The shuffle Hopf algebra and the commutative Hopf algebra of labelled rooted trees

A. Murua*

April 11, 2005

Abstract

We establish an epimorphism ν of graded Hopf algebras from the Hopf algebra of labelled rooted trees $\mathcal{H}_R(X)$ to the shuffle Hopf algebra $\mathrm{Sh}(X)$, and we identify the graded Hopf ideal $\mathcal{I} = \ker \nu$, so that $\mathrm{Sh}(X)$ is isomorphic as a graded Hopf algebra to the quotient Hopf algebra $\mathcal{H}_R(X)/\mathcal{I}$. For each Hall set associated to the alphabet D ($X = \mathbb{K}\,D$, where $\mathbb{K}$ is the base ring), we assign a set of labelled rooted trees $\widehat{\mathcal{T}}^*$ and a set of labelled forests $\widehat{\mathcal{F}}^*$ ($\widehat{\mathcal{T}}^* \subset \widehat{\mathcal{F}}^*$) such that $\nu(\widehat{\mathcal{F}}^*)$ freely generates $\mathrm{Sh}(X)$ as a $\mathbb{K}$-module, and when the base ring is a $\mathbb{Q}$-algebra, $\nu(\widehat{\mathcal{T}}^*)$ freely generates $\mathrm{Sh}(X)$ as a $\mathbb{K}$-algebra. Moreover, we describe the coalgebra structure of $\mathrm{Sh}(X)$ in terms of the basis $\nu(\widehat{\mathcal{F}}^*)$. Finally, we show that the dual basis of $\nu(\widehat{\mathcal{F}}^*)$ is the Poincaré-Witt-Birkhoff basis of $T(X)$ corresponding to a Hall basis of the free Lie algebra $\mathcal{L}(D)$. Our results are closely related to available results [17] on Poincaré-Witt-Birkhoff basis of the tensor algebra $T(X)$ associated to Hall sets over D.

1 Introduction

Let $\mathbb{K}$ be a fixed commutative ring. Given a set D (an alphabet), consider $\mathcal{L}(D)$, the free Lie algebra over D (with base ring $\mathbb{K}$). The universal enveloping algebra of $\mathcal{L}(D)$ is isomorphic to the free associative algebra $\mathbb{K}\langle D\rangle$, or equivalently, the tensor algebra $T(X)$ over the free $\mathbb{K}$-module $X := \mathbb{K}D$ over the set D. Furthermore, if $\mathbb{K}$ has 0 characteristic, $\mathcal{L}(D)$ is isomorphic to the Lie algebra of primitive elements of the bialgebra $T(X)$. This means in particular that the coproduct in $T(X)$ can be used to identify the elements of $\mathcal{L}(D)$ in $T(X)$ [17].

An explicit description of the coalgebra structure of $T(X)$ in terms of its standard basis of words on the alphabet D involves the use of shuffles of words [17]. Basis of $T(X)$ other than the set of words on the alphabet D can be constructed by means of the Poincaré-Birkhoff-Witt Theorem from arbitrary basis of $\mathcal{L}(D)$. Such alternative basis have the advantage of allowing a very simple explicit description of the coalgebra structure of

*Konputazio Zientziak eta A. A. saila, EHU/UPV, Donostia/San Sebastián, (ander@si.ehu.es)

$T(X)$ (and in particular, an obvious way of identifying the elements in $\mathcal{L}(D)$), but on the contrary, the explicit description of the algebra structure of $T(X)$ becomes more involved. If a (generalized) Hall basis of $\mathcal{L}(D)$ has been chosen, this can be done using some rewriting rule (see [17] and references therein).

With the canonical grading of $T(X) = \mathbb{K} \oplus \bigoplus_{n\geq 1} X^{\otimes n}$, the tensor algebra $T(X)$ has a structure of graded connected cocommutative Hopf algebra. If D is finite, the graded dual of $T(X)$ has a graded connected (actually, strictly graded) commutative Hopf algebra structure denoted by $\mathrm{Sh}(X)$ (here, we identify the linear dual X^* with X). Working in the shuffle algebra $\mathrm{Sh}(X)$ is particularly useful in applications that require dealing with Lie series [17] and exponentials of Lie series (for instance, non-linear control theory [9], and the theory of geometric numerical integrators for ordinary differential equations [10, 13]). In this sense, a complete description of the Hopf algebra $\mathrm{Sh}(X)$ in terms of the dual basis of a Poincaré-Birkhoff-Witt basis of $T(X)$ corresponding to a given basis of $\mathcal{L}(D)$ seems of interest. The algebra structure of $\mathrm{Sh}(X)$ admits a convenient explicit description in such dual basis (Theorem 5.3 in [17]). The explicit description of the coalgebra structure of $\mathrm{Sh}(X)$ in terms of a dual Poincaré-Birkhoff-Witt basis is however more involved. The aim of the present work is to accomplish this task for an arbitrary generalized Hall basis of $\mathcal{L}(D)$. The main tool will be another graded connected commutative Hopf algebra associated to the set D, namely, the commutative Hopf algebra of rooted trees labelled by D, that we denote as $\mathcal{H}_R(X)$, $X = \mathbb{K}\, D$.

The referred commutative Hopf algebra structure $\mathcal{H}_R$ on the free $\mathbb{K}$-module over the set of (non-labelled) rooted trees was first described by Dür [5], who realized that Butcher's group [2] (developed in the context of numerical integration of ordinary differential equations) was actually an affine group scheme, and consequently has associated two dual Hopf algebra structures, a commutative one and a cocommutative one. Actually, many combinatorics and recursive formulae related to $\mathcal{H}_R$ were already present in Butcher's seminal work, in particular, recursion (5) (in the sense of Remark 4), which is equivalent to formula (2) given in [4]. In [7], the cocommutative dual of $\mathcal{H}_R$ is described together with several other cocommutative Hopf algebras on families of trees including the family of rooted trees labelled by a given set D. Independently, Kreimer [4] rediscovered the Hopf algebra $\mathcal{H}_R$ in the context of renormalization in quantum field theory. Brouder [3] seems to be the first author to note the relationship of Kreimer's work with Butcher's theory.

Foissy [6] studies the commutative Hopf algebra $\mathcal{H}_R(X)$ of labelled rooted trees as a quotient of a non-commutative Hopf algebra on (labelled planar rooted) trees. In [6], it is shown that under certain restrictions on the $\mathbb{K}$-module X, there exists another $\mathbb{K}$-module Y such that the Hopf algebra $\mathcal{H}_R(X)$ is isomorphic to a shuffle Hopf algebra $\mathrm{Sh}(Y)$. As a graded Hopf algebra, $\mathcal{H}_R(X)$ with its canonical grading ($X \subset \mathcal{H}_R(X)_1$) is isomorphic to $\mathrm{Sh}(Y)$ with a non-canonical grading ($Y \not\subset \mathrm{Sh}(X)_1$).

In the present work, we show that the Hopf algebra $\mathrm{Sh}(X)$ is isomorphic to the quotient Hopf algebra $\mathcal{H}_R(X)/\mathcal{I}$ for an explicitly given Hopf ideal $\mathcal{I}$, This isomorphism is compatible, for instance, with the canonical gradings of $\mathrm{Sh}(X)$ and $\mathcal{H}_R(X)$. Based on this isomorphism, we describe the Hopf algebra structure of $\mathrm{Sh}(X)$ in terms of a basis of its underlying $\mathbb{K}$-module structure associated to a Hall set of labelled rooted trees. This basis turns out to be the dual of the Poincaré-Witt-Birkhoff basis of $T(X)$ corresponding to a Hall basis of the free Lie algebra $\mathcal{L}(D)$. Subsets of labelled rooted trees associated to Hall sets (Hall sets of labelled rooted trees) were first considered (for the case $D = \{1, 2, 3, \ldots\}$) in [15] in a completely different context (actually, the results in [15] conveniently interpreted in algebraic terms are related to the present work).

The plan of the paper is as follows. In Section 2, definitions and fundamental results (together with some useful consequences) on the commutative Hopf algebra of labelled rooted trees are collected. The shuffle Hopf algebra is considered in Section 3. Section 4 is devoted to explore and to take advantage of the relation between the shuffle Hopf algebra $\mathrm{Sh}(X)$ and the Hopf algebra $\mathcal{H}_R(X)$ of labelled rooted trees. In Subsection 4.1, an epimorphism ν of graded Hopf algebras from $\mathcal{H}_R$ to $\mathrm{Sh}(X)$ is constructed, and the graded Hopf ideal $\mathcal{I} = \ker \nu$ is explicitly given, showing that $\mathrm{Sh}(X)$ is isomorphic as a graded Hopf algebra to the quotient Hopf algebra $\mathcal{H}_R/\mathcal{I}$. Hall sets of labelled rooted trees are introduced in Subsection 4.2, and in Subsection 4.3, some known results about basis of the shuffle algebra $\mathrm{Sh}(X)$ associated to Hall sets are stated with our notation. The main goal of the remaining subsections of Section 4 is to describe the coalgebra structure of $\mathrm{Sh}(X)$ in terms of basis associated to Hall sets, and in addition, proofs of the results stated in Subsection 4.3 are also obtained. Subsection 4.4 is of technical nature. In Subsection 4.5, it is shown that the image by $\nu : \mathcal{H}_R \to \mathrm{Sh}(X)$ of an arbitrary Hall set $\widehat{\mathcal{T}}$ of labelled rooted trees freely generates the shuffle algebra $\mathrm{Sh}(X)$ when the base ring $\mathbb{K}$ is a $\mathbb{Q}$-algebra. For arbitrary base rings $\mathbb{K}$, a basis of $\mathrm{Sh}(X)$ is constructed as the image by ν of a set $\widehat{\mathcal{F}}^*$ of labelled forest that is in one-to-one correspondence with the set $\widehat{\mathcal{F}}$ of forests of Hall rooted trees in $\widehat{\mathcal{T}}$. The results in Subsection 4.5 allows the description of the coalgebra structure of $\mathrm{Sh}(X)$ in terms of its basis $\nu(\widehat{\mathcal{F}}^*)$. Section 4.6 focuses on proving that the basis $\nu(\widehat{\mathcal{F}}^*)$ of $\mathrm{Sh}(X)$ is dual to the Poincaré-Witt-Birkhoff basis of $T(X)$ corresponding to a Hall basis of the free Lie algebra $\mathcal{L}(D)$. Section 5 closes the paper with concluding remarks.

2 The commutative Hopf algebra of labelled rooted trees

s:art

A forest is an isomorphism class of finite partially ordered sets F satisfying the following condition.

$$x, y, z \in F,\ x \neq y,\ y < x,\ z < x \quad \Longrightarrow \quad \text{either } y < z \text{ or } z < y. \tag{1}$$

eq:forestcon

A rooted tree t is a forest with only one minimal element, called the root of t. Forests and rooted trees can then be considered as finite directed graphs. Each forest can be uniquely decomposed as a direct union of rooted trees, its connected components.

Given a set D, rooted trees and forests labelled by D can be defined as follows.

A partially ordered set labelled by D is a partially ordered set F together with a map from F to D (the labelling of F). An isomorphism of partially ordered sets labelled by D is a bijection of the underlying sets that preserves the orderings and the labellings. A forest (resp. rooted tree) labelled by D is an isomorphism class of finite partially ordered sets labelled by D satisfying condition (1) (resp. with only one minimal element and satisfying condition (1)). The degree $|u|$ of a forest u labelled by D is the cardinal of the underling set of a representative partially ordered set (that is, the number of vertices in u). Given a forest u labelled by D, the partial degree $|u|_d$ of u with respect to $d \in D$ is the number of vertices in u that are labelled by d. We denote as $\mathcal{F}(D)$ (resp. $\mathcal{T}(D)$) the set of forests (resp. rooted trees) labelled by D, or simply $\mathcal{F}$ (resp. $\mathcal{T}$) if no ambiguity arises.

