

Free generators and Hoffman's isomorphism for the two-parameter shuffle algebra

Leonard Schmitz¹, Nikolas Tapia²

submitted: January 19, 2024

¹ University of Greifswald
Domstraße 11
17489 Greifswald
Germany
E-Mail: leonard.schmitz@uni-greifswald.de

² Weierstrass Institute
Mohrenstr. 39
10117 Berlin
Germany
E-Mail: nikolasesteban.tapiamunoz@wias-berlin.de

No. 3087
Berlin 2024



2020 *Mathematics Subject Classification.* 16T05, 60L70.

Key words and phrases. Signatures for images, matrix compositions, Hopf algebras, Lyndon words, two-parameter shuffles and quasi-shuffles.

LS has been supported by the trilateral French-Japanese-German research project *Enhanced Data stream Analysis with the Signature Method (EDDA)* of the French National Research Agency (ANR), together with the Japan Science and Technology Agency (JST), and the Deutsche Forschungsgemeinschaft (DFG). NT is funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under Germany's Excellence Strategy – The Berlin Mathematics Research Center MATH+ (EXC-2046/1, project ID: 390685689). Many of the initial discussions took place during the '23 workshop *Structural Aspects of Signatures and Rough Paths* (as part of the project *Signatures for Images*) at the Center of Advanced Study (CAS) in Oslo, Norway. Furthermore, LS would like to thank the *Stochastic Algorithms and Nonparametric Statistics* research group at the WIAS Berlin for the invitation and hospitality from October '23 until March '24.

Edited by
Weierstraß-Institut für Angewandte Analysis und Stochastik (WIAS)
Leibniz-Institut im Forschungsverbund Berlin e. V.
Mohrenstraße 39
10117 Berlin
Germany

Fax: +49 30 20372-303
E-Mail: preprint@wias-berlin.de
World Wide Web: <http://www.wias-berlin.de/>

Free generators and Hoffman’s isomorphism for the two-parameter shuffle algebra

Leonard Schmitz, Nikolas Tapia

Abstract

Signature transforms have recently been extended to data indexed by two and more parameters. With free Lyndon generators, ideas from \mathbf{B}_∞ -algebras and a novel two-parameter Hoffman exponential, we provide three classes of isomorphisms between the underlying two-parameter shuffle and quasi-shuffle algebras. In particular, we provide a Hopf algebraic connection to the (classical, one-parameter) shuffle algebra over the extended alphabet of connected matrix compositions.

Contents

1 Introduction	1
2 The matrix composition Hopf algebra	3
2.1 Two-parameter shuffles	3
2.2 Block shuffles	4
2.3 Two-parameter quasi-shuffles	5
3 Free Lyndon generators	5
3.1 Total order on connected compositions	5
3.2 Lyndon words	6
3.3 Isomorphisms due to Lyndon generators	8
4 Hoffman’s isomorphism for two parameters	10
4.1 Row and column action on matrix compositions	11
4.2 Multiplication	12
4.3 Invertibility	14
4.4 Comultiplication	15
5 Implicit isomorphisms of Hopf algebras	17
5.1 Leray’s theorem	18
5.2 Application: New proof of the two-parameter bialgebra relation	19
6 Conclusions and outlook	19

1 Introduction

The collection of iterated integrals of a path (termed *path signature*) has been used as a tool for classification in various settings since Chen’s seminal 1954 work [4]. In recent years—and in particular since pioneering work by Lyons and collaborators on the use of signatures as features for data streams in the early 2010s [12, 15]—there has been a surge

in the number of applications, which range from calibration of financial models [1] to motion recognition [3, 20] and deep learning [16]. We refer the interested reader to the surveys by Chevyrev and Kormilitzin [5], and Lyons and McLeod [17]. A discrete counterpart of the path signature has been introduced by one of the coauthors and collaborators [6, 7], and is likewise starting to see some applications [8].

Signature transforms, both continuous and discrete, have been extended to data indexed by two and more parameters by either following a topological approach [10], or an algebraic approach [9]. The algebraic picture in this setting becomes considerably more involved, and two-parameter analogues of the shuffle [10] and quasi-shuffle algebras [9] enter the frame.

It is a well-known fact that the set of Lyndon words provides an algebraic independent generating set of the (classical, one-parameter) shuffle and quasi-shuffle algebra, e.g. [19], [13, Thm. 2.6] or [11, Prop. 6.4.14]. The Hopf algebra structure from [9, Thm. 2.12] guarantees that the two-parameter quasi-shuffle algebra of matrix compositions is free. In this article, we address the following two questions posed in [9, Sec. 6]:

- 1 *Is there a free generating set akin to Lyndon words?*
- 2 *How are two-parameter shuffles and quasi-shuffles related to each other?*

We provide full answers to both questions: in Theorem 3.12 we construct an explicit family $(\mathcal{B}_w)_{w \in \mathcal{L}}$ of free generators indexed by Lyndon words, and in Theorem 4.1 we introduce a two-parameter version of Hoffman's isomorphism together with its explicit inverse, verifying that the two-parameter shuffle and quasi-shuffle are isomorphic products in the matrix composition Hopf algebra.

Note that $(\mathcal{B}_w)_{w \in \mathcal{L}}$ simultaneously generates not only the two-parameter shuffle and quasi-shuffle algebra, but even the (classical, one-parameter) shuffle algebra over the extended alphabet of connected matrix compositions. With this we relate the (classical, one-parameter) framework [13] to the recent two-parameter development [9, 10, 21]. Using ideas from the theory of \mathbf{B}_∞ -algebras, we can extend this connection even to the level of Hopf algebras.

In Section 5.2 we conclude with a fruitful application of our suggested machinery: a novel and transparent proof of the bialgebra relation with respect to diagonal deconcatenation and the two-parameter quasi-shuffle product, first stated in [9, Thm. 2.12]. In particular, we can drastically simplify its original proof.

Notation

Throughout, let \mathbb{Q} denote the rational number field, $\mathbb{N} = \{1, 2, \dots\}$ the strictly positive integers, and $\mathbb{N}_0 = \{0\} \cup \mathbb{N}$ the non-negative integers. For every matrix $\mathbf{a} \in M^{m \times n}$ with entries from an arbitrary set M , we denote by $\text{size}(\mathbf{a}) := (\text{rows}(\mathbf{a}), \text{cols}(\mathbf{a})) := (m, n) \in \mathbb{N}^2$ the number of its rows and columns, respectively.

Let \mathbb{K} be a commutative \mathbb{Q} -algebra and $(\mathfrak{M}_d, \star, \varepsilon)$ be the free commutative monoid generated by d letters $\{1, \dots, \mathbf{d}\}$. Here, \star denotes the multiplication and ε the neutral element with respect to the latter. From [9, Sec. 2] we recall the direct sum,

$$H := \bigoplus_{\mathbf{a} \in \text{Comp}} \mathbb{K}\mathbf{a}$$

of matrix compositions, i.e., matrices with entries in \mathfrak{M}_d which do not contain ε -rows or ε -columns. Additionally to those \mathfrak{M}_d -valued matrices, Comp contains the empty composition denoted by e . Recall from [9, Def. 2.1] that any two matrix compositions \mathbf{a} and \mathbf{b} can be concatenated along the diagonal, $\mathbf{c} = \text{diag}(\mathbf{a}, \mathbf{b})$. We denote by Comp_{con} the subset of connected compositions, i.e., all \mathbf{c} which have only trivial decompositions, that is $\mathbf{a} = e$ or $\mathbf{b} = e$.

Remark 1.1. *We can identify Comp with the Kleene star of connected compositions $\text{Comp}_{\text{con}}^*$. For this compare [9, Lem. 2.3] which defines a one-to-one correspondence by sending the composition $\text{diag}(\mathbf{u}_1, \dots, \mathbf{u}_\ell) \in \text{Comp}$ to the word $\mathbf{u}_1 \cdots \mathbf{u}_\ell \in \text{Comp}_{\text{con}}^*$. The empty composition e is identified with the empty word in $\text{Comp}_{\text{con}}^*$. This identification requires to select the explicit coproduct Δ dual to diagonal concatenation, i.e. [9, Def. 2.10]. Whenever we speak of such an identification, we implicitly make this choice and write $H = \mathbb{K}\langle \text{Comp}_{\text{con}} \rangle$.*

Let $\text{len}: \text{Comp}_{\text{con}}^* \rightarrow \mathbb{N}_0$ denote the **length** of monomials. With the identification from Remark 1.1 we have $\text{len}(e) = 0$ and $\text{len}(\mathbf{a}) := \ell$ for every nonempty $\mathbf{a} = \text{diag}(\mathbf{u}_1, \dots, \mathbf{u}_\ell)$ with $\mathbf{u} \in \text{Comp}_{\text{con}}^\ell$.

2 The matrix composition Hopf algebra

We begin with recalling the two-parameter shuffle from [10], presented here in the language of [9]. Note that we define the operation in the larger \mathbb{K} -module H , i.e., we use the extended alphabet Comp_{con} .

2.1 Two-parameter shuffles

For every $n \in \mathbb{N}$ let Σ_n denote the **permutations** of $\{1, \dots, n\}$. As in the classical setting, let $\text{sh}(m, s)$ with $m, s \in \mathbb{N}$ denote the subset of permutations $q \in \Sigma_{m+s}$ such that $q(1) < \dots < q(m)$ and $q(m+1) < \dots < q(m+s)$.

Definition 2.1. The **two-parameter shuffle product** is the bilinear mapping

$$\sqcup: H \times H \rightarrow H$$

determined on nonempty \mathbb{K} -basis elements $(\mathbf{a}, \mathbf{b}) \in \text{Comp} \times \text{Comp}$ via

$$\mathbf{a} \sqcup \mathbf{b} := \sum_{\substack{p \in \text{sh}(\text{rows}(\mathbf{a}), \text{rows}(\mathbf{b})) \\ q \in \text{sh}(\text{cols}(\mathbf{a}), \text{cols}(\mathbf{b}))}} \left(\text{diag}(\mathbf{a}, \mathbf{b})_{p^{-1}(u), q^{-1}(v)} \right)_{u,v}$$

and where $\mathbf{a} \sqcup \mathbf{e} := \mathbf{e} \sqcup \mathbf{a} := \mathbf{a}$ for all $\mathbf{a} \in \text{Comp}$.

Example 2.2.

$$\begin{aligned} [1] \sqcup [2] &= \begin{bmatrix} 1 & \varepsilon \\ \varepsilon & 2 \end{bmatrix} + \begin{bmatrix} \varepsilon & 1 \\ 2 & \varepsilon \end{bmatrix} + \begin{bmatrix} \varepsilon & 2 \\ 1 & \varepsilon \end{bmatrix} + \begin{bmatrix} 2 & \varepsilon \\ \varepsilon & 1 \end{bmatrix} \\ [1] \sqcup [2 \ 3] &= \begin{bmatrix} 1 & \varepsilon & \varepsilon \\ \varepsilon & 2 & 3 \end{bmatrix} + \begin{bmatrix} \varepsilon & 1 & \varepsilon \\ 2 & \varepsilon & 3 \end{bmatrix} + \begin{bmatrix} \varepsilon & \varepsilon & 1 \\ 2 & 3 & \varepsilon \end{bmatrix} \\ &\quad + \begin{bmatrix} \varepsilon & 2 & 3 \\ 1 & \varepsilon & \varepsilon \end{bmatrix} + \begin{bmatrix} 2 & \varepsilon & 3 \\ \varepsilon & 1 & \varepsilon \end{bmatrix} + \begin{bmatrix} 2 & 3 & \varepsilon \\ \varepsilon & \varepsilon & 1 \end{bmatrix} \end{aligned}$$

Theorem 2.3. (H, \sqcup, Δ) is a graded, connected, and commutative Hopf algebra.

Proof. An elementary way of proving this is similar to [9, Thm. 2.12]. Alternatively we can use the novel two-parameter version of Hoffman's isomorphism Φ developed in this article (Theorem 4.1), or an analogous proof presented in Section 5.2 via the one-parameter framework. \square

We can describe permutations in $\text{sh}(m, s) \subseteq \Sigma_{m+s}$ with a one-hot matrix encoding, similar to [9, Rem. 5.8] for quasi-shuffles. With this we can understand the two-parameter shuffle product via suitable matrix actions on the row and column space¹.

Remark 2.4. The following subset of permutation matrices

$$\text{SH}(m, s) := \left\{ [e_{l_1} \ \dots \ e_{l_m} \ e_{k_1} \ \dots \ e_{k_s}] \in \Sigma_{m+s} \mid l_p < l_{p+1}, k_q < k_{q+1} \right\}$$

is in one-to-one correspondence to $\text{sh}(m, s)$.

