the Lyndon words of multidegree α_n are the words $x_1x_{\beta(2)}\ldots x_{\beta(n)}$ with $\beta \in \mathfrak{S}_{\{2,3\ldots n\}}$. The results are given in the following theorem.

Theorem 6.1. *For $\beta \in \mathfrak{S}_{\{2,3\ldots n\}}$, set $K_\beta = (x_1x_{\beta(2)}\ldots x_{\beta(n)})\kappa_n = U_n\beta\kappa_n$. One has*

(i) *(K_β) is a basis of $L_{\alpha_n}\langle X\rangle$,*

(ii) $$\langle K_{\beta 1}|K_{\beta 2}\rangle = \langle K_{Id}|K_{\beta_1^{-1}\beta_2}\rangle = \frac{1}{n^2}\sum_{\sigma\in\mathfrak{S}_n} \varepsilon^{\mathrm{maj}(\sigma)+\mathrm{maj}(\beta_2^{-1}\beta_1\sigma)},$$

(iii) $$\langle K_\beta | U_n\rangle = \frac{1}{n}\,\varepsilon^{\mathrm{maj}(\beta^{-1})}.$$

Proof. (i) is straightforward from the fact that $(w\kappa_n)_{w\in L(n)}$ is a basis of $L_n\langle X\rangle$ and by counting dimensions.

(ii) $$\langle K_{\beta 1}|K_{\beta 2}\rangle = \frac{1}{n^2}\left(\sum_{\sigma\in\mathfrak{S}_n} \varepsilon^{\mathrm{maj}(\sigma)} U_n.\beta_1\sigma \,\middle|\, \sum_{\tau\in\mathfrak{S}_n} \varepsilon^{\mathrm{maj}(\tau)} U_n.\beta_2\tau\right).$$

Then (ii) follows from (∗): $\langle U_n.\beta_1\sigma | U_n.\beta_2\tau\rangle = \delta(\beta_1\sigma, \beta_2\tau)$ (Kronecker delta).

(iii) $\langle K_\beta | U_n\rangle = n^{-1}\sum_{\sigma\in\mathfrak{S}_n} \varepsilon^{\mathrm{maj}(\sigma)}\langle U_n.\beta\sigma | U_n\rangle$ and formula (∗) proves (iii). □

Example 6.2 (*Case $n = 3$*). See Table 1; here $i_1i_2i_3$ stands either for the permutation $k \to i_k$ or for the word $x_{i_1}x_{i_2}x_{i_3}$. The arrows stand for the "descents" i.e. the indices "i" such that $\sigma(i) > \sigma(i+1)$. We denote any element x' of k such that $x'^3 = 1$ also by j.

The Gram matrix is

$$\begin{pmatrix} 0 & 2j^2/3 \\ 2j^2/3 & 0 \end{pmatrix}$$

Table 1

Descents		↓	↓	↓	↓	↓ ↓
σ or w	1 2 3	1 3 2	2 1 3	2 3 1	3 1 2	3 2 1
Maj(σ)	0	2	1	2	1	3
K_{Id}	1/3	$j^2/3$	$j/3$	$j^2/3$	$j/3$	1/3
$K_{(2,3)}$	$j^2/3$	1/3	$j/3$	1/3	$j/3$	$j^2/3$

With (5.1) we get

$$\begin{aligned}\Pi_X(U_3) &= \tfrac{1}{2}K_{\mathrm{Id}} + \tfrac{1}{2}jK_{(2,3)}\\ &= \tfrac{1}{3}x_1x_2x_3 - \tfrac{1}{6}x_1x_3x_2 - \tfrac{1}{6}x_2x_1x_3 - \tfrac{1}{6}x_2x_3x_1 - \tfrac{1}{6}x_3x_1x_2 + \tfrac{1}{3}x_3x_2x_1\end{aligned}$$

6.2. The (D_I) basis

We keep the notations and the lexicographic order as above. Since X^* is in fact totally ordered we will call, for each $P \in k\langle X\rangle - \{0\}$, the least word v such that $(P|v) \neq 0$ the *valuation monomial.* This word will be denoted as $m(P)$. A family $(P_i)_{i\in I}$ in $k\langle X\rangle - \{0\}$ will be called *triangular* iff the mapping $i \to m(P_i)$ is injective. Such a family is obviously free. These notions will be used to prove the following theorem.