The symmetry number $\sigma(u)$ of a labelled forest u is the number of different bijections of the underlying set of a labelled partially ordered set representing u that are isomorphisms of labelled partially ordered sets.

It is already well known [6] that a commutative Hopf algebra structure can be given to the free $\mathbb{K}$-module over the set $\mathcal{F}$ of forests labelled by D. We denote this commutative Hopf algebra structure as $\mathcal{H}_R(X)$, where we denote $X = \mathbb{K}D$, or simply as $\mathcal{H}_R$ if no ambiguity arises. The product in $\mathcal{H}_R$ corresponds to the direct union of forests, and the unity element is the empty (labelled) forest e. As a commutative algebra, $\mathcal{H}_R$ is freely generated by $\mathcal{T}$.

The Hopf algebra structure $\mathcal{H}_R$ is compatible with the $\mathbb{Z}$-grading induced by the degree $|u|$ of labelled forests. Thus, for each $n \geq 0$, the homogeneous component $(\mathcal{H}_R)_n$ is freely generated as a $\mathbb{K}$-module by the set $\mathcal{F}_n$ of labelled forests of degree n. In particular, $(\mathcal{H}_R)_0 = \mathbb{K}e$, and $\mathcal{H}_R$ is a $\mathbb{Z}$-graded connected Hopf algebra. Recall that the counit of any $\mathbb{Z}$-graded connected Hopf algebra is uniquely defined. In particular, the counit $\epsilon : \mathcal{H}_R \to \mathbb{K}$ is determined by $\epsilon(e) = 1$, and $\epsilon(u) = 0$ for any non-empty forest u. The augmentation ideal $\mathcal{H}_R^+ = \ker \epsilon$ is the free $\mathbb{K}$-module over the set of non-empty forests $\mathcal{F}\backslash\{e\}$. Furthermore, as any $\mathbb{Z}$-graded connected bialgebra, the bialgebra $\mathcal{H}_R$ admits a unique $\mathbb{Z}$-graded connected Hopf algebra structure. That is, the antipode S is uniquely determined from the $\mathbb{Z}$-graded algebra structure of $\mathcal{H}_R$ and the definition of the coproduct Δ.

The coproduct Δ (and the antipode S) of a forest labelled by D can be defined in terms of cutting operations on the corresponding graphs [5]. In particular, $\Delta d = d \otimes e + e \otimes d$ for each $d \in D$ (that is, all the labelled rooted trees of degree 1 are primitive elements of the $\mathbb{Z}$-graded connected Hopf algebra $\mathcal{H}_R$).

Given $d \in D$, $t_1, \ldots, t_m \in \mathcal{T}$, $u = t_1 \cdots t_m \in \mathcal{F}$, we denote by $B_d(u)$ the labelled rooted tree of degree $|t_1| + \cdots + |t_m| + 1$ obtained by grafting the roots of $t_1, \ldots, t_m$ to a new root labelled by d. In particular, $B_d(e)$ is the labelled rooted tree with only one vertex, labelled by d. We hereafter identify $B_d(e)$ with d. Given a labelled rooted tree $t \in \mathcal{T}$ and a labelled forest $u \in \mathcal{F}$, we denote by $t \circ u$ the labelled rooted tree of degree $|u| + |t|$ obtained by grafting the labelled rooted trees in u to the root of t. In particular, we have that $B_d(u) = d \circ u$ for each $d \in D$, $u \in \mathcal{F}$, and $t \circ e = t$ for each $t \in \mathcal{T}$. The symmetry number of forests can be recursively obtained as follows.

l:symmetry **Lemma 1** *For each $d \in D$, $t_1, \cdots, t_m \in \mathcal{T}$, $t_i \neq t_j$ if $i \neq j$,*

$$\sigma(e) = 1, \quad \sigma(B_d(u)) = \sigma(u), \quad \sigma(u) = \prod_{j=1}^{m} i_j! \sigma(t_j)^{i_j}, \quad \textit{if} \quad u = \prod_{j=1}^{m} t_j^{i_j}.$$

Let us denote as $\mathcal{M}_R$ (resp. $(\mathcal{M}_R)_n$) the free $\mathbb{K}$-module over $\mathcal{T}$ (resp. over the set $\mathcal{T}_n$ of labelled rooted trees of degree n), viewed as a $\mathbb{K}$-submodule of $\mathcal{H}_R$ (resp. $(\mathcal{H}_R)_n$). An isomorphism $B : X \otimes \mathcal{H}_R \to \mathcal{M}_R$ of $\mathbb{Z}$-graded $\mathbb{K}$-modules can be defined as $B(d \otimes u) = B_d(u)$ for each $d \in D$, $u \in \mathcal{F}$.

The coproduct Δ in $\mathcal{H}_R$ can alternatively be defined (as an alternative to the definition in terms of admissible cuts of labelled forests) as the unique algebra map $\Delta : \mathcal{H}_R \to \mathcal{H}_R \otimes \mathcal{H}_R$ such that [4, 6],

$$\Delta B_d = B_d \otimes e + (\mathrm{id} \otimes B_d)\Delta, \quad d \in D, \tag{2}$$ eq:Delta

where id denotes the identity map in $\mathcal{H}_R$.

The commutative Hopf algebra of rooted trees over $X = \mathbb{K}D$ can be characterized by the following universal property [4, 6].

t:DeltaA **Theorem 1** *Given a commutative algebra $\mathcal{A}$ over $\mathbb{K}$ and a $\mathbb{K}$-module map $L : X \otimes \mathcal{A} \to \mathcal{A}$, there exists a unique algebra homomorphism $\phi : \mathcal{H}_R \to \mathcal{A}$ such that*

$$\phi B = L(\mathrm{id}_X \otimes \phi). \tag{3}$$ eq:commuting

If $\mathcal{A}$ has a Hopf algebra (alternatively, bialgebra) structure satisfying $\operatorname{Im} L \subset \ker \epsilon_{\mathcal{A}}$ and

$$\Delta_{\mathcal{A}} L_d = L_d \otimes 1_{\mathcal{A}} + (\mathrm{id}_{\mathcal{A}} \otimes L_d)\Delta_{\mathcal{A}}, \tag{4}$$ eq:DeltaA

where $L_d(a) = L(d \otimes a)$, then ϕ is a Hopf algebra (alternatively, bialgebra) homomorphism.

:phigraded **Remark 1** Recall that $\mathcal{H}_R(X)$ has a structure of $\mathbb{Z}$-graded Hopf algebra with the (canonical) $\mathbb{Z}$-grading induced by the degree $|u|$ of labelled forests, and that $B : X \otimes \mathcal{H}_R \to \mathcal{H}_R$ is an homomorphism of $\mathbb{Z}$-graded $\mathbb{K}$-modules. If in Theorem 1, $\mathcal{A}$ is a $\mathbb{Z}$-graded algebra and L is a homomorphism of $\mathbb{Z}$-graded $\mathbb{K}$-modules, then ϕ is an homomorphism of $\mathbb{Z}$-graded algebras. If in addition $\mathcal{A}$ has a $\mathbb{Z}$-graded Hopf algebra (resp. bialgebra) structure, then $\operatorname{Im} L \subset \ker \epsilon_{\mathcal{A}}$ automatically holds, and ϕ is an homomorphism of $\mathbb{Z}$-graded Hopf algebras (resp. bialgebras). $\square$

rtgradings **Remark 2** The Hopf algebra $\mathcal{H}_R(X)$ admits different $\mathbb{Z}$-gradings. Actually, the Hopf algebra structure of $\mathcal{H}_R(X)$ is compatible with any $\mathbb{Z}$-grading induced by an arbitrary $\mathbb{Z}$-grading of the free $\mathbb{K}$-module $X = \mathbb{K}\, D$ (i.e. induced by an arbitrary weight function $D \to \mathbb{Z}$). Furthermore, the Hopf algebra $\mathcal{H}_R(X)$ admits a more general grading based on the partial degrees $|u|_d$ for forests $u \in \mathcal{F}$ as follows. Consider the additive group G of maps $g : D \to \mathbb{Z}$, and consider for each $g \in G$ the set $\mathcal{F}^g = \{u \in \mathcal{F} : \ |u|_d = g(d)\}$. Then, the free $\mathbb{K}$-module $\mathcal{H}_R$ is G-graded as $\mathcal{H}_R = \bigoplus_{g \in G^+} (\mathcal{H}_R)^g$, where G^+ denotes the submonoid of G of non-negative maps, and each $(\mathcal{H}_R)^g$ is the free $\mathbb{K}$-module over $\mathcal{F}^g$. The homogeneous components $(\mathcal{H}_R)^g$ are sometimes referred as finely homogeneous components of $\mathcal{H}_R$. The Hopf algebra structure of $\mathcal{H}_R(X)$ is compatible with this G-grading. As each $\mathcal{T}^g$ is finite, the finely homogeneous components are of finite rank.

The statement in Remark 1 can be generalized as follows. If in Theorem 1, $\mathcal{A}$ is a graded algebra (resp. Hopf algebra, bialgebra) and L is a homomorphism of graded $\mathbb{K}$-modules, then ϕ is an homomorphism of graded algebras (resp. Hopf algebras, bialgebras), where the term graded refers to any of the $\mathbb{Z}$-gradings or the G-grading above. Hereafter, we will simply write 'graded, when meaning that it can be interpreted in the sense of any of the gradings above. $\square$

r:rho **Remark 3** The graded $\mathbb{K}$-module $\mathcal{M}_R$ can be endowed with a graded right $\mathcal{H}_R$-module structure by extending the grafting operation $t \circ u$ ($u \in \mathcal{F}$, $t \in \mathcal{T}$) to a graded $\mathbb{K}$-module map $\circ : \mathcal{M}_R \otimes \mathcal{H}_R \to \mathcal{M}_R$. Furthermore, (2) implies that $(\mathcal{M}_R, \circ, \rho)$ has a Hopf $\mathcal{H}_R$-module structure with $\rho : \mathcal{M}_R \to \mathcal{H}_R \otimes \mathcal{M}_R$ given by $\rho(t) = \Delta(t) - t \otimes e$ for $t \in \mathcal{M}_R$. In particular, we have that

$$\rho(t \circ u) = \rho(t) \circ \Delta(u), \quad u \in \mathcal{H}_R, \quad t \in \mathcal{M}_R, \tag{5}$$ eq:Deltarec

where $(u \otimes t) \circ (v \otimes w) = uv \otimes t \circ w$ for each $u, v, w \in \mathcal{H}_R$, $t \in \mathcal{M}_R$. $\square$

r:Butcher **Remark 4** Equality (5) applied for $t, u \in \mathcal{T}$ gives, together with $\rho(d) = e \otimes d$ ($d \in D$) and $\Delta(t) = t \otimes e + \rho(t)$ for $t \in \mathcal{T}$, a recursive definition of ρ (hence, the restriction of Δ to $\mathcal{M}_R$), which involves only labelled rooted trees. $\square$

3 The shuffle Hopf algebra $\mathrm{Sh}(X)$ over X

s:sh

3.1 The shuffle algebra over X

The shuffle algebra $\mathrm{Sh}(X)$ over $X = \mathbb{K}\,D$ is a commutative graded connected algebra that can be constructed as follows. A commutative algebra structure is given to the $\mathbb{K}$-module $\mathbb{K} \oplus X \oplus X^{\otimes 2} \oplus X^{\otimes 3} \oplus \cdots$ by defining the shuffle product $\sqcup\!\sqcup$ of two *words*. We follow the standard notation of denoting each element $d_1 \otimes \cdots \otimes d_m \in X^{\otimes m}$ (each word of degree m) as $d_1 \cdots d_m$, and the concatenation of two words $w_1 = d_1 \cdots d_m \in X^{\otimes m}$, $w_2 = d_{m+1} \cdots d_{m+l} \in X^{\otimes l}$ as $w_1 w_2 := d_1 \cdots d_{m+l} \in X^{\otimes (m+l)}$. The shuffle product $\sqcup\!\sqcup$ of two words is

$$(d_1 \cdots d_m) \sqcup\!\sqcup (d_{m+1} \cdots d_{m+l}) = \sum d_{i_1} \cdots d_{i_{m+l}} \tag{6}$$ eq:shufflepr

where $d_1, \ldots, d_{m+l} \in D$, and the summation goes over all permutations $(i_1, \ldots, i_{m+l})$ of $(1, \ldots, m+l)$ that preserve the partial orderings of $(1, \ldots, m)$ and $(m+1, \ldots, m+l)$. The unity element is the empty word, which we denote as $\widehat{e}$. The degree $|w|$ (resp. partial degree $|w|_d$, $d \in D$) of a word $w = d_1 \cdots d_m$ is m (resp. the number of letters in $d_1, \ldots, d_m$ that coincide with d).