Example 2.5. For $p \in \text{sh}(2, 1)$ with $p(1) = 1, p(2) = 3$ and $p(3) = 2$,

$$\left(\begin{bmatrix} 1 & \varepsilon \\ 2 & \varepsilon \\ \varepsilon & 3 \end{bmatrix}_{p^{-1}(u), v} \right)_{u,v} = \begin{bmatrix} 1 & \varepsilon \\ \varepsilon & 3 \\ 2 & \varepsilon \end{bmatrix}_{u,v} = \left(\begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & \varepsilon \\ 2 & \varepsilon \\ \varepsilon & 3 \end{bmatrix} \right)_{u,v}.$$

Lemma 2.6. For all nonempty $\mathbf{a}, \mathbf{b} \in \text{Comp}$, we have

$$\mathbf{a} \sqcup \mathbf{b} = \sum_{\substack{\mathbf{P} \in \text{SH}(\text{rows}(\mathbf{a}), \text{rows}(\mathbf{b})) \\ \mathbf{Q} \in \text{SH}(\text{cols}(\mathbf{a}), \text{cols}(\mathbf{b}))}} \mathbf{P} \text{diag}(\mathbf{a}, \mathbf{b}) \mathbf{Q}^\top.$$

¹The matrix action on the row and column space in Comp is defined in [9, Sec. 5.2].

2.2 Block shuffles

Let (H, \sqcup, Δ) denote the classical Hopf algebra (H, \sqcup, Δ) over the extended alphabet Comp_{con} which shuffles the blocks (connected components with respect to Δ) of matrix compositions. A formal way of defining this block shuffle is provided in Definition 2.8.

Example 2.7.

$$\begin{aligned} [1] \sqcup [2] &= \begin{bmatrix} 1 & \varepsilon \\ \varepsilon & 2 \end{bmatrix} + \begin{bmatrix} 2 & \varepsilon \\ \varepsilon & 1 \end{bmatrix} \\ [1] \sqcup [2 \ 3] &= \begin{bmatrix} 1 & \varepsilon & \varepsilon \\ \varepsilon & 2 & 3 \end{bmatrix} + \begin{bmatrix} 2 & 3 & \varepsilon \\ \varepsilon & \varepsilon & 1 \end{bmatrix} \\ [1] \sqcup \begin{bmatrix} 2 & \varepsilon & \varepsilon \\ \varepsilon & 3 & 4 \end{bmatrix} &= \begin{bmatrix} 1 & \varepsilon & \varepsilon & \varepsilon \\ \varepsilon & 2 & \varepsilon & \varepsilon \\ \varepsilon & \varepsilon & 3 & 4 \end{bmatrix} + \begin{bmatrix} 2 & \varepsilon & \varepsilon & \varepsilon \\ \varepsilon & 1 & \varepsilon & \varepsilon \\ \varepsilon & \varepsilon & 3 & 4 \end{bmatrix} + \begin{bmatrix} 2 & \varepsilon & \varepsilon \\ \varepsilon & 3 & 4 & \varepsilon \\ \varepsilon & \varepsilon & \varepsilon & 1 \end{bmatrix} \end{aligned}$$

Definition 2.8. The **block shuffle product** is the bilinear mapping

$$\sqcup : H \times H \rightarrow H,$$

which satisfies the recursion

$$\text{diag}(\mathbf{a}, \mathbf{u}) \sqcup \text{diag}(\mathbf{b}, \mathbf{v}) = \text{diag}(\mathbf{a}, \mathbf{u} \sqcup \text{diag}(\mathbf{b}, \mathbf{v})) + \text{diag}(\mathbf{b}, \text{diag}(\mathbf{a}, \mathbf{u}) \sqcup \mathbf{v})$$

for $\mathbf{a}, \mathbf{b} \in \text{Comp}_{\text{con}}$ and $\mathbf{u}, \mathbf{v} \in \text{Comp}$, and such that the empty matrix composition e is the neutral element with respect to this product.

With this we obtain the (classical, one-parameter) shuffle algebra over the extended alphabet Comp_{con} .

Theorem 2.9. (H, \sqcup, Δ) is a graded, connected, and commutative Hopf algebra.

As in Lemma 2.6, we encode block shuffles via matrix notation. For this, we index elements due to Remark 2.4,

$$\text{SH}(a, b) = \left\{ \begin{bmatrix} \mathbf{e}_{\sigma^{-1}(1)}^T \\ \vdots \\ \mathbf{e}_{\sigma^{-1}(a+b)}^T \end{bmatrix} \mid \sigma \in \text{sh}(a, b) \right\}$$

via its rows. To encode block shuffles let \otimes be the Kronecker product of matrices and

$$\text{bSH}_\sigma(u, v) := \begin{bmatrix} \mathbf{e}_{\sigma^{-1}(1)}^T \otimes I_{u_1} \\ \vdots \\ \mathbf{e}_{\sigma^{-1}(a)}^T \otimes I_{u_a} \\ \mathbf{e}_{\sigma^{-1}(a+1)}^T \otimes I_{v_1} \\ \vdots \\ \mathbf{e}_{\sigma^{-1}(a+b)}^T \otimes I_{v_b} \end{bmatrix} \in \text{SH} \left(\sum_{1 \leq \alpha \leq a} u_\alpha, \sum_{1 \leq \beta \leq b} v_\beta \right)$$

be a **block shuffle action matrix** for every $\sigma \in \text{sh}(a, b)$ and block sizes $\mathbf{u} = (u_1, \dots, u_a)$ and $\mathbf{v} = (v_1, \dots, v_b)$.

Lemma 2.10. For $\mathbf{a} = \text{diag}(\mathbf{u}_1, \dots, \mathbf{u}_a)$ and $\mathbf{b} = \text{diag}(\mathbf{v}_1, \dots, \mathbf{v}_b)$ with decompositions into connected compositions \mathbf{u} and \mathbf{v} , we have

$$\mathbf{a} \sqcup \mathbf{b} = \sum_{\sigma \in \text{sh}(a, b)} \text{bSH}_\sigma(\text{rows}(\mathbf{u}), \text{rows}(\mathbf{v})) \text{diag}(\mathbf{a}, \mathbf{b}) \text{bSH}_\sigma(\text{cols}(\mathbf{u}), \text{cols}(\mathbf{v}))^T$$

where rows and cols is applied on the components of \mathbf{u} and \mathbf{v} , respectively.

We can write the two-parameter shuffle product (Definition 2.1) as a block shuffle (Definition 2.8) plus some lower order terms with respect to the length in Comp .

Lemma 2.11. For all $\mathbf{a}, \mathbf{b} \in \text{Comp}$,

$$\mathbf{a} \sqcup \mathbf{b} = \mathbf{a} \sqcup \mathbf{b} + \sum_{1 \leq i \leq \ell} \mathbf{c}_i$$

where $\mathbf{c}_i \in \text{Comp}$ with $\text{len}(\mathbf{c}_i) < \text{len}(\mathbf{a}) + \text{len}(\mathbf{b})$ for all $1 \leq i \leq \ell$.

Proof. Follows with Lemmas 2.6 and 2.10. □

2.3 Two-parameter quasi-shuffles

As in the classical setting, let $\text{qsh}(m, s; j)$ with $m, s, j \in \mathbb{N}$ denote the set of surjections

$$q : \{1, \dots, m+s\} \rightarrow \{1, \dots, j\}$$

such that $q(1) < \dots < q(m)$ and $q(m+1) < \dots < q(m+s)$. From [9, Def. 2.8] we recall the **two-parameter quasi-shuffle product**

$$\mathbf{a} \overset{\text{qs}}{\sqcup} \mathbf{b} = \sum_{j, k \in \mathbb{N}} \sum_{\substack{p \in \text{qsh}(m, s; j) \\ q \in \text{qsh}(n, t; k)}} \begin{bmatrix} \mathbf{c}_{1,1}^{p,q} & \dots & \mathbf{c}_{1,k}^{p,q} \\ \vdots & & \vdots \\ \mathbf{c}_{j,1}^{p,q} & \dots & \mathbf{c}_{j,k}^{p,q} \end{bmatrix} \quad (1)$$

where

$$\mathbf{c}_{x,y}^{p,q} = \star_{\substack{u \in p^{-1}(x) \\ v \in q^{-1}(y)}} \text{diag}(\mathbf{a}, \mathbf{b})_{u,v} \in \mathfrak{M}_d.$$

As discussed in [9, Rem. 5.8 and Lem. 5.11], we know that $\text{qsh}(m, s; j)$ is in one-to-one correspondence to

$$\text{QSH}(m, s; j) := \left\{ \begin{bmatrix} \mathbf{e}_{l_1} & \dots & \mathbf{e}_{l_m} & \mathbf{e}_{k_1} & \dots & \mathbf{e}_{k_s} \end{bmatrix} \in \mathbb{N}_0^{j \times (m+s)} \mid \begin{array}{l} l_1 < \dots < l_m \\ k_1 < \dots < k_s \\ \text{right invertible} \end{array} \right\}$$

and that Equation (1) translates to

$$\mathbf{a} \overset{\text{qs}}{\sqcup} \mathbf{b} = \sum_{j, k \in \mathbb{N}} \sum_{\substack{\mathbf{P} \in \text{QSH}(m, s; j) \\ \mathbf{Q} \in \text{QSH}(n, t; k)}} \mathbf{P} \text{diag}(\mathbf{a}, \mathbf{b}) \mathbf{Q}^\top.$$

From [9, Thm. 2.12] we know that $(H, \overset{\text{qs}}{\sqcup}, \Delta)$ is a graded, connected, and commutative Hopf algebra.

Similar as in Lemma 2.11 for two-parameter shuffles, we can write Equation (1) as a block shuffle plus some lower order terms with respect to the length in Comp .

Lemma 2.12. For all nonempty $\mathbf{a}, \mathbf{b} \in \text{Comp}$,

$$\mathbf{a} \overset{\text{qs}}{\sqcup} \mathbf{b} = \mathbf{a} \sqcup \mathbf{b} + \sum_{1 \leq i \leq \ell} \mathbf{c}_i$$

where $\mathbf{c}_i \in \text{Comp}$ with $\text{len}(\mathbf{c}_i) < \text{len}(\mathbf{a}) + \text{len}(\mathbf{b})$ for all $1 \leq i \leq \ell$.

3 Free Lyndon generators

3.1 Total order on connected compositions

We equip Comp_{con} with a total order, e.g. part 2. of Definition 3.1. Note that this explicit order is arbitrary, and can be exchanged by any other total order. For convenience, this explicit choice is fixed throughout this section, and illustrated in Example 3.2.

Definition 3.1.

- 1 Let $(\mathfrak{M}_d, >)$ be ordered degree-lexicographically with $1 < \dots < d$. For arbitrary $n \in \mathbb{N}$, extend this lexicographically to $(\mathfrak{M}_d^n, >)$ via

$$\mathbf{p} > \mathbf{q} := \begin{cases} \mathbf{p}_1 > \mathbf{q}_1 \text{ or} \\ \mathbf{p}_i = \mathbf{q}_i \text{ for all } i \leq j-1 \text{ and } \mathbf{p}_j > \mathbf{q}_j, \end{cases}$$

where $\mathbf{p}, \mathbf{q} \in \mathfrak{M}_d^n$.

- 2 For every $n \in \mathbb{N}$, let $(\mathfrak{M}_d^n, >)$ be ordered according to part 1. Using this, we equip $(\text{Comp}_{\text{con}}, >)$ with a strict total order via

$$\mathbf{a} > \mathbf{b} := \begin{cases} \text{rows}(\mathbf{a}) > \text{rows}(\mathbf{b}) \text{ or} \\ (\text{rows}(\mathbf{a}) = \text{rows}(\mathbf{b}) \text{ and } \text{cols}(\mathbf{a}) > \text{cols}(\mathbf{b})) \text{ or} \\ \text{size}(\mathbf{a}) = \text{size}(\mathbf{b}) \text{ and } \text{vec}(\mathbf{a}) > \text{vec}(\mathbf{b}), \end{cases}$$

where $\mathbf{a}, \mathbf{b} \in \text{Comp}_{\text{con}}$. Furthermore, let $\mathbf{a} > \mathbf{e}$ for every \mathbf{a} .

Example 3.2. For $>$ according to part 2. of Definition 3.1, we have for instance

$$[1] < [2] < [1 \star 2 \star 3] < [1 \ 2] < [2 \ 1] < \begin{bmatrix} 1 \\ 2 \end{bmatrix} < \begin{bmatrix} 2 \\ 1 \end{bmatrix} < \begin{bmatrix} 1 & \varepsilon \\ \varepsilon & 2 \end{bmatrix}.$$

Having a total order on Comp_{con} we can extend it to $\text{Comp}_{\text{con}}^*$. Note that we do not yet identify $\text{Comp}_{\text{con}}^*$ with Comp .

Definition 3.3. Let $(\text{Comp}_{\text{con}}, >)$ be totally ordered.