Theorem 6.3. (i) (D_{I} basis): *For each word $w = y_1y_2 \ldots y_n$, let*

$$[w] = [\ldots[[y_1, y_2], y_3], \ldots, y_n].$$

Then the family $([U_n\beta])_{\beta\in\mathfrak{S}_{\{2,3,\ldots,n\}}}$ is a basis of $L_{\alpha_n}\langle X\rangle$.

(ii) *If we index the set $([U_n\beta])_{\beta\in\mathfrak{S}_{\{2,3,\ldots,n\}}}$ as a family $D_{\mathrm{I}} = (D_i)_{1\leq i\leq m}$ such that $D_1 = [U_n]$, we have*

$$\Pi_X(U_n) = \Big[\operatorname{Det}(D_i|D_j)_{\substack{1\leq i\leq m\\ 1\leq j\leq m}}\Big]^{-1}\Big(\sum_{1\leq k\leq m}(-1)^k \operatorname{Det}(D_i|D_j)_{\substack{1\leq i\leq m\\ 1\leq j\leq m\\ j\neq k}} D_k\Big). \tag{6.2}$$

Proof. (i) It can be easily checked that $m([U_n\beta]) = U_n\beta$. Since these words are all different, the family D_{I} is triangular and hence free. By Witt's formulas for the multidegree [1] we have dim $L_{\alpha_n}\langle X\rangle = (n-1)!$. It is also the number of elements in D_{I}, whence (i).

(ii) Formula (6.2) comes from (5.1) in view of the fact that $(U_n|D_i) = 1$ if $i = 1$ and 0 otherwise. □

Examples 6.4. (i) $(n = 3)$ X^{α_3} is a basis of $k_{\alpha_3}\langle X\rangle$, we have the decompositions

X^{α_3}	$x_1x_2x_3$	$x_1x_3x_2$	$x_2x_1x_3$	$x_2x_3x_1$	$x_3x_1x_2$	$x_3x_2x_1$
$[x_1x_2x_3]$	+1	0	−1	0	−1	+1
$[x_1x_3x_2]$	0	+1	−1	+1	−1	

The Gram matrix is $\left(\begin{smallmatrix}4&2\\2&4\end{smallmatrix}\right)$ and we get

$$\begin{aligned}\Pi_X(U_3) &= \tfrac{1}{3}[x_1x_2x_3] - \tfrac{1}{6}[x_1x_3x_2]\\ &= \tfrac{1}{3}x_1x_2x_3 - \tfrac{1}{6}x_1x_3x_2 - \tfrac{1}{6}x_2x_1x_3 - \tfrac{1}{6}x_2x_3x_1 - \tfrac{1}{6}x_3x_1x_2 + \tfrac{1}{3}x_3x_2x_1.\end{aligned}$$

(ii) $(n=4)$ The Gram matrix is

$$\begin{pmatrix} 8 & 4 & 4 & 2 & 2 & 0 \\ 4 & 8 & 2 & 4 & 0 & 2 \\ 4 & 2 & 8 & 0 & 4 & 2 \\ 2 & 4 & 0 & 8 & 2 & 4 \\ 2 & 0 & 4 & 2 & 8 & 4 \\ 0 & 2 & 2 & 4 & 4 & 8 \end{pmatrix}$$

and its inverse is

$$\frac{1}{20}\begin{pmatrix} 5 & -2 & -2 & -1 & -1 & 2 \\ -2 & 5 & -1 & 2 & -2 & -1 \\ -2 & -1 & 5 & -2 & 2 & -1 \\ -1 & 2 & -2 & 5 & 1 & -2 \\ -1 & -2 & 2 & -1 & 5 & -2 \\ 2 & -1 & -1 & -2 & -2 & 5 \end{pmatrix};$$

whence

$$\Pi_X(U_4)=\tfrac{1}{4}[x_1x_2x_3x_4]-\tfrac{1}{10}[x_1x_2x_4x_3]-\tfrac{1}{10}[x_1x_3x_2x_4]$$
$$-\tfrac{1}{20}[x_1x_3x_4x_2]-\tfrac{1}{20}[x_1x_4x_2x_3]+\tfrac{1}{10}[x_1x_4x_3x_2].$$