As $\mathrm{Sh}(X)$ is graded connected, it admits a unique augmentation $\widehat{\epsilon} : \mathrm{Sh}(X) \to \mathbb{K}$, which is determined by $\widehat{\epsilon}(\widehat{e}) = 1$ and $\widehat{\epsilon}(u) = 0$ for arbitrary non-empty words u.

r:Ggraded **Remark 5** The term graded referred above can be interpreted, as in the rest of the present work, in the sense given at the end of Remark 2. In particular, the algebra structure of $\mathrm{Sh}(X)$ (and the Hopf algebra structure on it below) is compatible with the G-grading given in Remark 2, and its finely homogeneous components $(\mathrm{Sh}(X))^g$ $(g \in G)$ are of finite rank. $\square$

The shuffle product satisfies the following identity, that can be used as an alternative recursive definition to (6). Given $d_1, \ldots, d_m \in D$, let us denote $C_{d_1}(\widehat{e}) := d_1$ and $C_{d_m}(d_1 \cdots d_{m-1}) := d_1 \cdots d_{m-1} d_m$. Then, each non-empty word can be uniquely written as $C_d(u)$ with $d \in D$ and $u \in \mathrm{Sh}(X)$. It then holds that

$$C_d(u) \sqcup\!\sqcup C_f(v) = C_d(u \sqcup\!\sqcup C_f(v)) + C_f(v \sqcup\!\sqcup C_d(u)), \quad d, f \in D, \quad u, v \in \mathrm{Sh}(X). \tag{7}$$ eq:shufflepr

Let us denote $\mathrm{Sh}(X)^+$ the augmentation ideal $\mathrm{Sh}(X)^+ = \ker \widehat{\epsilon}$ (that is, the free $\mathbb{K}$-module over the set of non-empty words). Then, $C : X \otimes \mathrm{Sh}(X) \to \mathrm{Sh}(X)^+$ given by $C(d \otimes u) = C_d(u)$, $d \in D$, $u \in \mathrm{Sh}(X)$, is an isomorphism of graded $\mathbb{K}$-modules.

3.2 The Hopf algebra structure of $\mathrm{Sh}(X)$

The commutative graded connected algebra $\mathrm{Sh}(X)$ is endowed with a unique (commutative graded connected) Hopf algebra structure by considering $\widehat{\epsilon}$ as counit, and defining the coproduct $\widehat{\Delta} : \mathrm{Sh}(X) \to \mathrm{Sh}(X) \otimes \mathrm{Sh}(X)$ as follows. For the empty word $\widehat{\Delta}\widehat{e} = \widehat{e} \otimes \widehat{e}$, and for each non-empty word $u = d_1 \cdots d_m$, $d_1, \ldots, d_m \in D$,

$$\Delta u = \widehat{e} \otimes u + \sum_{l=1}^{m-1} d_1 \cdots d_l \otimes d_{l+1} \cdots d_m + u \otimes \widehat{e}. \tag{8}$$ eq:shuffleco

Clearly, the coproduct $\widehat{\Delta}$ satisfies the identity

$$\widehat{\Delta} C_d = C_d \otimes \widehat{e} + (\widehat{\mathrm{id}} \otimes C_d)\widehat{\Delta}, \quad d \in D. \tag{9}$$ eq:shuffleco

Therefore, Theorem 1 can be applied with $(\mathcal{A}, L) = (\mathrm{Sh}(X), C)$. In the remaining of the paper, we denote by ν the corresponding graded Hopf algebra map $\mathcal{H}_R \to \mathrm{Sh}(X)$.

Remark 6 The map $\nu : \mathcal{H}_R \to \mathrm{Sh}(X)$ can be explicitly be defined as follows. Given $u \in \mathcal{F} \backslash \{e\}$, consider a labelled partially ordered set U representing the forest u, and let $x_1, \ldots, x_n$ be the elements in U labelled as $l(x_i) = d_i \in D$ for each $i = 1, \ldots, n$. Then

$$\nu(u) = \sum_{(i_1, \ldots, i_n) \in \mathcal{P}(U)} d_{i_1} \cdots d_{i_n} \tag{10}$$ eq:dalpha

where $(i_1, \ldots, i_n) \in \mathcal{P}(U)$ if $x_{i_1} > \cdots > x_{i_n}$ is a total order relation on $\{x_1, \ldots, x_n\}$ that extends the partial order relation in U. $\square$

r:ideal **Remark 7** In particular,

$$\nu(B_{d_m}\cdots B_{d_2}(d_1)) = d_1\cdots d_m,\ m\geq 1,\ d_1,\ldots,d_m\in D, \tag{11}$$ eq:nusurject

which provides a bijection between the set of non-empty words and the set of labelled rooted trees without ramifications. This shows that ν is surjective. Hence, the graded Hopf algebra $\mathrm{Sh}(X)$ is isomorphic to the graded quotient Hopf algebra $\mathcal{H}_R/(\ker\nu)$. Theorem 2 below explicitly provides $\ker\nu$. $\square$

3.3 A $\mathrm{Sh}(X)$-module structure of $\mathrm{Sh}(X)$

As $C : X\otimes \mathrm{Sh}(X)\to \mathrm{Sh}(X)^+$ is an isomorphism of graded $\mathbb{K}$-modules, the canonical right $\mathrm{Sh}(X)$-module structure of $X\otimes\mathrm{Sh}(X)$ induces a right $\mathrm{Sh}(X)$-module structure for $\mathrm{Sh}(X)^+$. In particular, we have that $C_d(w) = d\bullet w$ for each $d\in D$, $w\in\mathrm{Sh}(X)$. Theorem 1 applied for $(\mathcal{A},L) := (\mathrm{Sh}(X),C)$ implies that

$$\nu(t\circ u) = \nu(t)\bullet\nu(u) \quad \text{for each} \quad u\in\mathcal{H}_R, \quad t\in\mathcal{M}_R. \tag{12}$$ eq:nucirc

It is interesting to note that, by definition of the right $\mathrm{Sh}(X)$-module structure of $\mathrm{Sh}(X)^+$, (7) reads $C_d(u)⧢C_f(v) = C_d(u)\bullet C_f(v) + C_f(v)\bullet C_d(u)$, that is,

$$u⧢v = u\bullet v + v\bullet u, \quad \text{for each} \quad u,v\in\mathrm{Sh}(X)^+. \tag{13}$$ eq:uvvu

Similar to Remark 3, consider $\widehat{\rho} : \mathrm{Sh}(X)^+\to\mathrm{Sh}(X)\otimes\mathrm{Sh}(X)^+$ given by $\widehat{\rho}(w) = \widehat{\Delta}(w) - w\otimes\widehat{e}$ for each $w\in\mathrm{Sh}(X)^+$. Then, (9) implies that $(\mathrm{Sh}(X)^+,\bullet,\widehat{\rho})$ has a Hopf $\mathrm{Sh}(X)$-module structure, in particular,

$$\widehat{\rho}(v\bullet u) = \widehat{\rho}(v)\bullet\widehat{\Delta}(u), \quad u\in\mathrm{Sh}(X), \quad v\in\mathrm{Sh}(X)^+. \tag{14}$$ eq:deltauv

where $(v_1\otimes v_2)\bullet(w_1\otimes w_2) = v_1w_1\otimes v_2\bullet w_2$ for each $v_2\in\mathrm{Sh}(X)^+$ and $w_1,w_2,v_1\in\mathrm{Sh}(X)$.

Actually, (14) together with $\widehat{\rho}d = \widehat{e}\otimes d$ for $d\in D$ and $\widehat{\Delta} = \mathrm{id}\otimes\widehat{e} + \widehat{\rho}$ can be used to define $\widehat{r}ho$ and $\widehat{\Delta}$ recursively in terms of $\bullet : \mathrm{Sh}(X)^+\otimes\mathrm{Sh}(X)\to\mathrm{Sh}(X)^+$.

r:zienbel **Remark 8** The $\mathbb{K}$-module $\mathrm{Sh}(X)$ has with $\bullet : \mathrm{Sh}(X)^+\otimes\mathrm{Sh}(X)\to\mathrm{Sh}(X)^+$ a non-associative algebra structure called Zienbel algebra [11, 12], which is actually the free Zienbel algebra over the $\mathbb{K}$-module X. In [12], an epimorphism of Dendriform algebras from the free Dendriform algebra over X to the free Zienbel algebra over X is considered. As free dendriform algebras can be described in terms of planar binary trees (with labelled leaves) [12], such epimorphism can be used to work in the free Zienbel algebra over X in terms of such trees. This has strong similarities with our approach exploiting the epimorphism $\nu : \mathcal{H}_R\to\mathrm{Sh}(X)$ for working in the shuffle algebra $\mathrm{Sh}(X)$ (or equivalently, in the free Zienbel algebra over X) in terms of labelled rooted trees.

The Zienbel algebra structure of $\mathrm{Sh}(X)$ is also considered in the context of non-linear control theory [18], which is sometimes referred as chronological algebra (see [8] and references therein). $\square$

3.4 The dual algebra $\mathrm{Sh}(X)^*$

s:dual

Let us now consider the dual algebra $\mathrm{Sh}(X)^*$ of the coalgebra structure of $\mathrm{Sh}(X)$. That is, $\alpha \in \mathrm{Sh}(X)^*$ if $\alpha : \mathrm{Sh}(X) \to \mathbb{K}$ is a $\mathbb{K}$-module map, the unit in $\mathrm{Sh}(X)^*$ is the counit $\widehat{\epsilon}$ of $\mathrm{Sh}(X)$, and for each $\alpha, \beta \in \mathrm{Sh}(X)^*$, the product $\alpha\beta$ is defined by

$$\langle \alpha\beta, w\rangle = \langle \alpha \otimes \beta, \widehat{\Delta} w\rangle, \quad w \in \mathrm{Sh}(X). \tag{15}$$ eq:alphabeta

The subalgebra of $\mathrm{Sh}(X)^*$ of elements α such that $\langle \alpha, w\rangle \neq 0$ for a finite number of words w is isomorphic to the tensor algebra $T(X)$.