- 1 We recall the **lexicographic order** \leq_{lex} on $\text{Comp}_{\text{con}}^*$ via

$$u \leq_{\text{lex}} v := \begin{cases} \text{either } \exists i \leq \min\{\text{len}(u), \text{len}(v)\} : u_i < v_i \wedge u_j = v_j \ \forall j \leq i-1 \\ \text{or } \exists a \in \text{Comp}_{\text{con}}^* : v = ua. \end{cases}$$

- 2 Let the **graded lexicographic order** on $\text{Comp}_{\text{con}}^*$ be denoted by $<_{\text{grlex}}$, that is

$$u <_{\text{grlex}} v := \begin{cases} \text{len}(u) < \text{len}(v) \text{ or} \\ \text{len}(u) = \text{len}(v) \text{ and } u <_{\text{lex}} v. \end{cases}$$

The order $<_{\text{grlex}}$ in part 2. of Definition 3.3 is **len-compatible** by construction, i.e., elements are first ordered by its length, and afterwards lexicographically to break ties. Furthermore it is a **monomial order**, i.e.,

$$a <_{\text{grlex}} b \implies uav <_{\text{grlex}} ubv$$

for all $a, b, u, v \in \text{Comp}_{\text{con}}^*$.

Example 3.4. We continue with Example 3.2, i.e., we have a total order on Comp_{con} according to Definition 3.1. Let $<_{\text{grlex}}$ be due to Definition 3.3, e.g.,

$$[1] <_{\text{grlex}} [1 \star 2 \star 3] <_{\text{grlex}} \begin{bmatrix} 1 & \varepsilon \\ 3 & 2 \end{bmatrix} <_{\text{grlex}} [1][2] <_{\text{grlex}} [2][1] <_{\text{grlex}} \begin{bmatrix} 1 \\ 2 \end{bmatrix} [3][4].$$

While the order of Comp_{con} from Definition 3.1 was arbitrary, the way Definition 3.3 extends it to $\text{Comp}_{\text{con}}^*$ is crucial for the following section.

3.2 Lyndon words

A word $w \in \text{Comp}_{\text{con}}^*$ is a **Lyndon word**, if and only if it is nonempty and lexicographically strictly smaller than any of its proper suffixes, that is $w <_{\text{lex}} v$ for all nonempty words $v \in \text{Comp}_{\text{con}}^*$ such that $w = uv$ and $u \in \text{Comp}_{\text{con}}^*$ is nonempty. Let $\mathfrak{L} = \mathfrak{L}(\text{Comp}_{\text{con}}, <_{\text{lex}})$ be the set of Lyndon words over the alphabet Comp_{con} . We define a family $(\mathcal{B}_w)_{w \in \mathfrak{L}}$ of compositions via

$$\mathcal{B}_w := \text{diag}(\mathbf{w}_1, \dots, \mathbf{w}_{\text{len}(w)}) \quad (2)$$

for every $w = \mathbf{w}_1 \dots \mathbf{w}_{\text{len}(w)} \in \mathfrak{L}$.

Example 3.5. In the setting of Example 3.4, we have for instance

$$[1], [2], [1][2], [3] \begin{bmatrix} 1 \\ 2 \end{bmatrix}, [1 \ 2] \begin{bmatrix} 1 \\ 2 \end{bmatrix} \in \mathfrak{L},$$

and as non-examples,

$$[2][1], \begin{bmatrix} 1 \\ 2 \end{bmatrix} [3], \begin{bmatrix} 1 \\ 2 \end{bmatrix} [1 \ 2], \begin{bmatrix} 1 \\ 2 \end{bmatrix} [3][4] \notin \mathfrak{L}.$$

In Theorem 3.12 we show that $(\mathcal{B}_w)_{w \in \mathfrak{L}}$ is a family of free generators for the block shuffle algebra, as well as for two-parameter shuffle algebra, and for the two-parameter quasi-shuffle algebra. Definition 3.6 treats these three products from above in parallel, and requires the so-called CFL factorization of words.

For nonempty $u \in \text{Comp}_{\text{con}}^*$ let (a_1, \dots, a_p) be its **Chen-Fox-Lyndon (CFL) factorization**, i.e., we have $u = a_1 \dots a_p$ and $a_1 \geq_{\text{lex}} \dots \geq_{\text{lex}} a_p$ for $a_i \in \mathfrak{L}$ with $1 \leq i \leq p$. This factorization always exists and it is unique, see e.g. [11, Thm. 6.1.27].

Definition 3.6. Let $(H, m, +)$ be a commutative \mathbb{K} -algebra. For every nonempty word $u \in \text{Comp}_{\text{con}}^*$ we define

$$\mathcal{B}_u^m := m(\mathcal{B}_{a_1}, \dots, \mathcal{B}_{a_p}) \in H$$

where (a_1, \dots, a_p) is the CFL factorization of u , and \mathcal{B}_{a_i} is according to Equation (2). If u is empty, we define $\mathcal{B}_u^m := e$.

Note that for every Lyndon word $w \in \mathfrak{L}$ the identification in Remark 1.1 and \mathcal{B}_w from eq. (2) provide the same element in H . Otherwise, if $u = \mathbf{u}_1 \dots \mathbf{u}_{\text{len}(u)} \notin \mathfrak{L}$ is nonempty with $\mathbf{u}_i \in \text{Comp}_{\text{con}}$ for $1 \leq i \leq \text{len}(u)$, then Definition 3.6 yields \mathcal{B}_u^m , which is distinct from $\text{diag}(\mathbf{u}_1, \dots, \mathbf{u}_{\text{len}(u)})$.

Example 3.7. We continue with the framework of Example 3.5.

1 For Lyndon word $w = [3] \begin{bmatrix} 1 \\ 2 \end{bmatrix} \in \mathfrak{L}$ we have

$$\mathcal{B}_w^m = \mathcal{B}_w = \begin{bmatrix} 3 & \varepsilon \\ \varepsilon & 1 \\ \varepsilon & 2 \end{bmatrix}$$

regardless of the product m in H .

2 For $u = \begin{bmatrix} 1 \\ 2 \end{bmatrix} [3] \in \text{Comp}_{\text{con}}^*$ we have $a = (a_1, a_2) = (\begin{bmatrix} 1 \\ 2 \end{bmatrix}, [3]) \in \mathfrak{L}^2$.

In the algebras $(H, \sqcup, +)$ and $(H, \sqcup, +)$ we have

$$\mathcal{B}_u^{\sqcup} = \mathcal{B}_{a_1} \sqcup \mathcal{B}_{a_2} = \begin{bmatrix} 1 \\ 2 \end{bmatrix} \sqcup [3] \quad \text{and} \quad \mathcal{B}_u^{\sqcup} = \mathcal{B}_{a_1} \sqcup \mathcal{B}_{a_2} = \begin{bmatrix} 1 \\ 2 \end{bmatrix} \sqcup [3].$$

From now on, we identify $\text{Comp}_{\text{con}}^*$ with Comp as discussed in Remark 1.1. Then, $<_{\text{grlex}}$ extends to the graded lexicographic order in $H = \mathbb{K}\langle \text{Comp}_{\text{con}} \rangle$. Let $\text{Im} : H \setminus \{0\} \rightarrow \text{Comp}$ denote the **leading monomial** with respect to $<_{\text{grlex}}$.

Corollary 3.8. For every $a, b \in H \setminus \{0\}$, we have

$$\text{Im}(a \sqcup b) = \text{Im}(a \sqcup b) = \text{Im}(a \overset{\text{qs}}{\sqcup} b).$$

Proof. This is an immediate consequence of Lemmas 2.11 and 2.12. □

For nonempty $\mathbf{a} \in \text{Comp}$ let $\mathcal{B}_{\mathbf{a}}^m := \mathcal{B}_{\mathbf{u}_1 \dots \mathbf{u}_{\text{len}(\mathbf{a})}}^m$ be according to Definition 3.6, and where \mathbf{u} is the decomposition of \mathbf{a} into connected compositions. Furthermore, let $\mathcal{B}_{\mathbf{e}}^m := e$.

Lemma 3.9. In the three \mathbb{K} -algebras $(H, m, +)$ with $m \in \{\sqcup, \sqcup, \overset{\text{qs}}{\sqcup}\}$ we have

$$\text{Im}(\mathcal{B}_{\mathbf{a}}^m) = \mathbf{a}$$

for every $\mathbf{a} \in \text{Comp}$.

Proof. Clearly $\text{Im}(\mathbf{e}) = \mathbf{e}$, hence we can assume that \mathbf{a} is nonempty. We use induction over the length of \mathbf{a} , i.e., we show

$$\text{Im}(\mathcal{B}_{\mathbf{u}_1 \dots \mathbf{u}_n}^m) = \text{diag}(\mathbf{u}_1, \dots, \mathbf{u}_n)$$

for every $n \in \mathbb{N}$ and $\mathbf{u}_i \in \text{Comp}_{\text{con}}$ with $1 \leq i \leq n$. The base case $n = 1$ is clear with $\text{Comp}_{\text{con}} \subseteq \mathcal{Q}$. For the induction step, let (a_1, \dots, a_p) be the CFL factorization of a word $\mathbf{u}_1 \dots \mathbf{u}_n$ with length n . The case $p = 1$ is clear again with $\text{Comp}_{\text{con}} \subseteq \mathcal{Q}$. Assuming $p > 1$, the CFL decompositions of $u := a_1$ and $v := a_2 \dots a_p$ are a_1 and (a_2, \dots, a_p) respectively. Clearly $u \in \mathcal{Q}$ hence $\mathcal{B}_u^m = \text{diag}(\mathbf{u}_1, \dots, \mathbf{u}_\ell)$ for a unique $\ell \in \mathbb{N}$. Furthermore $\text{len}(v) < n$, thus inductively

$$\text{Im}(\mathcal{B}_v^m) = \text{Im}(\mathcal{B}_{\mathbf{u}_{\ell+1} \dots \mathbf{u}_n}^m) = \text{diag}(\mathbf{u}_{\ell+1}, \dots, \mathbf{u}_n). \quad (3)$$

Now we have to distinguish between the underlying product m .

1 If $m = \sqcup$ then

$$\begin{aligned} \mathcal{B}_{\mathbf{u}_1 \dots \mathbf{u}_n}^{\sqcup} &= \mathcal{B}_{a_1}^{\sqcup} \sqcup \dots \sqcup \mathcal{B}_{a_p}^{\sqcup} = \mathcal{B}_u^{\sqcup} \sqcup \mathcal{B}_v^{\sqcup} \\ &= \text{diag}(\mathbf{u}_1, \dots, \mathbf{u}_\ell) \sqcup \text{diag}(\mathbf{u}_{\ell+1}, \dots, \mathbf{u}_n) \end{aligned}$$

thus with a basic fact [11, Thm. 6.2.2] about Lyndon words,

$$\begin{aligned} \text{Im}(\mathcal{B}_{\mathbf{u}_1 \dots \mathbf{u}_n}^{\sqcup}) &= \text{Im}(\text{diag}(\mathbf{u}_1, \dots, \mathbf{u}_\ell) \sqcup \text{diag}(\mathbf{u}_{\ell+1}, \dots, \mathbf{u}_n)) \\ &= \text{diag}(\mathbf{u}_1, \dots, \mathbf{u}_n). \end{aligned}$$

2 In the remaining cases $m \in \{\sqcup, \sqcup^{\text{qs}}\}$ we use $p - 1$ times Corollary 3.8, and also part 1., that is

$$\text{Im}(\mathcal{B}_{\mathbf{u}_1 \dots \mathbf{u}_n}^m) = \text{Im}(\mathcal{B}_{\mathbf{u}_1 \dots \mathbf{u}_n}^{\sqcup}) = \text{diag}(\mathbf{u}_1, \dots, \mathbf{u}_n).$$

□

Corollary 3.10. *Via the \mathbb{K} -algebras $(H, m, +)$ with $m \in \{\sqcup, \sqcup, \sqcup^{\text{qs}}\}$ we obtain three distinct \mathbb{K} -bases $(\mathcal{B}_{\mathbf{a}}^m)_{\mathbf{a} \in \text{Comp}}$ for the underlying \mathbb{K} -module $(H, +)$.*

Proof. We know that Comp is a \mathbb{K} -basis of H . Lemma 3.9 implies that $(\mathcal{B}_{\mathbf{a}}^m)_{\mathbf{a} \in \text{Comp}}$ expands invertibly triangularly with respect to Comp for every m so it is a \mathbb{K} -basis, too. □

We recall another fact about Lyndon words.

Lemma 3.11. *The family $(\mathcal{B}_w)_{w \in \mathcal{Q}}$ freely generates $(H, m, +)$ if and only if $(\mathcal{B}_{\mathbf{a}}^m)_{\mathbf{a} \in \text{Comp}}$ is a \mathbb{K} -basis of $(H, +)$.*

Proof. Consider for instance [11, Lem. 6.3.7]. □

Theorem 3.12. *The family $(\mathcal{B}_w)_{w \in \mathcal{Q}}$ freely generates the three \mathbb{K} -algebras $(H, \sqcup, +)$, $(H, \sqcup, +)$ and $(H, \sqcup^{\text{qs}}, +)$.*

Proof. Follows with Corollary 3.10 and Lemma 3.11. □

Tables 1 and 2 provide examples of non-trivial expressions in terms of their generators. One way of producing these is by using Corollary 3.10 and \langle_{griex} to subtract leading terms by \mathcal{B}_u^m when considered as monomials in \mathcal{B}_w for $w \in \mathcal{Q}$.