This then yields, by alphabetic substitution, the projections of all the words of length 4. For example, we have

$$\Pi_X(abca)=\tfrac{1}{4}[abca]-\tfrac{1}{10}[abac]-\tfrac{1}{10}[acba]-\tfrac{1}{20}[acab].$$

Note. The Lie monomials in the expression above are linearly dependent because $\dim L_{(2,1,1)}(X)=3$.

We also have $\Pi_X(abba)=0$ (see [2]).

Remark. The group $\mathfrak{S}_{\{2,3,\ldots,n\}}$ can be viewed as a submonoid of $\mathscr{S}(X)$: it then acts on the left on $k\langle X\rangle$. It can be easily checked that the basis (K_β) and D_{I} are invariant under this action.

6.3. Fast computation of the inner products

We will now give properties of the inner products arising in the matrices $(D_i|D_j)$ that will allow easy implementation and fast computation. The first rule to use is the invariance of $(\ |\ )_X$ under the Pólya action, that is,

$$(P.\sigma|Q.\sigma)_X=(P|Q)_X \quad \text{for every } P, Q\in k_n\langle X\rangle \text{ and } \sigma\in\mathfrak{S}_n. \qquad \text{(R0)}$$

Recall that for any word $w=y_1y_2\ldots y_n$ the *reversal* of w is defined by $\tilde{w}=y_ny_{n-1}\ldots y_1$. This involution extends to an anti-automorphism of $k\langle X\rangle$ given by

$\tilde{P}=\sum(P|w)\tilde{w}$. It can be easily shown (cf. [2]) that if $P\in L_n(X)$, we have $\tilde{P}=(-1)^{n+1}P$. The two following rules hold for P, $Q\in L_\alpha\langle X\rangle$ such that α has no repetition (i.e. such that $\alpha(a)\in\{0,1\}$ for every $a\in X$):

$$\text{if } x\neq y,\quad ([P,x]|[Q,y])=-2(Px|vQ)=-2(xP|Qy), \tag{R1}$$

$$\text{if } x=y,\quad ([P,x]|[Q,y])=2(P|Q). \tag{R2}$$

Now we can see that, using rules (R1) and (R2), one needs less than n steps.

If $A\subseteq X^*$, set $\mathrm{Proj}_A(P)=\sum_{w\in A}(P,w)w$. Then we have

$$\mathrm{Proj}_{x_iX^*}[x_1x_2\ldots x_n]=-x_1[x_1x_2\ldots x_{i-1}]x_{i+1}\ldots x_n, \tag{R3}$$

$$\mathrm{Proj}_{X^*x_i}[x_1x_2\ldots x_n]=(-1)^{n-1}x_nx_{n-1}\ldots x_{i+1}[x_1x_2\ldots x_{i-1}]x_i. \tag{R4}$$

An easy consequence of these rules is the following corollary.

Corollary 6.5. *For $n\geqslant 2$ the coefficients in the Gram matrix of (D_I) are* 0 *or* 2^k *with* $k\geqslant 1$.

7. Total decomposition: a basis for $S_{\alpha_n}\langle X\rangle=k_{\alpha_n}\langle X\rangle\cap S_X$ $(n\geqslant 2)$

Theorem 7.1. (D_{II} basis). *Let D be the set of ordered pairs (v,w) such that $v\neq 1$ and $\mu(vw)=\alpha_{n-1}$. For $(v,w)\in D$, set $R_{v,w}=v \sqcup\!\sqcup\, x_nw$. Then $D_{\mathrm{II}}=(R_{v,w})_{(v,w)\in D}$ is a basis of $S_{\alpha_n}\langle X\rangle$.*