Let us denote as $\mathrm{Der}(\mathrm{Sh}(X))$ the Lie algebra of $\widehat{\epsilon}$-derivations of $\mathrm{Sh}(X)$, namely,

$$\mathrm{Der}(\mathrm{Sh}(X)) = \{\alpha \in \mathrm{Sh}(X)^* : \ \alpha(uv) = \alpha(u)\widehat{\epsilon}(v) + \widehat{\epsilon}(u)\alpha(v), \text{ for all } u, v \in \mathrm{Sh}(X)\}. \tag{16}$$ eq:der

That is, given $\alpha \in \mathrm{Sh}(X)^*$, $\alpha \in \mathrm{Der}(\mathrm{Sh}(X))$ if and only if

$$\ker \widehat{\epsilon} \oplus (\mathrm{Sh}(X)^+)^{\sqcup\!\sqcup 2} = \mathbb{K} \oplus (\mathrm{Sh}(X)^+)^{\sqcup\!\sqcup 2} \subset \ker \alpha. \tag{17}$$ eq:keralpha

Recall that $\mathrm{Der}(\mathrm{Sh}(X))$ is a Lie algebra over $\mathbb{K}$ under the bracket $[\alpha, \beta] = \alpha\beta - \beta\alpha$.

Remark 9 When $\mathbb{K}$ has 0 characteristic, the Lie algebra of primitive elements of $T(X)$ is the free Lie algebra $\mathcal{L}(D)$ over the set D. Then, the duality between $T(X)$ and $\mathrm{Sh}(X)$ implies that $\mathcal{L}(D)$ is isomorphic to the Lie subalgebra of $\mathrm{Der}(\mathrm{Sh}(X))$ of elements α such that $\langle \alpha, w\rangle \neq 0$ for a finite number of words w. $\square$

4 The shuffle algebra and Hall sets of rooted trees

s:shrt

4.1 The Hopf algebras $\mathcal{H}_R(X)$ and $\mathrm{Sh}(X)$

ss:artsh

According to Remark 7, the Hopf algebra $\mathrm{Sh}(X)$ is isomorphic to the quotient Hopf algebra $\mathcal{H}_R/\mathcal{I}$ where $\mathcal{I} = \ker \nu$. Next, the Hopf ideal $\mathcal{I}$ is explicitly determined.

l:xi

Lemma 2 *Consider the graded $\mathbb{K}$-module map $\xi : \mathcal{H}_R^+ \to \mathcal{M}_R$ given by*

$$\xi(t_1 \cdots t_m) = \sum_{i=1}^{m} t_i \circ (t_1 \cdots t_{i-1} t_{i+1} \cdots t_m), \quad t_1, \ldots, t_m \in \mathcal{T}, \tag{18}$$ eq:xi

and $\xi(t) = t$ if $t \in \mathcal{T}$. It holds that $\nu\xi = \nu$.

Proof: This can be proven by induction on m as follows. It trivially holds that $\nu\xi(t) = \nu(t)$ if $m = 1$. It is straightforward from the definition of ξ that

$$\xi(uv) = \xi(v) \circ u + \xi(u) \circ v, \quad u, v \in \mathcal{F}\backslash\{e\}. \tag{19}$$ eq:xirec

Application of induction hypothesis, (12) and (13) leads to the required result. $\square$

t:kerphi **Theorem 2** *The graded ideal $\mathcal{I}$ generated by* $\mathrm{Im}\,(\mathrm{id}-\xi)$ *is a graded Hopf ideal. Furthermore, the shuffle Hopf algebra* $\mathrm{Sh}(X)$ *is isomorphic as a graded Hopf algebra to the quotient Hopf algebra* $\mathcal{H}_R/\mathcal{I}$.

Proof: Let us consider the canonical algebra map $\varphi : \mathcal{H}_R \to \mathcal{H}_R/\mathcal{I}$. By virtue of Lemma 2, $\mathcal{I} \subset \ker \nu$, and thus there exists a unique algebra map $\bar{\nu} : \mathcal{H}_R/\mathcal{I} \to \mathrm{Sh}(X)$ such that $\nu = \bar{\nu}\varphi$. We will prove that $\bar{\nu}$ is bijective, so that it is an isomorphism of graded algebras. The statement of Theorem 2 then follows from the fact that $\nu : \mathcal{H}_R \to \mathrm{Sh}(X)$ is an homomorphism of graded Hopf algebras.

It then only remains to prove that $\bar{\nu}$ is bijective. The identity (11) shows that the restriction of ν to the $\mathbb{K}$-submodule $\widehat{\mathcal{M}_R}$ of $\mathcal{M}_R$ (freely) generated by the set

$$\{B_{d_1} \cdots B_{d_{m-1}}(d_m) : \quad m \geq 1,\ d_1, \ldots, d_m \in D, \}$$

of labelled rooted trees without ramifications is bijective. This implies that $\bar{\nu}$ is surjective, and it is sufficient to show that the restriction of φ to $\widehat{\mathcal{M}_R}$ is surjective. We thus need to show that each $u \in \mathcal{F}\backslash\{e\}$ is congruent modulo $\mathcal{I}$ to some $t \in \widehat{\mathcal{M}_R}$. This can be shown by induction on the degree $|u|$. This is trivial if $|t| = 1$. For $|u| > 1$, let u be $u = t_1 \cdots t_m$ with $m \geq 1$, $t_1, \ldots, t_m \in \mathcal{T}$, and let us consider for each $i = 1, \ldots, m$, $d_i \in D$, $u_i, v_i \in \widehat{\mathcal{F}}$ such that $u = t_i u_i$ and $t_i = B_{d_i}(v_i)$. Then we have that

$$u = (u - \xi(u)) + \sum_{i=1}^{m} B_{d_i}(u_i v_i).$$

By induction hypothesis, each $u_i v_i$ ($|u_i v_i| = |u| - 1$) is congruent modulo $\mathcal{I}$ to some $z_i \in \widehat{\mathcal{M}_R}$, so that u is congruent modulo $\mathcal{I}$ to $\sum_{i=1}^{m} B_{d_i}(z_i) \in \widehat{\mathcal{M}_R}$. $\Box$

Remark 10 Let us denote $\mathcal{S}_m = \{\xi(t_1 \cdots t_m) - t_1 \cdots t_m :\ t_1, \ldots, t_m \in \mathcal{M}_R\}$ for each $m \geq 1$. It is not difficult to check that $\mathcal{I} = \ker \nu$ (the ideal generated by $\mathrm{Im}\,(\mathrm{id}-\xi) = \sum_{m\geq 2} \mathcal{S}_m$) is actually generated by the set $\mathcal{S}_2 \cup \mathcal{S}_3$, or alternatively, by the set $\mathcal{S}_2 \cup (\mathcal{M}_R \circ \mathcal{S}_2)$. $\Box$

4.2 Hall sets of rooted trees

s:Halltrees

Given a subset $\widehat{\mathcal{T}}$ of the set $\mathcal{T}$ of rooted trees labelled by D, we consider the set of forests $u = t_1 \cdots t_m$, where $t_1, \ldots, t_m \in \widehat{\mathcal{T}}$. We denote by $\widehat{\mathcal{F}}$ the set of such forests, including the empty forest e, and we denote as $\widetilde{\mathcal{T}}$ the subset of labelled rooted trees of the form $B_d(u)$, $d \in D$, $u \in \widehat{\mathcal{F}}$.

If $\widehat{\mathcal{T}}$ has a total order relation, we give a total ordering to $\widehat{\mathcal{T}} \cup \{e\}$ by considering $e < t$ for each $t \in \widehat{\mathcal{T}}$. If $u = t_1 \cdots t_m \in \widehat{\mathcal{F}}$, we define $\min(u) = \min(t_1, \ldots, t_m)$, $\max(u) = \max(t_1, \ldots, t_m)$, $\min(e) = e$, and $\max(e) = e$.

Definition 1 *A subset* $\widehat{\mathcal{T}} \subset \mathcal{T}$ *is* consistent *if the following condition holds. Given* $t_1, \ldots, t_m \in \mathcal{T}$, $d \in D$, *if* $B_d(t_1 \cdots t_m) \in \widehat{\mathcal{T}}$, *then* $d, t_1, \ldots, t_m \in \widehat{\mathcal{T}}$.

composition **Definition 2** *Given a totally ordered consistent subset $\widehat{\mathcal{T}}$ of $\mathcal{T}$, the corresponding set of forests $\widehat{\mathcal{F}}$, and $\widetilde{\mathcal{T}} := \bigcup_{d\in D} B_d(\widehat{\mathcal{F}})$, the* standard decomposition (t', t'') *of each $t \in \widetilde{\mathcal{T}}$ is defined as follows. If $|t| = 1$, then $t' = t$ and $t'' = e$. If $t = B_d(t_1 \cdots t_m)$, $d \in D$, $t_1, \dots, t_m \in \widehat{\mathcal{T}}$, $t_1 \geq \cdots \geq t_m$, then $t'' = t_m$, $t' = B_d(t_1 \cdots t_{m-1})$.*

d:Hall **Definition 3** *We say that a consistent set $\widehat{\mathcal{T}} \subset \mathcal{T}$ supplied with a total ordering $<$ is a* Hall set *of rooted trees labelled by D (or simply a Hall set of rooted trees, if D is clear from the context), if $D \subset \widehat{\mathcal{T}}$ and the following condition holds.*

$$t, z \in \widehat{\mathcal{T}}, \quad t < z \leq t'' \quad \Longrightarrow \quad t \circ z \in \widehat{\mathcal{T}}, \quad t \circ z < z, \tag{20}$$ eq:Hall

where (t', t'') is the standard decomposition of $t \in \widetilde{\mathcal{T}}$.

Reutenauer **Remark 11** Given a Hall set H of words over the alphabet D [17], a Hall set $\widehat{\mathcal{T}}$ of rooted trees labelled by D can be obtained as the image of a map $r : H \to \mathcal{T}$ from the set of Hall words H to the set of labelled rooted trees defined as follows. For $d \in D \subset H$, set $r(d) = d$. For a Hall word $w \in H$ of degree $|w| > 1$, let $d \in D$ be the leftmost letter in w, so that $w = v \otimes d$, where v is a (non-necessarily Hall) word. It is a standard result [17] that there exists a unique non-increasing decomposition of v in Hall words, that is, $v = w_m \otimes \cdots \otimes w_1$, where $w_1, \dots, w_m \in H$ are Hall words satisfying that $w_m \geq \cdots \geq w_1$. Then, we set $t = r(w) = B_d(r(w_1) \cdots r(w_m))$. Conversely, given a Hall rooted tree $t = B_d(t_1 \cdots t_m) \in \widehat{\mathcal{T}}$ of degree $|t| > 1$, where $d \in D$, $t_1, \dots, t_m \in \widehat{\mathcal{T}}$, $t_1 \geq \cdots \geq t_m$, then the corresponding Hall word is $w = r^{-1}(t) = dr^{-1}(t_1) \cdots r^{-1}(t_m)$. We thus have that $r(w) = r(w') \circ r(w'')$ if $w = w'w''$ is the standard factorization of the Hall word $w \in H$, and $r^{-1}(t) = r^{-1}(t'')r^{-1}(t')$ if (t', t'') is the standard decomposition of the Hall rooted tree $t \in \widehat{\mathcal{T}}$. □