3.3 Isomorphisms due to Lyndon generators

Corollary 3.13. *We have $(H, \sqcup, +) \cong (H, \sqcup, +) \cong (H, \sqcup^{\text{qs}}, +)$ as \mathbb{K} -algebras.*

In Theorem 4.1 and corollary 5.6 we lift this statement even to the level of Hopf algebras. Note that the explicit mappings constructed in Corollary 3.13 are not compatible with Δ , and thus, they cannot be considered as isomorphisms of Hopf algebras.

Comp	$(H, \sqcup, +)$ in terms of its free generators $(\mathcal{B}_w)_{w \in \Omega}$
$\begin{bmatrix} 2 & \varepsilon \\ \varepsilon & 1 \end{bmatrix}$	$\begin{bmatrix} 1 \\ \varepsilon \end{bmatrix} \sqcup \begin{bmatrix} 2 \\ \varepsilon \end{bmatrix} - \begin{bmatrix} 1 & \varepsilon \\ \varepsilon & 2 \end{bmatrix}$
$\begin{bmatrix} 1 & \varepsilon \\ \varepsilon & 1 \end{bmatrix}$	$\frac{1}{2} \begin{bmatrix} 1 \\ \varepsilon \end{bmatrix} \sqcup \begin{bmatrix} 1 \\ \varepsilon \end{bmatrix}$
$\begin{bmatrix} 1 & 2 & \varepsilon \\ \varepsilon & \varepsilon & 3 \end{bmatrix}$	$\begin{bmatrix} 1 & 2 \\ \varepsilon & \varepsilon \end{bmatrix} \sqcup \begin{bmatrix} 3 \\ \varepsilon \end{bmatrix} - \begin{bmatrix} 3 & \varepsilon & \varepsilon \\ \varepsilon & 1 & 2 \end{bmatrix}$
$\begin{bmatrix} \varepsilon & 1 & \varepsilon \\ 1 & \varepsilon & \varepsilon \\ \varepsilon & \varepsilon & 1 \end{bmatrix}$	$\begin{bmatrix} \varepsilon & 1 \\ 1 & \varepsilon \end{bmatrix} \sqcup \begin{bmatrix} 1 \\ \varepsilon \end{bmatrix} - \begin{bmatrix} 1 & \varepsilon & \varepsilon \\ \varepsilon & \varepsilon & 1 \\ \varepsilon & 1 & \varepsilon \end{bmatrix}$
$\begin{bmatrix} 2 & \varepsilon & \varepsilon \\ \varepsilon & 3 & \varepsilon \\ \varepsilon & \varepsilon & 1 \end{bmatrix}$	$\begin{bmatrix} 2 & \varepsilon \\ \varepsilon & 3 \end{bmatrix} \sqcup \begin{bmatrix} 1 \\ \varepsilon \end{bmatrix} - \begin{bmatrix} 2 \\ \varepsilon \end{bmatrix} \sqcup \begin{bmatrix} 1 & \varepsilon \\ \varepsilon & 3 \end{bmatrix} + \begin{bmatrix} 1 & \varepsilon & \varepsilon \\ \varepsilon & 3 & \varepsilon \\ \varepsilon & \varepsilon & 2 \end{bmatrix}$
$\begin{bmatrix} 3 & \varepsilon & \varepsilon \\ \varepsilon & 1 & \varepsilon \\ \varepsilon & \varepsilon & 2 \end{bmatrix}$	$\begin{bmatrix} 3 \\ \varepsilon \end{bmatrix} \sqcup \begin{bmatrix} 1 & \varepsilon \\ \varepsilon & 2 \end{bmatrix} - \begin{bmatrix} 1 & \varepsilon & \varepsilon \\ \varepsilon & 2 & \varepsilon \\ \varepsilon & \varepsilon & 3 \end{bmatrix} - \begin{bmatrix} 1 & \varepsilon & \varepsilon \\ \varepsilon & 3 & \varepsilon \\ \varepsilon & \varepsilon & 2 \end{bmatrix}$
$\begin{bmatrix} 3 & \varepsilon & \varepsilon \\ \varepsilon & 2 & \varepsilon \\ \varepsilon & \varepsilon & 1 \end{bmatrix}$	$\begin{bmatrix} 1 \\ \varepsilon \end{bmatrix} \sqcup \begin{bmatrix} 2 \\ \varepsilon \end{bmatrix} \sqcup \begin{bmatrix} 3 \\ \varepsilon \end{bmatrix} - \begin{bmatrix} 2 & \varepsilon \\ \varepsilon & 3 \end{bmatrix} \sqcup \begin{bmatrix} 1 \\ \varepsilon \end{bmatrix} - \begin{bmatrix} 3 \\ \varepsilon \end{bmatrix} \sqcup \begin{bmatrix} 1 & \varepsilon \\ \varepsilon & 2 \end{bmatrix} + \begin{bmatrix} 1 & \varepsilon & \varepsilon \\ \varepsilon & 2 & \varepsilon \\ \varepsilon & \varepsilon & 3 \end{bmatrix}$
$\begin{bmatrix} 1 & \varepsilon & \varepsilon \\ \varepsilon & 2 & \varepsilon \\ \varepsilon & \varepsilon & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & \varepsilon \\ \varepsilon & 2 \end{bmatrix} \sqcup \begin{bmatrix} 1 \\ \varepsilon \end{bmatrix} - 2 \begin{bmatrix} 1 & \varepsilon & \varepsilon \\ \varepsilon & 1 & \varepsilon \\ \varepsilon & \varepsilon & 2 \end{bmatrix}$

Table 1: Block shuffles

Proof of Corollary 3.13. With the universal property of $(H, \sqcup, +)$, we obtain an isomorphism of algebras Ψ to $(H, \sqcup, +)$ by setting $\Psi(\mathcal{B}_w) := \mathcal{B}_w$ for every $w \in \Omega$. Its inverse is defined analogously via $\Psi^{-1}(\mathcal{B}_w) = \mathcal{B}_w$. The remaining isomorphisms are constructed in the same way. \square

In the following, we illustrate one of the isomorphisms from Corollary 3.13.

Example 3.14. Let Ψ be the \mathbb{K} -algebra isomorphism from $(H, \sqcup, +)$ to $(H, \sqcup, +)$. Lyndon generators are mapped to each other, e.g.

$$\Psi\left(\begin{bmatrix} 1 \\ \varepsilon \end{bmatrix}\right) = \begin{bmatrix} 1 \\ \varepsilon \end{bmatrix} \quad \text{or} \quad \Psi\left(\begin{bmatrix} 1 & \varepsilon \\ \varepsilon & 2 \end{bmatrix}\right) = \begin{bmatrix} 1 & \varepsilon \\ \varepsilon & 2 \end{bmatrix}.$$

Otherwise we write compositions in terms of their generators and apply Ψ such that it respects sums and products, e.g.,

$$\begin{aligned} \Psi\left(\begin{bmatrix} 2 & \varepsilon \\ \varepsilon & 1 \end{bmatrix}\right) &= \Psi\left(\begin{bmatrix} 1 \\ \varepsilon \end{bmatrix} \sqcup \begin{bmatrix} 2 \\ \varepsilon \end{bmatrix} - \begin{bmatrix} 1 & \varepsilon \\ \varepsilon & 2 \end{bmatrix}\right) = \Psi\left(\begin{bmatrix} 1 \\ \varepsilon \end{bmatrix}\right) \sqcup \Psi\left(\begin{bmatrix} 2 \\ \varepsilon \end{bmatrix}\right) - \Psi\left(\begin{bmatrix} 1 & \varepsilon \\ \varepsilon & 2 \end{bmatrix}\right) \\ &= \begin{bmatrix} 1 \\ \varepsilon \end{bmatrix} \sqcup \begin{bmatrix} 2 \\ \varepsilon \end{bmatrix} - \begin{bmatrix} 1 & \varepsilon \\ \varepsilon & 2 \end{bmatrix} = \begin{bmatrix} 2 & \varepsilon \\ \varepsilon & 1 \end{bmatrix} + \begin{bmatrix} \varepsilon & 2 \\ 1 & \varepsilon \end{bmatrix} + \begin{bmatrix} \varepsilon & 1 \\ 2 & \varepsilon \end{bmatrix} \end{aligned}$$

Comp	$(H, \sqcup, +)$ in terms of its free generators $(\mathcal{B}_w)_{w \in \mathcal{Q}}$
$\begin{bmatrix} 2 & \varepsilon \\ \varepsilon & 1 \end{bmatrix}$	$[1] \sqcup [2] - \begin{bmatrix} 1 & \varepsilon \\ \varepsilon & 2 \end{bmatrix} - \begin{bmatrix} \varepsilon & 1 \\ 2 & \varepsilon \end{bmatrix} - \begin{bmatrix} \varepsilon & 2 \\ 1 & \varepsilon \end{bmatrix}$
$\begin{bmatrix} 1 & \varepsilon \\ \varepsilon & 1 \end{bmatrix}$	$\frac{1}{2}[1] \sqcup [1] - \begin{bmatrix} \varepsilon & 1 \\ 1 & \varepsilon \end{bmatrix}$
$\begin{bmatrix} 1 & 2 & \varepsilon \\ \varepsilon & \varepsilon & 3 \end{bmatrix}$	$[1 \ 2] \sqcup [3] - \begin{bmatrix} 3 & \varepsilon & \varepsilon \\ \varepsilon & 1 & 2 \end{bmatrix} - \begin{bmatrix} 1 & \varepsilon & 2 \\ \varepsilon & 3 & \varepsilon \end{bmatrix} - \begin{bmatrix} \varepsilon & \varepsilon & 3 \\ 1 & 2 & \varepsilon \end{bmatrix} - \begin{bmatrix} \varepsilon & 3 & \varepsilon \\ 1 & \varepsilon & 2 \end{bmatrix} - \begin{bmatrix} \varepsilon & 1 & 2 \\ 3 & \varepsilon & \varepsilon \end{bmatrix}$
$\begin{bmatrix} \varepsilon & 1 & \varepsilon \\ 1 & \varepsilon & \varepsilon \\ \varepsilon & \varepsilon & 1 \end{bmatrix}$	$\begin{bmatrix} \varepsilon & 1 \\ 1 & \varepsilon \end{bmatrix} \sqcup [1] - \begin{bmatrix} 1 & \varepsilon & \varepsilon \\ \varepsilon & \varepsilon & 1 \\ \varepsilon & 1 & \varepsilon \end{bmatrix} - 2 \begin{bmatrix} \varepsilon & \varepsilon & 1 \\ 1 & \varepsilon & \varepsilon \\ \varepsilon & 1 & \varepsilon \end{bmatrix} - 2 \begin{bmatrix} \varepsilon & 1 & \varepsilon \\ \varepsilon & \varepsilon & 1 \\ 1 & \varepsilon & \varepsilon \end{bmatrix} - 3 \begin{bmatrix} \varepsilon & \varepsilon & 1 \\ \varepsilon & 1 & \varepsilon \\ 1 & \varepsilon & \varepsilon \end{bmatrix}$

Table 2: Two-parameter shuffles

or

$$\begin{aligned}
\Psi\left(\begin{bmatrix} 3 & \varepsilon & \varepsilon \\ \varepsilon & 1 & 2 \end{bmatrix}\right) &= \Psi\left(\begin{bmatrix} 1 & 2 \\ \varepsilon & \varepsilon \end{bmatrix} \sqcup [3] - \begin{bmatrix} 1 & 2 & \varepsilon \\ \varepsilon & \varepsilon & 3 \end{bmatrix}\right) \\
&= \Psi\left(\begin{bmatrix} 1 & 2 \\ \varepsilon & \varepsilon \end{bmatrix}\right) \sqcup \Psi\left([3]\right) - \Psi\left(\begin{bmatrix} 1 & 2 & \varepsilon \\ \varepsilon & \varepsilon & 3 \end{bmatrix}\right) \\
&= \begin{bmatrix} 1 & 2 \\ \varepsilon & \varepsilon \end{bmatrix} \sqcup [3] - \begin{bmatrix} 1 & 2 & \varepsilon \\ \varepsilon & \varepsilon & 3 \end{bmatrix} \\
&= \begin{bmatrix} 3 & \varepsilon & \varepsilon \\ \varepsilon & 1 & 2 \end{bmatrix} + \begin{bmatrix} 1 & \varepsilon & 2 \\ \varepsilon & 3 & \varepsilon \end{bmatrix} + \begin{bmatrix} \varepsilon & \varepsilon & 3 \\ 1 & 2 & \varepsilon \end{bmatrix} + \begin{bmatrix} \varepsilon & 3 & \varepsilon \\ 1 & \varepsilon & 2 \end{bmatrix} + \begin{bmatrix} \varepsilon & 1 & 2 \\ 3 & \varepsilon & \varepsilon \end{bmatrix}.
\end{aligned}$$

However, an isomorphism of Hopf algebras is not obtained with this construction, as illustrated in the following.