Proof. The valuation monomial of $R_{v,w}$ is vx_nw hence $(R_{v,w})_{(v,w)\in D}$ is triangular and free. We have

$$\dim(S_{\alpha_n}\langle X\rangle)=\dim(k_{\alpha_n}\langle X\rangle)-\dim(L_{\alpha_n}\langle X\rangle)=(n-1)!\cdot n=|D|;$$

this proves that $(R_{v,w})_{(v,w)\in D}$ is a basis of $S_{\alpha_n}\langle X\rangle$. □

Example 7.2 ($n=3$)

	$x_1x_2x_3$	$x_1x_3x_2$	$x_2x_1x_3$	$x_2x_3x_1$	$x_3x_1x_2$	$x_3x_2x_1$
$[x_1x_2x_3]$	+1	0	−1	0	−1	+1
$[x_1x_3x_2]$	0	+1	−1	+1	−1	0
$x_1x_2 \sqcup\!\sqcup\, x_3$	+1	+1	0	0	+1	0
$x_1 \sqcup\!\sqcup\, x_3x_2$	0	+1	0	0	+1	+1
$x_2x_1 \sqcup\!\sqcup\, x_3$	0	0	+1	+1	0	+1
$x_2 \sqcup\!\sqcup\, x_3x_1$	0	0	0	+1	+1	+1

Once we have computed $\Pi_X(U_n)$, the total decomposition of U_n can be obtained by cancelling the valuation monomials of the complement $U_n-\Pi_X(U_n)$ as in a division between polynomials.

Example 7.3 ($n=3$)

$$\begin{aligned} U_3 = {} & \tfrac{1}{3}[x_1x_2x_3] - \tfrac{1}{6}[x_1x_3x_2] + \tfrac{2}{3}x_1x_2 ш x_3 \\ & - \tfrac{1}{2}x_1 ш x_3x_2 + \tfrac{1}{6}x_2x_1 ш x_3. \end{aligned}$$

Further, by alphabetic substitution, we can obtain, for example,

$$\begin{aligned} aba &= \tfrac{1}{3}[aba] - \tfrac{1}{6}[aab] + \tfrac{2}{3}ab ш a - \tfrac{1}{2}a ш ab + \tfrac{1}{6}ba ш a \\ &= \tfrac{1}{3}[aba] + \tfrac{1}{6}a ш ab + \tfrac{1}{6}a ш ba, \\ abb &= \tfrac{1}{6}[abb] + \tfrac{2}{3}ab ш b - \tfrac{1}{2}a ш bb + \tfrac{1}{6}ba ш b. \end{aligned}$$

8. Conclusion

Here we only applied the method of Sections 1, 2, 3 and 4 to $L(X)$. This method is however much more powerful, and can be used to establish orthogonal projections on subspaces that are $\mathcal{S}(X)$-spanned by $\mathbb{Q}$-multilinear polynomials with a commuting diagram as (4.1). That is the case, in particular, of the factors $L_n(X)$ of the lower central series of $L(X)$, on which the corresponding projections Π_n tend to zero.

Acknowledgment

I must here thank M.P. Schützenberger for many stimulating remarks and also C. Reutenauer and A. Lascoux for the unpublished paper [3] they imparted to me.

References

[1] N. Bourbaki, *Groupes et Algèbres de Lie*, Chapters 2 and 3 (Diffusion CCLS, 1972).

[2] G. Duchamp et J.Y. Thibon, Le support de l'algèbre de Lie libre, *Discrete Math.* **76** (1989) 123–129.

[3] A. Garsia, Combinatorics of the free Lie algebra and the symmetric group, Unpublished.

[4] A.A. Klyachko, Lie elements in the tensor algebra, *Siberian Math. J.* **15** (1974) 914–920.

[5] M. Lothaire, *Combinatorics on Words* (Addison-Wesley, Reading, MA, 1974).

[6] G. Melancon and C. Reutenauer, Lyndon words, free algebras and shuffles, Rapport de recherche No. 36 UQUAM, and 87-63 LITP, 1987.

[7] R. Ree, Lie elements and algebra associated with shuffles, *Ann. Math.* **68** (1958) 210–220.

[8] C. Reutenauer, Theorem of Poincaré–Birkhoff–Witt and symmetric group representations of degrees equal to Stirling numbers, in: Lecture Notes in Mathematics **1234** (Springer, Berlin, 1986) 267–293.