4.3 Basis of $\mathrm{Sh}(X)$ associated to a Hall set over D

reutenauer

Recall that each Hall set of words over D, or equivalently (see Remark 11), each Hall set of rooted trees labelled by D has associated a basis of the free Lie algebra $\mathcal{L}(D)$, which by virtue of the Poincaré-Witt-Birkhoff Theorem, provides a basis of the tensor algebra $T(X)$. We next consider such a basis, with $T(X)$ viewed as a subalgebra of the dual algebra $\mathrm{Sh}(X)^*$ of the coalgebra structure of $\mathrm{Sh}(X)$.

d:E_u **Definition 4** *Consider a Hall set $\widehat{\mathcal{T}}$ of rooted trees labelled by D, and the corresponding set of Hall forests $\widehat{\mathcal{F}}$. We set $E_e = \widehat{\epsilon}$, and for each $d \in D$, $E_d \in \mathrm{Der}(\mathrm{Sh}(X))$ is such that $\langle E_d, w\rangle = 0$ for all words $w = d_1 \cdots d_m$ except for $w = d$. For each $t \in \widehat{\mathcal{T}}$ with $|t| > 1$, let (t', t'') be its standard decomposition, then*

$$E_t = [E_{t''}, E_{t'}]. \tag{21}$$ eq:[F,F]

Furthermore, for arbitrary $t_1, \dots, t_m \in \widehat{\mathcal{T}}$ such that $t_1 \leq \cdots \leq t_m$,

$$E_u = E_{t_1} \cdots E_{t_m}, \quad \text{for} \quad u = t_1 \cdots t_m. \tag{22}$$ eq:FF

Theorem 5.3 in [17] (originally due to [19] and improved in [14]) can be interpreted (by virtue of Remark 11 and the recursive definition of symmetry number $\sigma(u)$ of labelled forests given in Lemma 1) in terms of the (Hopf) algebra map $\nu : \mathcal{H}_R \to \mathrm{Sh}(X)$ as follows.

Reutenauer **Theorem 3** *For each $u, v \in \widehat{\mathcal{F}}$, it holds that*

$$\langle E_u, \nu(v) \rangle = \begin{cases} \sigma(u) & \textit{if} \quad u = v \\ 0 & \textit{otherwise.} \end{cases} \tag{23}$$

eq:Reutenaue

This implies that, if the base ring $\mathbb{K}$ is a $\mathbb{Q}$-algebra, $\{\nu(u)/\sigma(u) : \ u \in \widehat{\mathcal{F}}\}$ is the dual basis of the basis $\{E_u : \ u \in \widehat{\mathcal{F}}\}$ of $T(X)$. In particular, it implies the following.

nu(u)basis **Corollary 1** *If the base ring $\mathbb{K}$ is a $\mathbb{Q}$-algebra, then, as a graded algebra, $\mathrm{Sh}(X)$ is freely generated by the set $\{\nu(t) : \ t \in \widehat{\mathcal{T}}\}$, where $\nu : \mathcal{H}_R \to \mathrm{Sh}(X)$ is the unique graded Hopf algebra morphism given by Theorem 1.*

For arbitrary base rings $\mathbb{K}$, a basis of $\mathrm{Sh}(X)$ associated to $\widehat{\mathcal{F}}$ will be obtained if one can find a map $\psi : \widehat{\mathcal{F}} \to \mathrm{Sh}(X)$ such that $\nu(u) = \sigma(u)\psi(u)$ for each $u \in \widehat{\mathcal{F}}$.

d:psi **Definition 5** *For each $u \in \mathcal{F}$, we consider a new labelled forest $u^* \in \mathcal{F}$ as follows. If $d \in D$, $v \in \mathcal{F}\backslash\{e\}$, $k > 1$, $t = B_d(v)$, then*

$$(t^k)^* = t^* \circ (t^{k-1})^*, \quad t^* = B_d(v^*), \quad e^* = e, \tag{24}$$

eq:dpsi

and, if $u = t_1^{k_1} \cdots t_m^{k_m}$, where $t_1, \ldots, t_m \in \mathcal{T}$ are distinct and $k_1, \ldots, k_m \geq 1$, then

$$u^* = (t_1^{k_1})^* \cdots (t_m^{k_m})^*.$$

We denote as $\widehat{\mathcal{T}}^*$ the set $\{t^* : \ t \in \widehat{\mathcal{T}}\}$, and as $\widehat{\mathcal{F}}^*$ the set $\{u^* : \ u \in \widehat{\mathcal{F}}\}$, and define the $\mathbb{K}$-module map $\psi : \mathcal{H}_R \to \mathrm{Sh}(X)$ by setting $\psi(u) = \nu(u^*)$ for $u \in \mathcal{F}$.

p:psi1 **Proposition 1** *For each $u \in \mathcal{F}$, it holds that $\nu(u) = \sigma(u)\nu(u^*)$.*

Proof: Induction on $|u|$. This is trivial for $|u| \leq 1$. If $u = t_1^{k_1} \cdots t_m^{k_m}$, where $t_1, \ldots, t_m \in \mathcal{T}$ are distinct and $k_1, \ldots, k_m \geq 1$, $m > 1$, then, $\sigma(u) = \sigma(t_1^{k_1}) \cdots \sigma(t_m^{k_m})$, and assuming by induction hypothesis that $\nu(t_i^{k_i}) = \sigma(t_i^{k_i})\nu((t_i^{k_i})^*)$, we arrive at $\nu(u) = \sigma(u)\nu(u^*)$. If $u = t^k$, where $t \in \widehat{\mathcal{T}}$, $k > 1$, then $\sigma(t^k) = k\sigma(t^{k-1})\sigma(t)$, and induction hypothesis and $\nu(t^k) = \nu(\xi(t^k)) = \nu(k\, t \circ t^{k-1}) = k\nu(t) \bullet \nu(t^{k-1})$ leads to $\sigma(t^k)\nu((t^k)^*) = k\, \sigma(t^{k-1})\sigma(t)\nu(t^*) \bullet \nu((t^{k-1})^*) = k\, \nu(t) \bullet \nu(t^{k-1}) = \nu(\xi(t^k)) = \nu(t^k)$. Finally, if $u = t \in \widehat{\mathcal{T}}$, with $t = B_d(v)$, $d \in D$, and $v \in \widehat{\mathcal{T}}$, then $\sigma(t) = \sigma(v)$, and by induction hypothesis and the identity $C_d \nu = \nu B_d$ we arrive at $\nu(t) = C_d(\nu(v)) = \sigma(v) C_d(\nu(v^*)) = \sigma(t)\nu(t^*)$. $\square$

Theorem 5.3 in [17] written in the form of Theorem 3 together with Proposition 1 can be used to prove that $\{\nu(u) : \ u \in \widehat{\mathcal{F}}^*\}$ is a basis of the shuffle algebra $\mathrm{Sh}(X)$ when the base ring is $\mathbb{Z}$, and then for arbitrary base rings $\mathbb{K}$. Our aim now is to describe the coalgebra structure of $\mathrm{Sh}(X)$ in this basis. In order to do that, we can use the fact that ν is a

Hopf algebra homomorphism, and in particular, that $\widehat{\Delta}\nu = (\nu \otimes \nu)\Delta$. We then need to rewrite arbitrary $\nu(v)$, $v \in \mathcal{F}$ in the basis $\nu(\widehat{\mathcal{F}}^*)$ which can be done recursively if the maps $C_d : \mathrm{Sh}(X) \to \mathrm{Sh}(X)^+$ (or more generally, the $\mathrm{Sh}(X)$-module map $\bullet : \mathrm{Sh}(X)^+ \otimes \mathrm{Sh}(X) \to \mathrm{Sh}(X)^+$) are described in terms of the basis $\nu(\widehat{\mathcal{F}}^*)$. The same need will arise if the recursions (9) or (14) are applied to compute the coproduct in $\mathrm{Sh}(X)$. This task will be accomplished in the remaining of the present work. In addition, alternative proofs of Theorem 3 and Corollary 1 will be obtained from scratch, without assuming the results in [17].

ss:tech

4.4 Technical results on Hall rooted trees and forests

d:k(v,u) **Definition 6** *Given arbitrary $u, v \in \mathcal{F}$ and $t \in \mathcal{T}$, we define $r(t,u), k(u,v) \in \mathbb{Z}$ as follows. If the forests u and v have no common labelled rooted tree, then $k(v,u) = 1$, and if $t \in \mathcal{T}$ is not a factor of the forest uv then $k(vt^i, ut^j) = (i+j)!/(i!j!)k(v,u)$ for each $i, j \geq 1$. If $t = B_d(v)$, then $r(u,t) = k(u,v)$.*

The following result directly follows from Lemma 1 and Definition 6.

l:r(t,u) **Lemma 3** *Given arbitrary $u, v \in \mathcal{F}$ and $t \in \mathcal{T}$,*

$$\sigma(t \circ u) = r(u,t)\sigma(u)\sigma(t), \quad \sigma(vu) = k(v,u)\sigma(v)\sigma(u).$$

d:chi **Definition 7** *We define the $\mathbb{K}$-linear map $\chi : \mathcal{H}_R^+ \to \mathcal{M}_R$ such that, for each $u \in \mathcal{F}$,*

$$\chi(u) = \sum_{tv=u} r(v,t)\, t \circ v, \tag{25}$$ eq:chi

where the summation is over all pairs $t \in \widehat{\mathcal{T}}$, $v \in \widehat{\mathcal{F}} \backslash \{e\}$ such that $tv = u$, and $r(v,t)$ is the positive integer given in Definition 6.

l:xiSigma **Lemma 4** *Consider the graded $\mathbb{K}$-module maps $\xi, \chi : \mathcal{H}_R^+ \to \mathcal{M}_R$, given by (18) and Definition 7, and the graded $\mathbb{K}$-module map $\Sigma : \mathcal{H}_R^+ \to \mathcal{H}_R^+$ given by $\Sigma(u) = \sigma(u)u$ for each $u \in \mathcal{F}$. Then it holds that $\chi\Sigma = \Sigma\xi$.*

Proof: For each $u \in \mathcal{H}_R^+$, $\xi(u)$ can be rewritten as

$$\xi(u) = \sum_{tv=u} k(v,t)\, t \circ v.$$

The required result then follows from the identity $r(v,t)\sigma(vt) = k(v,t)\sigma(t \circ v)$ given by Lemma 3. $\square$

Hereafter, $\widehat{\mathcal{T}}$ will denote a given Hall set of rooted trees labelled by D, and $\widehat{\mathcal{F}}$ will be the corresponding set of Hall forests. Let us denote $\widehat{\mathcal{H}}_R = \mathbb{K}[\widehat{\mathcal{T}}]$. As a graded connected $\mathbb{K}$-module, its augmentation ideal $\widehat{\mathcal{H}}_R^+$ is free over the set $\widehat{\mathcal{F}} \backslash \{e\}$ of non-empty Hall forests. We also denote, $\widetilde{\mathcal{T}} := \bigcup_{d \in D} B_d(\widehat{\mathcal{F}})$, so that the graded $\mathbb{K}$-module $B(X \otimes \widehat{\mathcal{H}}_R)$ is free over $\widetilde{\mathcal{T}}$. For each $t \in \widetilde{\mathcal{T}}$ of degree $|t| > 1$, we consider, the standard decomposition $(t', t'') \in \widetilde{\mathcal{T}} \times \widehat{\mathcal{T}}$.

A key property of Hall sets of rooted trees is the existence of a suitable bijection of the set of non-empty Hall forests and the set $\widetilde{\mathcal{T}}$, which provides and isomorphism of graded $\mathbb{K}$-modules of $\widehat{\mathcal{H}}_R^+$ and $B(X \otimes \widehat{\mathcal{H}}_R)$.