Example 3.15. We continue in the framework of Example 3.14, i.e., let Ψ be the \mathbb{K} -algebra isomorphism from $(H, \sqcup, +)$ to $(H, \sqcup, +)$. Then, with

$$[1], [2], [1][2], [1][1][2] \in \mathcal{Q},$$

and Equation (2), we have

$$\begin{aligned}
(\Psi \otimes \Psi) \circ \Delta\left(\begin{bmatrix} 1 & \varepsilon & \varepsilon \\ \varepsilon & 1 & \varepsilon \\ \varepsilon & \varepsilon & 2 \end{bmatrix}\right) \\
&= \begin{bmatrix} 1 & \varepsilon & \varepsilon \\ \varepsilon & 1 & \varepsilon \\ \varepsilon & \varepsilon & 2 \end{bmatrix} \otimes e + [1] \otimes \begin{bmatrix} 1 & \varepsilon \\ \varepsilon & 2 \end{bmatrix} + \Psi\left(\begin{bmatrix} 1 & \varepsilon \\ \varepsilon & 1 \end{bmatrix}\right) \otimes [2] + e \otimes \begin{bmatrix} 1 & \varepsilon & \varepsilon \\ \varepsilon & 1 & \varepsilon \\ \varepsilon & \varepsilon & 2 \end{bmatrix} \\
&\neq \Delta\left(\begin{bmatrix} 1 & \varepsilon & \varepsilon \\ \varepsilon & 1 & \varepsilon \\ \varepsilon & \varepsilon & 2 \end{bmatrix}\right) = \Delta \circ \Psi\left(\begin{bmatrix} 1 & \varepsilon & \varepsilon \\ \varepsilon & 1 & \varepsilon \\ \varepsilon & \varepsilon & 2 \end{bmatrix}\right),
\end{aligned}$$

since with Table 1,

$$\begin{aligned}
\Psi\left(\begin{bmatrix} 1 & \varepsilon \\ \varepsilon & 1 \end{bmatrix}\right) &= \Psi\left(\frac{1}{2}[1] \sqcup [1]\right) \\
&= \frac{1}{2}[1] \sqcup [1] = \begin{bmatrix} 1 & \varepsilon \\ \varepsilon & 1 \end{bmatrix} + \begin{bmatrix} \varepsilon & 1 \\ 1 & \varepsilon \end{bmatrix} \neq \begin{bmatrix} 1 & \varepsilon \\ \varepsilon & 1 \end{bmatrix}
\end{aligned}$$

so Ψ does not respect the coproduct Δ .

4 Hoffman's isomorphism for two parameters

In this section we introduce a novel two-parameter version of Hoffman's isomorphism (Definition 4.2) together with its explicit inverse (Lemma 4.11). With this we obtain the following main result.

Theorem 4.1. *The Hopf algebras (H, \sqcup, Δ) and $(H, \overset{\text{qs}}{\sqcup}, \Delta)$ are isomorphic.*

We prove this in this section. A sequence $I = (I_1, \dots, I_\ell) \in \mathbb{N}^\ell$ of positive integers is called a (classical, one-parameter) **composition** of $n \in \mathbb{N}_0$, if $I_1 + \dots + I_\ell = n$. Conventionally the empty composition is counted as the sole composition of 0. Denote the set of all compositions of n by $C(n)$.

For nonempty $\mathbf{a} \in \text{Comp}$, $I \in C(\text{rows}(\mathbf{a}))$ and $J \in C(\text{cols}(\mathbf{a}))$ let $\mathbf{a}_{I,J}$ denote the action of I and J on the rows and columns of \mathbf{a} , respectively. This action is formally provided in Definition 4.7. Let $\text{len}(I) = \ell$ denote the **length** and $I! = I_1! \dots I_{\text{len}(I)}!$ the **factorial** of $I \in \mathbb{N}^\ell$.

The following explicit mapping Φ is motivated by Hoffman's isomorphism [13, Thm. 2.5], and here generalized for two parameters.

Definition 4.2. Let Φ be the \mathbb{K} -linear mapping from (H, \sqcup, Δ) to $(H, \overset{\text{qs}}{\sqcup}, \Delta)$ which satisfies $\Phi(\mathbf{e}) := \mathbf{e}$ and

$$\Phi(\mathbf{a}) := \sum_{\substack{I \in C(\text{rows}(\mathbf{a})) \\ J \in C(\text{cols}(\mathbf{a}))}} \frac{1}{I!J!} \mathbf{a}_{I,J}$$

for every nonempty \mathbb{K} -basis element $\mathbf{a} \in \text{Comp}$.

Example 4.3.

$$\begin{aligned} \Phi\left(\begin{bmatrix} 1 \\ 2 \end{bmatrix}\right) &= \begin{bmatrix} 1 \\ 2 \end{bmatrix}, & \Phi\left(\begin{bmatrix} 1 \\ 2 \end{bmatrix}\right) &= \begin{bmatrix} 1 \\ 2 \end{bmatrix} + \frac{1}{2} [1 \star 2], \\ \Phi\left(\begin{bmatrix} 1 & \varepsilon \\ \varepsilon & 2 \end{bmatrix}\right) &= \begin{bmatrix} 1 & \varepsilon \\ \varepsilon & 2 \end{bmatrix} + \frac{1}{2} \begin{bmatrix} 1 \\ 2 \end{bmatrix} + \frac{1}{2} \begin{bmatrix} 1 & 2 \end{bmatrix} + \frac{1}{4} [1 \star 2], \\ \Phi\left(\begin{bmatrix} 1 & \varepsilon \\ \varepsilon & 2 \\ \varepsilon & 3 \end{bmatrix}\right) &= \begin{bmatrix} 1 & \varepsilon \\ \varepsilon & 2 \\ \varepsilon & 3 \end{bmatrix} + \frac{1}{2} \begin{bmatrix} 1 & 2 \\ \varepsilon & 3 \end{bmatrix} + \frac{1}{2} \begin{bmatrix} 1 & \varepsilon \\ \varepsilon & 2 \star 3 \end{bmatrix} + \frac{1}{2} \begin{bmatrix} 1 \\ 2 \\ 3 \end{bmatrix} \\ &\quad + \frac{1}{4} \begin{bmatrix} 1 \star 2 \\ 3 \end{bmatrix} + \frac{1}{4} \begin{bmatrix} 1 \\ 2 \star 3 \end{bmatrix} + \frac{1}{12} [1 \star 2 \star 3] \end{aligned}$$

We first show that Φ is multiplicative.

Lemma 4.4. *For all $\mathbf{a}, \mathbf{b} \in \text{Comp}$,*

$$\Phi(\mathbf{a} \sqcup \mathbf{b}) = \Phi(\mathbf{a}) \overset{\text{qs}}{\sqcup} \Phi(\mathbf{b}).$$

4.1 Row and column action on matrix compositions

In order to prove Lemma 4.4, we rewrite Definition 4.2 using matrix notation. For this, we introduce a one-hot matrix encoding of a (classical, one-parameter) composition.

Lemma 4.5. *For all $v, \ell \in \mathbb{N}$, the set*

$$\text{fuse}(v, \ell) := \left\{ \begin{bmatrix} e_{\iota_1} & \dots & e_{\iota_\ell} \end{bmatrix} \in \mathbb{N}_0^{v \times \ell} \mid \iota_1 \leq \dots \leq \iota_\ell \text{ and } \iota_j - \iota_{j-1} \leq 1 \right\}$$

is in one-to-one correspondence to the set $\{I \in C(\ell) \mid \text{len}(I) = v\}$ of compositions with length v .

Example 4.6. *The one-hot encodings of all $C(4)$ with length 2 are given by*

$$\text{fuse}(2, 4) = \left\{ \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \end{bmatrix} \right\}.$$

Proof of Lemma 4.5. For any $a \in \mathbb{N}$ let

$$a.e_j := \begin{bmatrix} e_j & \dots & e_j \end{bmatrix} \in \mathbb{N}_0^{v \times a}. \quad (4)$$

With this we obtain a bijective mapping via

$$\begin{bmatrix} I_1.e_1 & \dots & I_v.e_v \end{bmatrix} \in \text{fuse}(v, \ell)$$

for every $I \in C(\ell)$ with $\text{len}(I) = v$. □

Definition 4.7. For all nonempty $\mathbf{a} \in \text{Comp}$ and

$$(I, J) \in C(\text{rows}(\mathbf{a})) \times C(\text{cols}(\mathbf{a}))$$

let

$$(\mathbf{P}, \mathbf{Q}) \in \text{fuse}(\text{len}(I), \text{rows}(\mathbf{a})) \times \text{fuse}(\text{len}(J), \text{cols}(\mathbf{a}))$$

denote the corresponding one-hot encodings due to Lemma 4.5. Then, we set

$$\mathbf{a}_{I,J} := \mathbf{P}\mathbf{a}\mathbf{Q}$$

using the matrix action of \mathbf{P} and \mathbf{Q} on the rows and columns of \mathbf{a} , respectively. For \mathbf{P} let $\mathbf{P}! := I!$ denote the **factorial** of its corresponding composition I .

The one-hot encodings of compositions satisfy the following properties.

Lemma 4.8. For all $\ell = \ell_1 + \ell_2$ and $\nu = \nu_1 + \nu_2$ we have

$$\left\{ \text{diag}(\mathbf{U}, \mathbf{V}) \in \text{fuse}(\ell, \nu) \mid \begin{array}{l} \text{size}(\mathbf{U}) = (\ell_1, \nu_1) \\ \text{size}(\mathbf{V}) = (\ell_2, \nu_2) \end{array} \right\} = \text{diag}(\text{fuse}(\ell_1, \nu_1), \text{fuse}(\ell_2, \nu_2)),$$

where the operation diag is applied entrywise.

Lemma 4.9. If $\mathbf{V} = \text{diag}(\mathbf{V}_1, \mathbf{V}_2) \in \text{fuse}(\ell, \nu)$ with $\mathbf{V}_i \in \text{fuse}(\ell_i, \nu_i)$ for $i \in \{1, 2\}$, then $\mathbf{V}! = \mathbf{V}_1!\mathbf{V}_2!$.

Furthermore, all matrices in $\text{fuse}(\nu, \ell)$ are right invertible, and Definition 4.2 translates to

$$\Phi(\mathbf{a}) = \sum_{u, v \in \mathbb{N}} \sum_{\substack{\mathbf{U} \in \text{fuse}(u, \text{rows}(\mathbf{a})) \\ \mathbf{V} \in \text{fuse}(v, \text{cols}(\mathbf{a}))}} \frac{1}{\mathbf{U}!\mathbf{V}!} \mathbf{U}\mathbf{a}\mathbf{V}^T. \quad (5)$$

4.2 Multiplication

From the proof of [13, Thm. 2.5] we recall the following combinatorial (one-parameter) argument in the language of our one-hot matrix encodings. We apply this argument on both axes simultaneously, and thus show that Φ is multiplicative (Lemma 4.4).

Lemma 4.10. Let $a, b \in \mathbb{N}$ be fixed.

1 For all $u_1, u_2, j \in \mathbb{N}$, the mapping

$$\begin{aligned} M_{u_1, u_2, j} : \text{QSH}(u_1, u_2; j) \times \text{fuse}(u_1, a) \times \text{fuse}(u_2, b) &\rightarrow \mathbb{N}_0^{j \times (a+b)} \\ (\mathbf{A}, \mathbf{U}_1, \mathbf{U}_2) &\mapsto \mathbf{A} \text{diag}(\mathbf{U}_1, \mathbf{U}_2) \end{aligned}$$

is injective.

2 For all $j \in \mathbb{N}$ and $\mathbf{W} \in \text{Im}(N_j)$ with

$$\begin{aligned} N_j : \text{fuse}(j, a+b) \times \text{SH}(a, b) &\rightarrow \mathbb{N}_0^{j \times (a+b)} \\ (\mathbf{U}, \mathbf{P}) &\mapsto \mathbf{U}\mathbf{P} \end{aligned}$$

there is a unique \mathbf{U} such that $N_j(\mathbf{U}, \mathbf{P}) = \mathbf{W}$.

3 For all $j \in \mathbb{N}$,

$$\text{Im}(N_j) = \bigsqcup_{u_1, u_2} \text{Im}(M_{u_1, u_2, j}).$$

4 Each non-empty preimage $N_j^{-1}(\mathbf{U}\mathbf{P})$ has the cardinality

$$\#N_j^{-1}(\mathbf{U}\mathbf{P}) = \frac{\mathbf{U}!}{\mathbf{U}_1!\mathbf{U}_2!}$$

where $\mathbf{U}\mathbf{P} = \mathbf{A} \text{diag}(\mathbf{U}_1, \mathbf{U}_2)$ due to part 3.

Despite this being well-known, we provide a proof for completeness.