Definition 8 *We define the* $\mathbb{K}$*-linear map* $\Gamma : \widehat{\mathcal{H}}_R^+ \to B(X \otimes \widehat{\mathcal{H}}_R)$ *given as follows. Given* $t \in \widehat{\mathcal{T}}$*,* $u \in \widehat{\mathcal{F}}$*, such that* $\max(tu) = t$*, then we set* $\Gamma(tu) = t \circ u$ *(in particular,* $(t) = t$*).*

l:Gamma **Lemma 5** *The map* Γ *is an isomorphism of graded* $\mathbb{K}$*-modules that maps* $\widehat{\mathcal{F}} \backslash \{e\}$ *onto* $\widetilde{\mathcal{T}}$*. Given* $t \in \widetilde{\mathcal{T}}$*, let* (t', t'') *be its standard decomposition. For each* $t \in \widetilde{\mathcal{T}}$*, it holds that* $\Gamma^{-1}(t) = t$ *if* $t \in \widehat{\mathcal{T}}$ *and* $\Gamma^{-1}(t) = t''\Gamma^{-1}(t')$ *otherwise.*

Proof: Let us now consider arbitrary $z, s \in \widehat{\mathcal{T}}$, $v \in \widehat{\mathcal{F}}$. Let $t = z \circ (sv) \in \widetilde{\mathcal{T}}$, and let (t', t'') be the standard decomposition of t. We have that

$$\min(sv) = s, \ z \geq \max(vs) \quad \Longleftrightarrow \quad t' = z \circ v, \ t'' = s, \text{ and } z = \max(zv).$$

Or equivalently,

$$\min(sv) = s, \ t = z \circ (vs) = \Gamma(svz) \quad \Longleftrightarrow \quad t' = z \circ v = \Gamma(vz), \ t'' = s. \tag{26}$$ eq:lGammalag

We will show by induction on $|t|$ that, for each $t \in \widetilde{\mathcal{T}}$, there exist unique $z \in \widehat{\mathcal{T}}$, $u \in \widehat{\mathcal{F}}$ such that $t = z \circ u = \Gamma(uz)$. This trivially holds if $t \in \widehat{\mathcal{T}}$, and in particular if $|t| = 1$. If $t \notin \widehat{\mathcal{T}}$, then we have by induction hypothesis that there exist unique $z \in \widehat{\mathcal{T}}$, $v \in \widehat{\mathcal{F}}$ such that $t' = z \circ v = \Gamma(vz)$, and the required statement follows from (26). Furthermore, (26) implies that, if $t \notin \widehat{\mathcal{T}}$, then $\Gamma^{-1}(t) = svz = t''\Gamma^{-1}(t')$. □

d:S_u **Definition 9** *For each* $u, v \in \widehat{\mathcal{F}} \backslash \{e\}$ *such that*

$$v = \Gamma^{-1}(t \circ w) \neq wt = u, \ \textit{for some } w \in \widehat{\mathcal{F}} \backslash \{e\}, \ t \in \widehat{\mathcal{T}}, \tag{27}$$ eq:dS_u

we denote $\lambda(u, v) = -r(w, t)$*, where the positive integer* $r(w, t)$ *is given in Definition 6. We define, for each* $u \in \widehat{\mathcal{F}} \backslash \{e\}$*, the set* $S_u \subset \widehat{\mathcal{F}}$ *of Hall forests* v *such that (27) holds. We also define* S_e *as the empty set.*

r:S_u **Remark 12** The $\mathbb{K}$-linear map Γ is by construction G-graded (in the sense of Remark 2). Hence, given $u, v \in \widehat{\mathcal{F}} \backslash \{e\}$, if $v \in S_u$, then $|u|_d = |v|_d$ for each $d \in D$. □

l:chi **Lemma 6** *For each* $u \in \widehat{\mathcal{F}} \backslash \{e\}$*,*

$$\chi(u) = \Gamma(u) - \sum_{v \in S_u} \lambda(u, v) \Gamma(v),$$

Proof: The required result is now a direct consequence of Definitions 7 and 9 once it is proven that $r(u, t) = 1$ if $\Gamma(tu) = t \circ u$. It then only remains to prove that, given $u \in \widehat{\mathcal{F}}$, $t \in \widehat{\mathcal{T}}$, if $t \geq \max(u)$ then $r(u, t) = 1$. In effect, let $d \in D$, $v \in \widehat{\mathcal{F}}$ be such that $t = B_d(v)$, so that $r(u, t) = k(u, v)$. We have that $\min(v) = t'' > t \geq \max(u)$, which implies that the forests u and v have no common labelled rooted tree, and thus $1 = k(u, v) = r(u, t)$. □

Remark 13 In particular, $\chi(t^k) = \Gamma(t^k) = t \circ t^{k-1}$ for each $t \in \widehat{\mathcal{T}}$, as S_{t^k} is the empty set. □

l:key **Lemma 7** *Given $u, v \in \widehat{\mathcal{F}} \backslash \{e\}$ such that $v \in S_u$, consider $t = \max(v)$, and tet (t', t'') be the standard decomposition of t. It holds that $\max(u) \geq t''$ and $\min(v) \geq \min(u)$.*

Proof: Under the assumptions of Lemma 7, there exist unique $s \in \widehat{\mathcal{T}}$, $w_1, w_2, w_3 \in \widehat{\mathcal{F}}$ such that

$$v = w_3 w_2 (s \circ w_1), \quad u = w_3 w_1 (s \circ w_2), \quad s \circ w_1 \geq \max(w_2 w_3), \quad w_1 w_2 \neq e, \tag{28}$$ eq:lkeylag

and w_1 and w_2 have no common factors. Let us first assume that $w_1 \neq e$ and $w_2 \neq e$. The inequality in (28) implies that $t = \max(v) = s \circ w_1$ and $\min(w_1) \geq t'' > t \geq \max(w_2 w_3)$. This, together with $s \circ w_2 < \min(w_2) \leq \max(w_2)$ implies that $\max(u) = \max(w_1) \geq \min(w_1) \geq t''$.

As for $\min(u) = \min(w_3 w_1 (s \circ w_2))$ we have that $\min(u) \leq \min(w_3 w_1 w_2) = \min(w_3 w_2) = \min(v)$.

ORAIN, FROGATU BEHAR DA $w_1 \neq e$.

ETA ZER PASATZEN DA $w_2 = e$ DENEAN? □

r:uvvu **Remark 14** Lemma 7 implies that $\max(u) > \max(v) \geq \min(v) \geq \min(u)$ provided that $v \in S_u$. In addition, it can be seen from its proof that under the assumptions of Lemma 7, $|\max(u)| < |\max(v)|$, and $|\max(u)|_d \leq |\max(v)|_d$, for each $d \in D$. □

d:>> **Definition 10** *Given $u, v \in \widehat{\mathcal{F}} \backslash \{e\}$, a path of length m from u to v is a finite sequence $W = (w_0, \ldots, w_m)$ such that $m \geq 0$, $w_0, \ldots, w_m \in \widehat{\mathcal{F}} \backslash \{e\}$, $w_0 = u$, $w_m = v$ and $w_{j+1} \in S_{w_j}$, $0 \leq j \leq m-1$. In such case, we write*

$$\lambda(W) = \prod_{j=0}^{m-1} \lambda(w_j, w_{j+1}).$$

We define a partial order $\succ$ in $\widehat{\mathcal{F}} \backslash \{e\}$ as follows. Given $u, v \in \widehat{\mathcal{F}} \backslash \{e\}$, we write $u \succ v$ if there exists some path from u to v. In such case, we denote $\lambda(u, v) = \sum_W \lambda(W)$ where the summation is over all paths from u to v. For each $u \in \widehat{\mathcal{F}} \backslash \{e\}$ we denote $\overline{S}_u = \{v \in \widehat{\mathcal{F}} \backslash \{e\} : \ u \succ v\}$.

r:bS_u **Remark 15** Lemma 7 implies that $\max(u) \geq \max(v)'' > \max(v) \geq \min(v) \geq \min(u)$ provided that $u \succ v$. Hence, $\succ$ is a well defined partial order on $\widehat{\mathcal{F}} \backslash \{e\}$. Moreover, according to Remark 12, if $u \succ v$, then $|u|_d = |v|_d$ for each $d \in D$. As the subsets of forests with same partial degrees are finite, the connected components of $\widehat{\mathcal{F}} \backslash \{e\}$ with respect to the partial order $\succ$ are finite (actually, with the partial order $\succ$, the connected components represent finite oriented graphs). In particular, $\overline{S}_u$ is finite for each $u \in \widehat{\mathcal{F}} \backslash \{e\}$. □

l:chiinv **Lemma 8** *The restriction* $\widehat{\chi} : \widehat{\mathcal{H}}_R^+ \to B(X \otimes \widehat{\mathcal{H}}_R)$ *to the map* χ *given in Definition 7 is an isomorphism of graded* $\mathbb{K}$*-modules. For each* $u \in \widehat{\mathcal{F}}$,

$$\widehat{\chi}^{-1}(\Gamma(u)) = u + \sum_{v \in \overline{S}_u} \lambda(u,v)v. \tag{29}$$ eq:chiinv

Proof: We first observe that, according to Remark 15, the summation in the right-hand side of (29) is finite. Let us consider the $\mathbb{K}$-linear map $\widehat{\chi}^- : B(X \otimes \widehat{\mathcal{H}}_R) \to \widehat{\mathcal{H}}_R^+$ such that $\chi^-(\Gamma(u))$ is for each $u \in \widehat{\mathcal{F}}$ the the right-hand side of (29). We first show that χ^- is a right inverse of χ. Application of Lemma 6 gives

$$\begin{aligned}\chi(\chi^-(u)) &= \Gamma(u) + \sum_{v \in \overline{S}_u} \lambda(u,v)\Gamma(v) \\ &\quad - \sum_{v \in S_u} \lambda(u,v)\Gamma(v) - \sum_{v \in S_u} \lambda(u,v) \sum_{w \in \overline{S}_v} \lambda(v,w)\Gamma(w),\end{aligned}$$

which by definition of S_u and $\lambda(u,v)$ coincides with $\Gamma(u)$. One similarly obtains that χ^- is the left inverse of χ. $\square$

Next result is a straightforward consequence of Lemma 8 and Lemma 4.

l:xiinv **Lemma 9** *If the base ring* $\mathbb{K}$ *is a* $\mathbb{Q}$*-algebra, then the restriction* $\widehat{\xi} : \widehat{\mathcal{H}}_R^+ \to B(\widehat{\mathcal{H}}_R \otimes X)$ *to the map* ξ *given in (18) is an isomorphism of graded* $\mathbb{K}$*-modules.*

4.5 Some results on basis for $\mathrm{Sh}(X)$ associated to Hall sets

s:Hallbasis

p:psi2 **Proposition 2** *Consider the graded* $\mathbb{K}$*-module isomorphism* $\psi : \widehat{\mathcal{H}}_R \to \mathrm{Sh}(X)$ *in Definition 5. For each* $u, v \in \mathcal{F}$, $t \in \mathcal{T}$ *it holds that*

$$\psi(u)\psi(v) = k(u,v)\psi(uv), \quad \psi(t) \bullet \psi(u) = r(u,t)\psi(t \circ u), \tag{30}$$ eq:psiuv

$$\psi(\chi(u)) = \psi(u) \quad \textit{for each} \quad u \in \widehat{\mathcal{F}}. \tag{31}$$ eq:nusigmaps

Proof: Equality (30) can be proven by induction in a similar way to Proposition 1. Also, it follows directly from Proposition 1 and Lemma 3 when the base ring is $\mathbb{K} = \mathbb{Z}$.