Proof of Lemma 4.10. The elements in $\text{Im}(M_{u_1, u_2, j})$ are given by actions on the columns in \mathbf{A} , that is

$$\begin{aligned} & \mathbf{A} \text{diag}(\mathbf{U}_1, \mathbf{U}_2) \\ &= \begin{bmatrix} e_{\iota_1} & \dots & e_{\iota_{u_1}} & e_{\kappa_1} & \dots & e_{\kappa_{u_2}} \end{bmatrix} \begin{bmatrix} I_1 \cdot e_1 & \dots & I_{u_1} \cdot e_{u_1} & 0 & \dots & 0 \\ 0 & \dots & 0 & J_1 \cdot e_1 & \dots & J_{u_2} \cdot e_{u_2} \end{bmatrix} \\ &= \begin{bmatrix} I_1 \cdot e_{\iota_1} & \dots & I_{u_1} \cdot e_{\iota_{u_1}} & J_1 \cdot e_{\kappa_1} & \dots & J_{u_2} \cdot e_{\kappa_{u_2}} \end{bmatrix} \end{aligned} \quad (6)$$

where $t \cdot e_j$ is according to eq. (4) for $t \in \mathbb{N}$. Whenever

$$\begin{aligned} & \begin{bmatrix} I_1 \cdot e_{\iota_1} & \dots & I_{u_1} \cdot e_{\iota_{u_1}} & J_1 \cdot e_{\kappa_1} & \dots & J_{u_2} \cdot e_{\kappa_{u_2}} \end{bmatrix} \\ &= \begin{bmatrix} I'_1 \cdot e_{\iota'_1} & \dots & I'_{u_1} \cdot e_{\iota'_{u_1}} & J'_1 \cdot e_{\kappa'_1} & \dots & J'_{u_2} \cdot e_{\kappa'_{u_2}} \end{bmatrix} \end{aligned}$$

then $I = I'$, $J = J'$, $\iota = \iota'$ and $\kappa = \kappa'$, i.e., part 1.

For part 2. let $\mathbf{UP} = \mathbf{U}'\mathbf{P}'$ with $\mathbf{U}, \mathbf{U}' \in \text{fuse}(j, a+b)$ and $\mathbf{P}, \mathbf{P}' \in \text{SH}(a, b)$. Then $\mathbf{U} = \mathbf{U}'\mathbf{P}'\mathbf{P}^{-1}$, and therefore $\mathbf{U} = \mathbf{U}'$ due to $\mathbf{P}'\mathbf{P}^{-1} \in \Sigma_{a+b}$.

For part 3. the elements $\mathbf{UP} \in \text{Im}(N_j)$ are given by \mathbf{U} , acting on the rows in

$$\mathbf{P} = \begin{bmatrix} e_{\sigma_1} & \dots & e_{\sigma_{a+b}} \end{bmatrix} = \begin{bmatrix} e_{\mu_1} & \dots & e_{\mu_a} & e_{\nu_1} & \dots & e_{\nu_b} \end{bmatrix}$$

with permutation $\sigma \in \Sigma_{a+b}$ and two strictly increasing and disjoint μ and ν . This determines unique $K \in C(j, a+b)$ and $m, n \in \mathbb{N}_0^j$ such that

$$\begin{aligned} \mathbf{UP} &= \begin{bmatrix} K_1 \cdot e_1 & \dots & K_j \cdot e_j \end{bmatrix} \begin{bmatrix} e_{\sigma_1} & \dots & e_{\sigma_{a+b}} \end{bmatrix} \\ &= \begin{bmatrix} m_1 \cdot e_1 & \dots & m_j \cdot e_j & n_1 \cdot e_1 & \dots & n_j \cdot e_j \end{bmatrix} \end{aligned} \quad (7)$$

with $0 \cdot e_i$ encoding an empty block whenever m_i or n_i is zero for $1 \leq i \leq j$. We obtain eq. (6) by viewing m and n as elements $I \in C(u_1, a)$ and $J \in C(u_2, b)$, i.e., by omitting all the $j - u_1$ zero entries in m , and the $j - u_2$ zero entries in n . This implies

$$\text{Im}(N_j) \subseteq \bigcup_{u_1, u_2} \text{Im}(M_{u_1, u_2, j}). \quad (8)$$

In eq. (6) we can count the number of non-zero rows u_1 and u_2 in the first a and remaining b columns, which implies that the union in eq. (8) is disjoint. In part 2. we showed already that the only freedom for eq. (7) comes from different choices of \mathbf{P} . In particular there are exactly

$$\frac{K_1! \dots K_j!}{m_1! \dots m_j! n_1! \dots n_j!} = \frac{K_1! \dots K_j!}{I_1! \dots I_{\text{len}(I)}! J_1! \dots J_{\text{len}(J)}!} = \frac{\mathbf{U}!}{\mathbf{U}_1! \mathbf{U}_2!}$$

choices of $\mathbf{P}' \in \text{SH}(a, b)$ such that $\mathbf{UP} = \mathbf{UP}'$ is satisfied. It remains to show equality in eq. (8). For this let

$$\mathbf{W} \in \bigoplus_{u_1, u_2} \text{Im}(M_{u_1, u_2, j}),$$

so there are unique u_1 and u_2 such that $\mathbf{W} \in \text{Im}(M_{u_1, u_2, j})$. With part 1. there is a unique

$$(\mathbf{A}, \mathbf{U}_1, \mathbf{U}_2) \in \text{QSH}(u_1, u_2; j) \times \text{fuse}(u_1, a) \times \text{fuse}(u_2, b)$$

such that $\mathbf{W} = \mathbf{A} \text{diag}(\mathbf{U}_1, \mathbf{U}_2)$. Let ι, κ, I and J as in eq. (6). Since \mathbf{A} is right invertible there exist disjoint $\tilde{\iota}_1 < \dots < \tilde{\iota}_a$ and $\tilde{\kappa}_1 < \dots < \tilde{\kappa}_b$ such that $\{\tilde{\iota}_1, \dots, \tilde{\iota}_a\} = \{\iota_1, \dots, \iota_{u_1}\}$, $\{\tilde{\kappa}_1, \dots, \tilde{\kappa}_b\} = \{\kappa_1, \dots, \kappa_{u_2}\}$ and

$$\{\tilde{\iota}_1, \dots, \tilde{\iota}_a\} \cup \{\tilde{\kappa}_1, \dots, \tilde{\kappa}_b\} = \{\iota_1, \dots, \iota_{u_1}\} \cup \{\kappa_1, \dots, \kappa_{u_2}\} = \{1, \dots, a+b\}.$$

This defines

$$\mathbf{P} := \begin{bmatrix} e_{\tilde{\iota}_1} & \dots & e_{\tilde{\iota}_a} & e_{\tilde{\kappa}_1} & \dots & e_{\tilde{\kappa}_b} \end{bmatrix} \in \text{SH}(a, b).$$

Choose now $\mathbf{U} \in \text{fuse}(j, a+b)$ such that $N_j(\mathbf{U}, \mathbf{P}) = \mathbf{UP} = \mathbf{W}$. \square

With this we verify that Φ is multiplicative.

Proof of Lemma 4.4. For all nonempty matrix compositions \mathbf{a} and \mathbf{b} ,

$$\begin{aligned}
\Phi(\mathbf{a} \sqcup \mathbf{b}) &= \sum_j \sum_k \sum_{\substack{\mathbf{U} \in \text{fuse}(j, \text{rows}(\text{diag}(\mathbf{a}, \mathbf{b}))) \\ \mathbf{V} \in \text{fuse}(k, \text{cols}(\text{diag}(\mathbf{a}, \mathbf{b}))) \\ \mathbf{P} \in \text{SH}(\text{rows}(\mathbf{a}), \text{rows}(\mathbf{b})) \\ \mathbf{Q} \in \text{SH}(\text{cols}(\mathbf{a}), \text{cols}(\mathbf{b}))}} \frac{1}{\mathbf{U}! \mathbf{V}!} \mathbf{UP} \text{diag}(\mathbf{a}, \mathbf{b}) \mathbf{Q}^T \mathbf{V}^T \\
&\stackrel{4.10.4}{=} \sum_j \sum_k \sum_{\substack{\mathbf{UP} \in \text{Im}(N_j) \\ \mathbf{VQ} \in \text{Im}(N_k)}} \frac{\#N_j^{-1}(\mathbf{UP}) \#N_k^{-1}(\mathbf{VQ})}{\mathbf{U}! \mathbf{V}!} \mathbf{UP} \text{diag}(\mathbf{a}, \mathbf{b}) \mathbf{Q}^T \mathbf{V}^T \\
&\stackrel{(9)}{=} \sum_j \sum_k \sum_{\substack{\mathbf{U}_1 \in \text{fuse}(u_1, \text{rows}(\mathbf{a})) \\ \mathbf{U}_2 \in \text{fuse}(u_2, \text{rows}(\mathbf{b})) \\ u_1 \mathbf{V}_1 \in \text{fuse}(v_1, \text{cols}(\mathbf{a})) \\ u_2 \mathbf{V}_2 \in \text{fuse}(v_2, \text{cols}(\mathbf{b})) \\ v_1 \mathbf{A} \in \text{QSH}(u_1, u_2; j) \\ v_2 \mathbf{B} \in \text{QSH}(v_1, v_2; k)}} \frac{1}{\mathbf{U}_1! \mathbf{U}_2! \mathbf{V}_1! \mathbf{V}_2!} \mathbf{A} \text{diag}(\mathbf{U}_1 \mathbf{a} \mathbf{V}_1^T, \mathbf{U}_2 \mathbf{b} \mathbf{V}_2^T) \mathbf{B}^T \\
&= \Phi(\mathbf{a}) \stackrel{\text{qs}}{\sqcup} \Phi(\mathbf{b}),
\end{aligned}$$

with summands

$$\begin{aligned}
\mathbf{UP} \text{diag}(\mathbf{a}, \mathbf{b}) \mathbf{Q}^T \mathbf{V}^T &= M(\mathbf{A}, \mathbf{U}_1, \mathbf{U}_2) \text{diag}(\mathbf{a}, \mathbf{b}) M(\mathbf{B}, \mathbf{V}_1, \mathbf{V}_2)^T \\
&= \mathbf{A} \text{diag}(\mathbf{U}_1, \mathbf{U}_2) \text{diag}(\mathbf{a}, \mathbf{b}) \text{diag}(\mathbf{V}_1, \mathbf{V}_2)^T \mathbf{B}^T \\
&= \mathbf{A} \text{diag}(\mathbf{U}_1 \mathbf{a} \mathbf{V}_1^T, \mathbf{U}_2 \mathbf{b} \mathbf{V}_2^T) \mathbf{B}^T,
\end{aligned} \tag{9}$$

with Lemma 4.10.3, and due to elementary block arithmetic. \square

4.3 Invertibility

We provide the explicit inverse of our two-parameter Hoffman's isomorphism.

Lemma 4.11. *The homomorphism Φ is invertible, where*

$$\Phi^{-1}(\mathbf{a}) := \sum_{\substack{I \in C(\text{rows}(\mathbf{a})) \\ J \in C(\text{cols}(\mathbf{a}))}} \frac{(-1)^{\text{rows}(\mathbf{a}) - \text{len}(I) + \text{cols}(\mathbf{a}) - \text{len}(J)}}{I_1 \dots I_{\text{len}(I)} J_1 \dots J_{\text{len}(J)}} \mathbf{a}_{I,J}$$

for every nonempty $\mathbf{a} \in \text{Comp}$.

Example 4.12.

$$\begin{aligned}
\Phi^{-1}([1]) &= [1], & \Phi^{-1}\left(\begin{bmatrix} 1 \\ 2 \end{bmatrix}\right) &= \begin{bmatrix} 1 \\ 2 \end{bmatrix} - \frac{1}{2} [1 \star 2], \\
\Phi^{-1}\left(\begin{bmatrix} 1 & \varepsilon \\ \varepsilon & 2 \end{bmatrix}\right) &= \begin{bmatrix} 1 & \varepsilon \\ \varepsilon & 2 \end{bmatrix} - \frac{1}{2} \begin{bmatrix} 1 \\ 2 \end{bmatrix} - \frac{1}{2} [1 \ 2] + \frac{1}{4} [1 \star 2]
\end{aligned}$$

In order to prove this, we introduce further notation. For two fixed formal power series in one variable t , and without constant term,

$$f = \sum_{i \in \mathbb{N}} f_i t^i, \quad g = \sum_{i \in \mathbb{N}} g_i t^i \in t \cdot \mathbb{K}[[t]],$$

we define a \mathbb{K} -linear **evaluation** $\text{eval}_{f,g} \in \text{End}(H)$ via

$$\text{eval}_{f,g}(\mathbf{a}) := \sum_{\substack{I \in C(\text{rows}(\mathbf{a})) \\ J \in C(\text{cols}(\mathbf{a}))}} f_{I_1} \dots f_{I_{\text{len}(I)}} g_{J_1} \dots g_{J_{\text{len}(J)}} \mathbf{a}_{I,J}$$

for every \mathbb{K} -basis element $\mathbf{a} \in \text{Comp}$. For every $i \in \mathbb{N}_0$ let $[t^i]f := f_i$ denote the coefficient of f at monomial t^i . We introduce the two-parameter generalization of [14, Thm. 3.1].

Lemma 4.13. *We have*

$$\text{eval}_{f,p} \circ \text{eval}_{g,q} = \text{eval}_{f \circ g, p \circ q}$$

for every $f, g, p, q \in t \cdot \mathbb{K}[[t]]$.

We recall the one-parameter argument from [14, eq. (9)],

$$[t^k](f \circ g) = \sum_{j=1}^k [t^j]f [t^{k-j}]g^j \quad (10)$$

for every $f, g \in t \cdot \mathbb{K}[[t]]$ and $k \in \mathbb{N}$. Let $\mathbf{a} \in \text{Comp}$ be fixed. For $I \in C(\text{rows}(\mathbf{a}))$ with $\text{len}(I) = x$ and $J \in C(x)$ let

$$J \circ I := (I_1 + \cdots + I_{J_1}, I_{J_1+1} + \cdots + I_{J_1+J_2}, \dots, I_{J_1+\cdots+J_{\ell-1}+1} + I_x) \in C(\text{rows}(\mathbf{a}))$$

denote the concatenation of I and J . Note that $\text{len}(J \circ I) = \text{len}(J)$. Recall further from [14, eq. (11)] that for all $K \in C(\text{rows}(\mathbf{a}))$,

$$\begin{aligned} & [t^{K_1}](f \circ g) \dots [t^{K_{\text{len}(K)}}](f \circ g) \\ &= \sum_{x=1}^{\text{rows}(\mathbf{a})} \sum_{\substack{J \in C(x) \\ \text{len}(J)=\text{len}(K)}} \sum_{\substack{I \in C(\text{rows}(\mathbf{a})) \\ J \circ I = K}} [t^{J_1}]f \dots [t^{J_{\text{len}(K)}}]f [t^{I_1}]g \dots [t^{I_x}]g. \end{aligned} \quad (11)$$

Proof of Lemma 4.13. We use the recalled one-parameter argument from above on rows and columns, i.e.

$$\begin{aligned} & \text{eval}_{f \circ g, p \circ q}(\mathbf{a}) \\ &= \sum_{\substack{K \in C(\text{rows}(\mathbf{a})) \\ L \in C(\text{cols}(\mathbf{a}))}} [t^{K_1}](f \circ g) \dots [t^{K_{\text{len}(K)}}](f \circ g) [t^{L_1}](p \circ q) \dots [t^{L_{\text{len}(L)}}](p \circ q) \mathbf{a}_{K,L} \\ &\stackrel{(11)}{=} \sum_{\substack{K \in C(\text{rows}(\mathbf{a})) \\ L \in C(\text{cols}(\mathbf{a})) \\ 1 \leq x \leq \text{rows}(\mathbf{a}) \\ 1 \leq y \leq \text{cols}(\mathbf{a})}} \sum_{\substack{J \in C(x) \\ B \in C(y) \\ \text{len}(J)=\text{len}(K) \\ \text{len}(B)=\text{len}(L)}}} \sum_{\substack{I \in C(\text{rows}(\mathbf{a})) \\ A \in C(\text{cols}(\mathbf{a})) \\ \text{with} \\ J \circ I = K \\ B \circ A = L}} \left(\prod_a [t^{I_a}]g \right) \left(\prod_b [t^{A_b}]q \right) \left(\prod_s [t^{J_s}]f \right) \left(\prod_r [t^{B_r}]p \right) \mathbf{a}_{K,L} \\ &= \sum_{\substack{I \in C(\text{rows}(\mathbf{a})) \\ A \in C(\text{cols}(\mathbf{a}))}} \left(\prod_a [t^{I_a}]g \right) \left(\prod_b [t^{A_b}]q \right) \left(\sum_{\substack{1 \leq x \leq \text{rows}(\mathbf{a}) \\ 1 \leq y \leq \text{cols}(\mathbf{a}) \\ \text{with} \\ \text{len}(I)=x \\ \text{len}(A)=y}} \sum_{\substack{J \in C(x) \\ B \in C(y)}} \left(\prod_s [t^{J_s}]f \right) \left(\prod_r [t^{B_r}]p \right) \mathbf{a}_{I,A} \right)_{J,B} \\ &= \sum_{\substack{I \in C(\text{rows}(\mathbf{a})) \\ A \in C(\text{cols}(\mathbf{a}))}} [t^{I_1}]g \dots [t^{I_{\text{len}(I)}}]g [t^{A_1}]q \dots [t^{A_{\text{len}(A)}}]q \text{eval}_{f,p}(\mathbf{a}_{I,A}) \\ &= \text{eval}_{f,p} \circ \text{eval}_{g,q}(\mathbf{a}) \end{aligned}$$

for every \mathbb{K} -basis element $\mathbf{a} \in \text{Comp}$. □

Proof of Lemma 4.11. This follows by choosing $f(t) := g(t) := e^t - 1$ in the situation of Lemma 4.13. □

4.4 Comultiplication

Lemma 4.14. *The homomorphism Φ respects deconcatenation, i.e.,*

$$(\Phi \otimes \Phi) \circ \Delta = \Delta \circ \Phi.$$

In order to prove Lemma 4.14 we introduce splittings similar to [9, Sec. 5.3].

Definition 4.15. For fixed $\mathbf{a} = \text{diag}(\mathbf{u}_1, \dots, \mathbf{u}_{\text{len}(\mathbf{a})})$ and $0 < \alpha < \text{len}(\mathbf{a})$, we say that

$$(\mathbf{U}, \mathbf{V}) \in \text{fuse}(u, \text{rows}(\mathbf{a})) \times \text{fuse}(v, \text{cols}(\mathbf{a}))$$

is α -decomposable, if

$$(\mathbf{U}, \mathbf{V}) = (\text{diag}(\mathbf{U}_1, \mathbf{U}_2), \text{diag}(\mathbf{V}_1, \mathbf{V}_2)) \quad (12)$$

with $u = u_1 + u_2$ and $v = v_1 + v_2$ such that

$$(\mathbf{U}_1, \mathbf{U}_2) \in \text{fuse}\left(u_1, \sum_{1 \leq i \leq \alpha} \text{rows}(\mathbf{u}_i)\right) \times \text{fuse}\left(u_2, \sum_{\alpha+1 \leq i \leq \text{len}(\mathbf{a})} \text{rows}(\mathbf{u}_i)\right)$$

and

$$(\mathbf{V}_1, \mathbf{V}_2) \in \text{fuse}\left(v_1, \sum_{1 \leq i \leq \alpha} \text{cols}(\mathbf{u}_i)\right) \times \text{fuse}\left(v_2, \sum_{\alpha+1 \leq i \leq \text{len}(\mathbf{a})} \text{cols}(\mathbf{u}_i)\right).$$

Lemma 4.16. If (\mathbf{U}, \mathbf{V}) is α -decomposable, then its decomposition from eq. (12) is unique.

Similar to [9, Lem. 5.21] we describe the block structure of matrix compositions after the action due to Definition 4.7.

Lemma 4.17. For fixed \mathbf{U}, \mathbf{V} and \mathbf{a} , the set

$$\{(\mathbf{x}, \mathbf{y}) \in \text{Comp}^2 \mid \mathbf{x} \neq \mathbf{e} \neq \mathbf{y} \wedge \text{diag}(\mathbf{x}, \mathbf{y}) = \mathbf{U}\mathbf{a}\mathbf{V}^T\}$$

is in one-to-one correspondence to all **splittings**,

$$\mathfrak{S}_{\mathbf{U}, \mathbf{V}}^{\mathbf{a}} := \{1 \leq \alpha < \text{len}(\mathbf{a}) \mid (\mathbf{U}, \mathbf{V}) \text{ is } \alpha\text{-decomposable}\}.$$

Proof. If $\alpha \in \mathfrak{S}_{\mathbf{U}, \mathbf{V}}^{\mathbf{a}}$ then (\mathbf{U}, \mathbf{V}) is α -decomposable, and therefore,

$$\begin{aligned} \mathbf{U}\mathbf{a}\mathbf{V}^T &= \text{diag}(\mathbf{U}_1, \mathbf{U}_2) \text{diag}(\mathbf{u}_1, \dots, \mathbf{u}_{\text{len}(\mathbf{a})}) \text{diag}(\mathbf{V}_1, \mathbf{V}_2) \\ &= \text{diag}(\mathbf{U}_1 \text{diag}(\mathbf{u}_1, \dots, \mathbf{u}_\alpha) \mathbf{V}_1, \mathbf{U}_2 \text{diag}(\mathbf{u}_{\alpha+1}, \dots, \mathbf{u}_{\text{len}(\mathbf{a})}) \mathbf{V}_2) \\ &=: \text{diag}(\mathbf{x}^{(\alpha)}, \mathbf{y}^{(\alpha)}), \end{aligned} \quad (13)$$

where different α yield $\mathbf{x}^{(\alpha)}$ and $\mathbf{y}^{(\alpha)}$ of varying size.

Conversely, with $\text{size}(\mathbf{u}_i) = (u_i, v_i)$ and cumulative sum $\underline{u}_i := u_1 + \dots + u_i$, if

$$\begin{aligned} \mathbf{U}\mathbf{a}\mathbf{V}^T &= \star_{1 \leq s \leq \text{len}(\mathbf{a})} \left[\mathbf{e}_{\mu_{(\underline{u}_{(s-1)+1)}}} \quad \dots \quad \mathbf{e}_{\mu_{\underline{u}_s}} \right] \mathbf{v}_s \left[\mathbf{e}_{\iota_{(v_s+1)}} \quad \dots \quad \mathbf{e}_{\iota_{(v_{(s+1)})}} \right]^T \\ &= \text{diag}(\mathbf{x}, \mathbf{y}) \end{aligned}$$

with $\text{size}(\mathbf{x}) = (j_1, k_1)$ then all s -indexed factors

$$\left[\mathbf{e}_{\mu_{(\underline{u}_{(s-1)+1)}}} \quad \dots \quad \mathbf{e}_{\mu_{\underline{u}_s}} \right] \mathbf{v}_s \left[\mathbf{e}_{\iota_{(v_s+1)}} \quad \dots \quad \mathbf{e}_{\iota_{(v_{(s+1)})}} \right]^T =: \text{diag}(\mathbf{x}_1^{(s)}, \mathbf{y}_1^{(s)})$$

decompose with $\text{size}(\mathbf{x}_1^{(s)}) = (j_1, k_1)$. Furthermore, $\mathbf{x}_1^{(s)}$ has all entries equal to ε or $\mathbf{y}_1^{(s)}$ does. With $\mathbf{U}\mathbf{a}\mathbf{V}^T \in \text{Comp}$ and increasing μ and ι , there is a unique $0 \leq \alpha \leq \text{len}(\mathbf{a})$ such that $\mathbf{x}_1^{(1)}, \dots, \mathbf{x}_1^{(\alpha)}$ have entries different from ε , and $\mathbf{x}_1^{(\alpha+1)}, \dots, \mathbf{x}_1^{(\text{len}(\mathbf{a}))}$ have all entries equal to ε . Therefore, \mathbf{U} and \mathbf{V} are of shape (12). If $\mathbf{U}\mathbf{a}\mathbf{V}^T = \text{diag}(\mathbf{x}', \mathbf{y}')$ has a second decomposition with resulting splitting $\alpha' \in \mathfrak{S}_{\mathbf{U}, \mathbf{V}}^{\mathbf{a}}$ then $\text{rows}(\mathbf{x}) < \text{rows}(\mathbf{x}')$ and $\text{cols}(\mathbf{x}) < \text{cols}(\mathbf{x}')$ without loss of generality, thus $\alpha < \alpha'$. \square