Given $t \in \widehat{\mathcal{T}}$, $k \geq 1$, as $r(t^{k-1}, t) = 1$, second equality in (30) implies that $\psi((t \circ t^{k-1})) = \psi(t) \bullet \psi(t^{k-1})$. If in addition, $v \in \widehat{\mathcal{F}}$, such that $k(v,t) = 1$, then

$$\psi(t) \bullet \psi(vt^{k-1}) = \psi(t) \bullet (\psi(v)\psi(t^{k-1})) = \psi(v) \bullet (\psi(t) \bullet \psi(t^{k-1})) = \psi(t^k) \bullet \psi(v). \tag{32}$$ eq:lagppsi2

Then, equality (31) trivially holds if $u = t^k$, as $\chi(t^k) = t \circ (t^{k-1})$. Otherwise, $u = t_1^{k_1} \cdots t_m^{k_m} \in \mathcal{F} \backslash \{e\}$, where $k_1, \ldots, k_m \geq 1$ and $t_1, \ldots, t_m \in \mathcal{T}$ are distinct, so that u can be factored, for each $i = 1, \ldots, m$, as $u = u_i t_i^{k_i}$, where $k(u_i, t_i^{k_i}) = 1$. By Definition 7 and equalities (30) and (32), we have that

$$\psi(\chi(u)) = \sum_{i=1}^m \psi(t_i) \bullet \psi(u_i t_i^{k_i - 1}) = \sum_{i=1}^m \psi(t_i^{k_i}) \bullet \psi(u_i),$$

and thus, $\psi(\chi(u)) = \psi(t_i^{k_i}) \bullet \psi(u_i) + \psi(\chi(u_i)) \bullet \psi(t_i^{k_i})$. The required result then follows (recall (13)), by induction on m. $\square$

Definition 5, Lemma 8, and Proposition 2 imply the following.

l:psi **Lemma 10** *Given $d \in D$, $w \in \widehat{\mathcal{F}}$, consider $u = \Gamma{-}1(B_d(w))$, then it holds that*

$$\begin{aligned} C_d(\psi(w)) &= \psi(\widehat{\chi}^{-1} B_d(w)) && (33) \\ &= \psi(u) + \sum_{v \in \overline{S}_u} \lambda(u,v)\psi(v). && (34) \end{aligned}$$

eq:C(psi(w))
eq:C(psi(w))

Remark 16 In particular, if $B_d(w) = t \in \widehat{\mathcal{T}}$, then $C_d(\psi(w)) = t$. More generally, if $B_d(w) = t \circ t^{k-1}$, where $t \in \widehat{\mathcal{T}}$ and $k \geq 1$, then $C_d(\psi(w)) = \psi(t^k)$. $\square$

t:psi **Theorem 4** *As a graded $\mathbb{K}$-module,* $\mathrm{Sh}(X)$ *is freely generated by the set*

$$\nu(\widehat{\mathcal{F}}^*) = \psi(\widehat{\mathcal{F}}) = \{\psi(u) : \ u \in \widehat{\mathcal{F}}\}.$$

Proof: We first observe that (11) also holds with ν replaced by ψ, so that ψ is surjective. We next prove that $\psi(\widehat{\mathcal{F}})$ generates $\mathrm{Sh}(X)$ by showing that it generates the image $\mathrm{Im}\,\psi$. That is, each $\psi(u)$, $u \in \mathcal{F}\backslash\{e\}$, can be rewritten as a $\mathbb{K}$-linear combination of terms of the form $\psi(v)$, $v \in \widehat{\mathcal{F}}\backslash\{e\}$. And this can be proven by induction on the degree $|u|$ from Definition 5, first equality in (30), and Lemma 10.

It follows from Definition 5 that ψ is an homomorphism of G-graded $\mathbb{K}$-modules, and as $\psi(\widehat{\mathcal{F}})$ generates $\mathrm{Sh}(X)$, we have that, for each $g \in G$, the restriction $\psi^g : (\widehat{\mathcal{H}}_R)^g \to (\mathrm{Sh}(X))^g$ of ψ to each finely homogeneous component of $\widehat{\mathcal{H}}_R = \mathbb{K}\,\widehat{\mathcal{F}}$ is an epimorphism of $\mathbb{K}$-modules. As $(\widehat{\mathcal{H}}_R)^g$ and $(\mathrm{Sh}(X))^g$ are, for each $g \in G$, finitely generated free $\mathbb{K}$-modules, it is then enough to prove that their basis have the same number of elements. Finally, we consider $B^{-1}\Gamma : \widehat{\mathcal{H}}_R \otimes X \to \widehat{\mathcal{H}}_R^+$ and $C : \mathrm{Sh}(X) \otimes X \to \mathrm{Sh}(X)^+$, which are both of them isomorphisms of G-graded $\mathbb{K}$-modules. This implies that $(\widehat{\mathcal{H}}_R)^g$ and $(\mathrm{Sh}(X))^g$ have the same rank for each $g \in G$. $\square$

Remark 17 The algebra structure of $\mathrm{Sh}(X)$ described in terms of its basis $\nu(\widehat{\mathcal{F}}^*) = \psi(\widehat{\mathcal{F}})$ is given by first equality in (30), while the coalgebra structure of $\mathrm{Sh}(X)$ can determined from (9), by applying Lemma 10 to describe each $C_d : \mathrm{Sh}(X) \to \mathrm{Sh}(X)^+$ in terms of the basis $\psi(\widehat{\mathcal{F}})$. Alternatively, a description of the coalgebra structure of $\mathrm{Sh}(X)$ in the basis $\psi(\widehat{\mathcal{F}})$ can be derived from the coalgebra structure of $\mathcal{H}_R$ by applying Lemma 10 to rewrite each $\nu(u)$, $u \in \mathcal{F}$ in such basis. $\square$

Hereafter, we denote as $\mathbb{K}_0$ the prime ring of $\mathbb{K}$, that is, either $\mathbb{K}_0 = \mathbb{Z}$ or $\mathbb{K}_0 = \mathbb{Z}/(k)$, $k \geq 1$.

l:ucircv2 **Lemma 11** *Given $u, v \in \widehat{\mathcal{F}}$, $\psi(v) \bullet \psi(u)$ is a $\mathbb{K}_0$-linear combination of $\psi(uv)$ and terms of the form $\psi(w)$, where $w \in \widehat{\mathcal{F}}\backslash\{e\}$, $uv \succ w$.*

Proof: We first observe that, given $w \in \widehat{\mathcal{F}}\backslash\{e\}$, $t \in \widehat{\mathcal{T}}$ such that $v = wt$, then $\Gamma^{-1}(t \circ (uw))$ is a $\mathbb{K}_0$-linear combination of uv and Hall forests $w \in S_{uv}$. Then, (29) implies that $\widehat{\chi}^{-1}\Gamma^{-1}(t \circ (uw))$ is a $\mathbb{K}_0$-linear combination of $\psi(uv)$ and terms of the form $\psi(\bar{w})$, where $\bar{w} \in \widehat{\mathcal{F}}\backslash\{e\}$, $uv \succ \bar{w}$. Second equality in (31), Definition 7, and (30) finally implies that $\psi(v) \bullet \psi(u) = \psi(\chi(v)) \bullet \psi(u)$ is a $\mathbb{K}_0$-linear combination of terms of the form $\widehat{\chi}^{-1}\Gamma^{-1}(t \circ (uw))$ with $w \in \widehat{\mathcal{F}}\backslash\{e\}$, $t \in \widehat{\mathcal{T}}$, and $v = wt$. □

Now, Corollary 1 is a consequence of Theorem 4, Proposition 1, and the fact that ν is an algebra map. We thus have that, when $\mathbb{K}$ is a $\mathbb{Q}$-algebra, $\nu(\widehat{\mathcal{F}})$ is a basis of the underlying $\mathbb{K}$-module of $\mathrm{Sh}(X)$. Next result, which is of interest when using such a basis, follows from the identities $C_d \nu = \nu B_d$ ($d \in D$) and (12), Lemma 2, and Lemma 9.

p:C(nu(w)) **Proposition 3** *Under the conditions of Corollary 1,*

$$C_d(\nu(u)) = \nu(\widehat{\xi}^{-1} B_d(u)), \quad \nu(v) \bullet \nu(u) = \nu(\widehat{\xi}^{-1}(\widehat{\xi}(v) \circ u)), \tag{35}$$ eq:C(nu(w))

for each $d \in D$ and $u, v \in \widehat{\mathcal{F}}$,

4.6 The dual basis of $\psi(\widehat{\mathcal{F}})$

s:dualbasis

We next prove Theorem 3 in an alternative way to the proof of Theorem 5.3 in [17]. In [17], the bialgebra structure of $T(X)$ described in terms of the basis $\{E_u : u \in \widehat{\mathcal{F}}\}$ is used to prove Theorem 5.3, while our prove directly works with the bialgebra structure of $\mathrm{Sh}(X)$ described in the basis $\nu(\widehat{\mathcal{F}}^*) = \psi(\widehat{\mathcal{F}})$.

l:hdelta2 **Lemma 12** *For each $t \in \widehat{\mathcal{T}}$ such that $|t| > 1$, $\widehat{\Delta}\psi(t) - \psi(t) \otimes \widehat{e} - \widehat{e} \otimes \psi(t) - \psi(t'') \otimes \psi(t')$ is a $\mathbb{K}_0$-linear combination of terms of the form*

1. *$\psi(v) \otimes \psi(w)$ with $v, w \in \widehat{\mathcal{F}}\backslash\{e\}$, $v \notin \widehat{\mathcal{T}}$,*
2. *$\psi(s) \otimes \psi(w)$, where $s \in \widehat{\mathcal{T}}$, $w \in \widehat{\mathcal{F}}\backslash\{e\}$, $w \notin \widehat{\mathcal{T}}$, $s > \max(t''w)$,*
3. *$\psi(s) \otimes \psi(z)$, where $s, z \in \widehat{\mathcal{T}}$, $s > \max(t''z'')$.*

Proof: We will prove by induction on $|t|$ the required result for a slightly wider class of labelled rooted trees. Namely, for $t \in \widetilde{\mathcal{T}}$ such that $t' \in \widehat{\mathcal{T}}$ and $t' \leq t''$ (note that, if $t' < t''$, then $t \in \widehat{\mathcal{T}}$). Any such labelled rooted tree of degree greater than one can be decomposed as $t \circ z^k$ where $k \geq 1$, $z, t \in \widehat{\mathcal{T}}$, and

$$t \leq z < t'', \quad z'' > \min(z'z), \quad t'' > \min(t't). \tag{36}$$ eq:tzlag

Clearly, $(t \circ z^k)'' = z$ and $(t \circ z^k)' = t \circ z^{k-1}$. Let us denote, for each $t \in \widehat{\mathcal{T}}$, $R(t) := \widehat{\Delta}(t) - \psi(t) \otimes \widehat{e} - \widehat{e} \otimes \psi(t) - \psi(t'') \otimes \psi(t')$.

If $k = 1$, and $|t| = |z| = 1$, then (14) with $u = \psi(z)$, $v = \psi(t)$ implies that $R(t) = 0$.

If $k = 1$ and $|z| + |t| > 2$, then application of (14) with $u = \psi(z)$, $v = \psi(t)$,the induction hypothesis and the inequalities (36), imply that $R(t \circ z)$ is a $\mathbb{K}_0$-linear combination of terms either of the form 1. in statement of Lemma 12, or of the form $\psi(s) \otimes \psi(t) \bullet \psi(w)$ or $\psi(s) \otimes \psi(w) \bullet \psi(z)$ with $s \in \widehat{\mathcal{T}}$, $w \in \widehat{\mathcal{F}} \backslash \{e\}$, and $s > \max(zw)$. The required result now follows from Lemma 11 and Remark 12.

If $k \geq 2$, then as $\psi(z^k) = \psi(z \circ z^{k-1})$, $(z \circ z^{k-1})'' = z$, and $\psi(z \circ z^{k-1})'' = \psi(z \circ z^{k-2}) = \psi(z^{k-1})$, induction hypothesis implies that $\widehat{\Delta}\psi(z^k) - \psi(z^k) \otimes \widehat{e} - \widehat{e} \otimes \psi(z^k) - \psi(z) \otimes \psi(z^{k-1})$ is a $\mathbb{K}_0$-linear combination of terms either of the form 1. in statement of Lemma 12, or of the form $\psi(s) \otimes \psi(w)$ where $s \in \widehat{\mathcal{T}}$, $w \in \widehat{\mathcal{F}} \backslash \{e\}$, $s > \max(zw)$ (and $w'' < s$ if $w \in \widehat{\mathcal{T}}$). Then, application of (14) with $u = \psi(z^k)$ and $v = \psi(t)$, and the inequalities (36), imply that $R(t \circ z^k)$ is a $\mathbb{K}_0$-linear combination of terms either of the form 1. in statement of Lemma 12, or of the form $\psi(s) \otimes \psi(t) \bullet \psi(w)$ or $\psi(s) \otimes \psi(w) \bullet \psi(z^k)$ with $s \in \widehat{\mathcal{T}}$, $w \in \widehat{\mathcal{F}} \backslash \{e\}$, and $s > \max(zw)$. The required result finally follows, as in the case $k = 1$, from Lemma 11 and Remark 12. □

l:hdelta3 **Lemma 13** *Given $u \in \widehat{\mathcal{F}} \backslash \{e\}$, if $u \notin \widehat{\mathcal{T}}$, then*

$$\widehat{\Delta}\psi(u) - \psi(u) \otimes \widehat{e} - \widehat{e} \otimes \psi(u) - \sum_{zv=u} \psi(z) \otimes \psi(v)$$

(where the summation is over all $z \in \widehat{\mathcal{T}}$, $v \in \widehat{\mathcal{F}}$ such that $zv = u$) is a $\mathbb{K}_0$-linear combination of terms of the form $w_1 \otimes w_2$ with $w_1, w_2 \in \widehat{\mathcal{F}} \backslash \{e\}$, such that, if $w_1 = s \in \widehat{\mathcal{T}}$ then $w_2 \notin \widehat{\mathcal{T}}$, $s > \min(w_2)$ and $s > \min(u)$.

Proof: We have proven a stronger statement for the case where $u = z^k$, $z \in \widehat{\mathcal{T}}$, $k > 1$, in the proof of Lemma 12, and the general result follows, for $u = z_1^{k_1} \cdots z_m^{k_m}$, with $z_i \in \widehat{\mathcal{T}}$ distinct, from $\psi(z_1^{k_1} \cdots z_m^{k_m}) = \psi(z_1^{k_1}) \cdots \psi(z_m^{k_m})$ and the fact that $\widehat{\Delta}$ is an algebra map. □

Lemma 12 and Lemma 13 imply the following theorem, that states that the basis $\nu(\widehat{\mathcal{F}}^*) = \psi(\widehat{\mathcal{F}})$ of the underlying $\mathbb{K}$-module of $\mathrm{Sh}(X)$ is the dual basis of the Poincaré-Witt-Birkhoff basis of $T(X)$ corresponding to the Hall basis $\{E_t : \ t \in \widehat{\mathcal{T}}\}$ of $\mathcal{L}(D)$.

t:main **Theorem 5** *Let us assume that $\widehat{\mathcal{T}}$ is a Hall set of rooted trees labelled by D, and $\widehat{\mathcal{F}}$ is the corresponding set of Hall forests. Then, for each $u, w \in \widehat{\mathcal{F}}$, it holds that*

$$\langle E_u, \psi(w) \rangle = \begin{cases} 1 & \text{if} \quad u = w \\ 0 & \text{otherwise.} \end{cases} \tag{37}$$ eq:main

Proof: Induction on $|u|$. It trivially holds when $|u| = 1$. If $u \notin \widehat{\mathcal{T}}$, then, let $z \in \widehat{\mathcal{T}}$, $v \in \widehat{\mathcal{F}} \backslash \{e\}$ such that $u = zv$, $z \leq \min(v)$. Now, for each $w \in \widehat{\mathcal{F}}$, if

$$0 \neq \langle E_u, \psi(w) \rangle = \langle E_z \otimes E_v, \widehat{\Delta}\psi(w) \rangle$$

then, induction hypothesis, together with Lemma 12 if $v \in \widehat{\mathcal{T}}$, and with Lemma 13 if $v \notin \widehat{\mathcal{T}}$, implies the required result.

If $u = z \in \widehat{\mathcal{T}}$, then, for each $w \in \widehat{\mathcal{F}} \backslash \widehat{\mathcal{T}}$, induction hypothesis and Lemma 13 implies that

$$\langle E_z, \psi(w) \rangle = \langle E_{z''} \otimes E_{z'} - E_{z'} \otimes E_{z''}, \widehat{\Delta}\psi(w) \rangle = 0,$$

and given $w = t \in \widehat{\mathcal{T}}$, as $(z')'' \geq z'' > z'$, we arrive at the required result by induction hypothesis and Lemma 12. □

Remark 18 Theorem 5, together with Proposition 1 obviously implies Theorem 3. □

5 Concluding remarks

s:remarks

We have established an epimorphism ν of graded Hopf algebras from $\mathcal{H}_R(X)$ to $\mathrm{Sh}(X)$ and we have identified the graded Hopf ideal $\mathcal{I} = \ker \nu$, so that $\mathrm{Sh}(X)$ is isomorphic as a graded Hopf algebra to the quotient Hopf algebra $\mathcal{H}_R(X)/\mathcal{I}$. For each Hall set associated to the alphabet D, we have assigned a set of labelled rooted trees $\widehat{\mathcal{T}}^*$ and a set of labelled forests $\widehat{\mathcal{F}}^*$ ($\widehat{\mathcal{T}}^* \subset \widehat{\mathcal{F}}^*$) such that $\nu(\widehat{\mathcal{F}}^*)$ freely generates $\mathrm{Sh}(X)$ as a $\mathbb{K}$-module, and when the base ring is a $\mathbb{Q}$-algebra, $\nu(\widehat{\mathcal{T}}^*)$ freely generates $\mathrm{Sh}(X)$ as an algebra. Moreover, we have described the coalgebra structure in terms of the basis $\nu(\widehat{\mathcal{F}}^*)$. Finally, we have shown that the dual basis of $\nu(\widehat{\mathcal{F}}^*)$ is the Poincaré-Witt-Birkhoff basis of $T(X)$ corresponding to a Hall basis of the free Lie algebra $\mathcal{L}(D)$, a result that, using a different approach, is esentially available in [17]. We believe that our approach of working directly on the shuffle algebra $\mathrm{Sh}(X)$ by taking advantage of the isomorphism between $\mathcal{H}_R(X)/\mathcal{I}$ and $\mathrm{Sh}(X)$ complements previous results stated in terms of the tensor algebra $T(X)$. Our approach has also conections with some results from [12] (see Remark [12]).

In [16], we present some applications and practical extensions of our results. In particular, we present practical rewriting algorithms that can be useful when one wants to work in the Hopf algebra $\mathrm{Sh}(X)$ in terms of the basis $\nu(\widehat{\mathcal{F}}^*)$ associated to an arbitrary Hall set over D. Applications to Lie series, exponential of Lie series, and the CBH formula and some generalizations are also presented in [16].

References

Agrachev [1] A. A. Agrachev, R. V. Gamkrelidze, *Exponential representation of flows and chronological calculus*, Mathem. Sbornik 107, (1978) 467–532. English transl. in : Math. USSR Sbornik 35 (1979), 727-785.

Butcher [2] J. C. Butcher, *An algebraic theory of integration methods*, Mathematics of Computation, Vol.26, 117 (1972)

Brouder [3] C. Brouder, *Runge-Kutta methods and renormalization*, Euro. Phys. J. C 12 (2000) 512–534.

nesKreimer [4] A. Connes, D. Kreimer, Hopf algebras, renormalization, and non-commutative geometry, Commun. Math. Phys. 199, (1998) 203–242.

Dur [5] A. Dür, *Möbius Functions, Incidence Algebras and Power-Series Representations*, Lecture Notes in Mathematics, 1202, Springer-Verlag, Berlin/Heidelberg, 1986

Foissy [6] L. Foissy, *Les algèbres de Hopf des arbres enracinés decorés, I*, Bulletin des Sciences Mathématiques, 126, 3 (2002), pp 193–239.

smanLarson [7] R. Grossman and R. G. Larson, *Hopf-algebaic structure of families of trees*, J. Algebra 126 (1989), 184–210.

Kawski1 [8] M. Kawski, *Chronological algebras: Combinatorics and control* Itogi Nauki i Techniki, vol.68 (2000) 144-178.

kiSussmann [9] M. Kawski, H. Sussmann, *Noncommutative power series and formal Lie-algebraic techniques in nonlinear control theory*, In Operators, Systems and Linear Algebra: Three Decades of Algebraic Systems Theory, U. Helmke, D. Praetzel-Wolters, E. Zerz Eds., B. G. Teubner Stuttgart, (1997), 111-129

HLW [10] E. Hairer, C. Lubich, and G. Wanner, *Geometric Numerical Integration. Structure-Preserving Algorithms for Ordinary Differential Equations*, Springer, Berlin, 2002.

Loday1 [11] J.-L. Loday, *Cup-product for Leibniz cohomology and dual Leibniz algebras*, Math Scand. (1995), 189–196

Loday2 [12] J.-L. Loday, *Dialgebras*, in “Dialgebras and related operads”, Springer Lecture Notes in Math. 1763 (2001), 7–66

McLQ [13] R.I. McLachlan and G.R.W. Quispel, *Splitting Methods*, Acta Numerica, 11 (2002), 341–434.

Reutenauer [14] G. Melançon and C. Reutenauer, *Lyndon words, free algebras and shuffles*, Canadian Journal of Mathematics, 41 (1989) 577-91.

MSS [15] A. Murua and J. M. Sanz-Serna, Order conditions for numerical integrators obtained by composing simpler integrators, *Philosophical Trans. Royal Soc.* A 357 (1999), 1079–1100.

shartlog [16] A. Murua, *The Hopf algebra of rooted trees, free Lie algebras, and Lie series*, (2003). Submitted.

Reutenauer [17] C. Reutenauer, *Free Lie Algebras*, London Math. Soc. monographs, new series 7, Oxford, 1993.

Rocha [18] E. Rocha, *On computation of the logarithm of the Chen-Fliess series for nonlinear systems*, Nonlinear and adaptive control (2001), 317-326

Schu [19] M. P. Schützenberger, *Sur une propiété combinatoire des algèbres de Lie libres pouvant être utilisée dans un problème de mathématiques appliquées*, Séminaire P. Dubreil. Faculté des Sciences, Paris (1958).

Sweedler [20] M. Sweedler, *Hopf Algebras*, Benjamin, New York, 1969.