Proof of Lemma 4.14. Let $\mathbf{a} = \text{diag}(\mathbf{u}_1, \dots, \mathbf{u}_a)$ with $\text{len}(\mathbf{a}) = a$, and for simplicity,

$$\tilde{\Delta}(\mathbf{b}) := \Delta(\mathbf{b}) - \mathbf{b} \otimes \mathbf{e} - \mathbf{e} \otimes \mathbf{b}$$

for every \mathbf{b} . Then, with Lemma 4.17,

$$\begin{aligned}
\tilde{\Delta} \circ \Phi(\mathbf{a}) &= \sum_{u,v} \sum_{\substack{\mathbf{U} \in \text{fuse}(u, \text{rows}(\mathbf{a})) \\ \mathbf{V} \in \text{fuse}(v, \text{cols}(\mathbf{a}))}} \frac{1}{\mathbf{U}!\mathbf{V}!} \Delta(\mathbf{U}\mathbf{a}\mathbf{V}^T) - \Phi(\mathbf{a}) \otimes \mathbf{e} - \mathbf{e} \otimes \Phi(\mathbf{a}) \\
&= \sum_{u,v} \sum_{\substack{\mathbf{U} \in \text{fuse}(u, \text{rows}(\mathbf{a})) \\ \mathbf{V} \in \text{fuse}(v, \text{cols}(\mathbf{a}))}} \frac{1}{\mathbf{U}!\mathbf{V}!} \sum_{\substack{\mathbf{x}, \mathbf{y} \in \text{Comp} \setminus \{\mathbf{e}\} \\ \text{diag}(\mathbf{x}, \mathbf{y}) = \mathbf{U}\mathbf{a}\mathbf{V}^T}} \mathbf{x} \otimes \mathbf{y} \\
&\stackrel{(13)}{=} \sum_{u,v} \sum_{\mathbf{U}, \mathbf{V}} \frac{1}{\mathbf{U}!\mathbf{V}!} \sum_{\alpha \in \mathfrak{S}_{u,v}^a} \mathbf{U}_1 \text{diag}(\mathbf{u}_1, \dots, \mathbf{u}_\alpha) \mathbf{V}_1^T \otimes \mathbf{U}_2 \text{diag}(\mathbf{u}_{\alpha+1}, \dots, \mathbf{u}_a) \mathbf{V}_2^T \\
&\stackrel{4.9}{=} \sum_{u,v} \sum_{\mathbf{U}, \mathbf{V}} \sum_{\substack{1 \leq \alpha < a \\ \text{such that } \mathbf{U}, \mathbf{V} \\ \alpha\text{-decomposable}}} \frac{\mathbf{U}_1 \text{diag}(\mathbf{u}_1, \dots, \mathbf{u}_\alpha) \mathbf{V}_1^T}{\mathbf{U}_1!\mathbf{V}_1!} \otimes \frac{\mathbf{U}_2 \text{diag}(\mathbf{u}_{\alpha+1}, \dots, \mathbf{u}_a) \mathbf{V}_2^T}{\mathbf{U}_2!\mathbf{V}_2!} \\
&= \sum_{1 \leq \alpha < a} \sum_{u,v} \sum_{\substack{\mathbf{U}, \mathbf{V} \\ \alpha\text{-decomposable}}} \frac{\mathbf{U}_1 \text{diag}(\mathbf{u}_1, \dots, \mathbf{u}_\alpha) \mathbf{V}_1^T}{\mathbf{U}_1!\mathbf{V}_1!} \otimes \frac{\mathbf{U}_2 \text{diag}(\mathbf{u}_{\alpha+1}, \dots, \mathbf{u}_a) \mathbf{V}_2^T}{\mathbf{U}_2!\mathbf{V}_2!} \\
&\stackrel{4.8}{=} \sum_{1 \leq \alpha < a} \left(\sum_{\substack{u_1 \\ v_1}} \sum_{\substack{\mathbf{U}_1 \\ \mathbf{V}_1}} \frac{\mathbf{U}_1 \text{diag}(\mathbf{u}_1, \dots, \mathbf{u}_\alpha) \mathbf{V}_1^T}{\mathbf{U}_1!\mathbf{V}_1!} \right) \otimes \left(\sum_{\substack{u_2 \\ v_2}} \sum_{\substack{\mathbf{U}_2 \\ \mathbf{V}_2}} \frac{\mathbf{U}_2 \text{diag}(\mathbf{u}_{\alpha+1}, \dots, \mathbf{u}_a) \mathbf{V}_2^T}{\mathbf{U}_2!\mathbf{V}_2!} \right) \\
&= \sum_{1 \leq \alpha < a} \Phi(\text{diag}(\mathbf{u}_1, \dots, \mathbf{u}_\alpha)) \otimes \Phi(\text{diag}(\mathbf{u}_{\alpha+1}, \dots, \mathbf{u}_a)) \\
&= (\Phi \otimes \Phi) \circ \tilde{\Delta}(\mathbf{a})
\end{aligned}$$

and thus the claim with $\Phi(\mathbf{e}) = \mathbf{e}$. □

Putting it all together, we can prove the main result of this section.

Proof of Theorem 4.1. Use Definition 4.2 and Lemmas 4.4, 4.11 and 4.14. □

5 Implicit isomorphisms of Hopf algebras

Let us recall from Remark 1.1 that as a coalgebra, $H = \mathbb{K}\langle \text{Comp}_{\text{con}} \rangle$ is isomorphic to a deconcatenation coalgebra, and therefore it is cofree over Comp_{con} . This means in particular that we have some tools at our disposal for defining Hopf maps to and from H . We denote by $\pi : H \rightarrow \text{Comp}_{\text{con}}$ the projection, orthogonal to

$$\bigoplus_{\mathbf{a} \in \text{Comp} \setminus \text{Comp}_{\text{con}}} \mathbb{K}\mathbf{a}.$$

We note that for any $\mathbf{a}, \mathbf{b} \in \text{Comp}$,

$$\pi(\mathbf{a} \sqcup \mathbf{b}) = 0. \quad (14)$$

Let (C, Δ_C) be any graded connected coalgebra. By cofreeness of H , a coalgebra homomorphism $\Psi : C \rightarrow H$ is characterized by its projectiol

$$\psi := \pi \circ \Psi : C^+ \rightarrow \text{Comp}_{\text{con}},$$

where $C^+ = \ker \epsilon_C$ denotes the augmentation ideal, and moreover

$$\Psi = \sum_{n \geq 1} \text{diag} \circ \psi^{\otimes n} \circ \tilde{\Delta}_C^{(n-1)}.$$

Further still, Ψ is a coalgebra isomorphism if and only if ψ is a linear isomorphism.

As a consequence, two coalgebra morphisms $\Psi, \Psi' : C \rightarrow H$ coincide if and only if $\psi = \psi'$. Applying this to $C = H \otimes H$, and the maps $\sqcup \circ (\Psi \otimes \Psi)$ and $\Psi \circ \sqcup$, we see that a coalgebra morphism Ψ is a bialgebra morphism, if and only if these are equal. By cofreeness and eq. (14) this condition is equivalent to requiring that for any $\mathbf{a}, \mathbf{b} \in \text{Comp}$,

$$\psi(\mathbf{a} \sqcup \mathbf{b}) = 0. \quad (15)$$

One can make use of this condition together with certain maps that decompose elements in H as two-parameter shuffle polynomials to obtain bialgebra (hence Hopf algebra) homomorphisms from (H, \sqcup) to (H, \sqcup^{\square}) .

5.1 Leray's theorem

In this section m denotes either \sqcup , \sqcup^{qs} or \sqcup^{\square} . For $f, g \in \text{End}(H)$ we have the convolution product

$$f * g := m \circ (f \otimes g) \circ \Delta \in \text{End}(H),$$

and in particular, $f^{*0} := \text{id}$ and $f^{*k} := f * f^{*(k-1)}$ for every $k \in \mathbb{N}$. The mapping $\text{id} - \mu \circ \epsilon$ with counit ϵ and unit μ is ***-nilpotent**, i.e., for all $a \in H$ there is $k \in \mathbb{N}$ such that $f^{*k}(a) = 0$. This defines the **Eulerian idempotent**

$$e := \log^*(\text{id}) := \sum_{k \geq 1} \frac{(-1)^{k-1}}{k} (\text{id} - \mu \circ \epsilon)^k \in \text{End}(H).$$

Note that

$$(\ker \epsilon)^2 := \{m(a \otimes b) \mid a, b \in \ker \epsilon\}$$

is a \mathbb{K} -submodule of $\ker \epsilon$.

For the following two results see [18, Sec. 7], [2, Sec. 4.3] or [11, Thm. 1.7.29].

Lemma 5.1. *We have*

- 1 $\ker \epsilon = \mathbb{K} + (\ker \epsilon)^2$ and
- 2 $\text{Im } \epsilon \cong (\ker \epsilon) / (\ker \epsilon)^2$ as \mathbb{K} -modules.

Theorem 5.2 (Leray). $H \cong \text{Sym}(\text{Im } \epsilon)$ as \mathbb{K} -algebras.

If \mathbb{K} is a field and B a \mathbb{K} -basis of $\text{Im } \epsilon$, then $H \cong \mathbb{K}[B]$ as \mathbb{K} -algebras, where $\mathbb{K}[B]$ denotes the polynomial algebra over B considered as a set of symbols.

By definition the identity

$$\text{id} = \exp^*(\epsilon)$$

holds, thus we get an explicit decomposition of any matrix composition as a polynomial in elements of $\text{Im } \epsilon$, namely

$$\mathbf{u}_1 \dots \mathbf{u}_\ell = \sum_{I \in \mathcal{C}(\ell)} \frac{1}{\text{len}(I)!} m \left(\epsilon(\mathbf{u}_{I_1} \dots \mathbf{u}_{I_1}) \otimes \dots \otimes \epsilon(\mathbf{u}_{I_1+\dots+I_{\text{len}(I)-1}+1} \dots \mathbf{u}_\ell) \right).$$

From Lemma 5.1 we see that ϵ fulfills condition (15). However, it is not always true that $\text{Im } \epsilon \subset \text{Comp}_{\text{con}}$, as the following example shows.

Example 5.3. *Let m be the two-parameter shuffle product \sqcup . Then*

$$\begin{aligned} \epsilon \left(\begin{bmatrix} 1 & \epsilon \\ \epsilon & 2 \end{bmatrix} \right) &= \begin{bmatrix} 1 & \epsilon \\ \epsilon & 2 \end{bmatrix} - \frac{1}{2} \left(\begin{bmatrix} 1 & \epsilon \\ \epsilon & 2 \end{bmatrix} + \begin{bmatrix} \epsilon & 1 \\ 2 & \epsilon \end{bmatrix} + \begin{bmatrix} \epsilon & 2 \\ 1 & \epsilon \end{bmatrix} + \begin{bmatrix} 2 & \epsilon \\ \epsilon & 1 \end{bmatrix} \right) \\ &= \frac{1}{2} \left(\begin{bmatrix} 1 & \epsilon \\ \epsilon & 2 \end{bmatrix} - \begin{bmatrix} 2 & \epsilon \\ \epsilon & 1 \end{bmatrix} \right) - \frac{1}{2} \begin{bmatrix} \epsilon & 1 \\ 2 & \epsilon \end{bmatrix} - \frac{1}{2} \begin{bmatrix} \epsilon & 2 \\ 1 & \epsilon \end{bmatrix} \notin \text{Comp}_{\text{con}}. \end{aligned}$$

Combining Theorem 5.2 with results from the previous section we obtain the following result.

Theorem 5.4. *Let $\text{Log}_{\sqcup^{\square}}: (H, \sqcup) \rightarrow (H, \sqcup^{\square})$ be the unique bialgebra map induced by $\pi \circ \epsilon$. It is an isomorphism, and its inverse*

$$\text{Exp}_{\sqcup^{\square}}: (H, \sqcup^{\square}) \rightarrow (H, \sqcup)$$

is recursively given by

$$\pi_n \left(\text{Exp}_{\sqcup}^{\sqcup}(\pi_m(\mathbf{a})) \right) = - \sum_{k=n}^m \pi_n \circ \text{Exp}_{\sqcup}^{\sqcup} \circ \pi_k \circ \text{Log}_{\sqcup}^{\sqcup} \circ \pi_m(\mathbf{a}), \quad n \leq m,$$

where for $k \in \mathbb{N}$, $\pi_k : H \rightarrow \text{Comp}_{\text{con}}^k$ denotes the canonical projection onto the space of matrix compositions with exactly k connected blocks. The same holds after replacing \sqcup by \sqcup^{qs} .

Proof. Note that the restriction of $\text{Log}_{\sqcup}^{\sqcup}$ to Comp_{con} is the identity map, thus it is a linear isomorphism. Hence, it is an isomorphism of algebras. The formula for $\text{Exp}_{\sqcup}^{\sqcup}$ follows from a general expression for inversion of lower-triangular maps. \square

Remark 5.5. Note that in the terminology of [14, Prop. 4.1] the map $\pi \circ \epsilon$ is a contraction, and the map $\text{Log}_{\sqcup}^{\sqcup}$ is the corresponding expansion.

In particular, by considering appropriate compositions of the exponential and logarithm maps we obtain:

Corollary 5.6. We have $(H, \sqcup, \Delta) \cong (H, \sqcup, \Delta) \cong (H, \sqcup^{\text{qs}}, \Delta)$ as Hopf algebras.

5.2 Application: New proof of the two-parameter bialgebra relation

In this section we present a new proof of the bialgebra relation in $(H, \sqcup^{\text{qs}}, \Delta)$, using the isomorphism to the (classical, one-parameter) block shuffle algebra introduced in this article.

Proof of Thm. 5.24 in [9]. With isomorphism Ψ from (H, \sqcup, Δ) to $(H, \sqcup^{\text{qs}}, \Delta)$ according to Theorem 5.4,

$$\begin{aligned} \Delta \circ \sqcup^{\text{qs}} &= \Delta \circ \sqcup^{\text{qs}} \circ (\Psi \otimes \Psi) \circ (\Psi^{-1} \otimes \Psi^{-1}) \\ &= \Delta \circ \Psi \circ \sqcup \circ (\Psi^{-1} \otimes \Psi^{-1}) \\ &= (\Psi \otimes \Psi) \circ \Delta \circ \sqcup \circ (\Psi^{-1} \otimes \Psi^{-1}) \\ &\stackrel{2.9}{=} (\Psi \otimes \Psi) \circ (\sqcup \otimes \sqcup) \circ (\text{id} \otimes \tau \otimes \text{id}) \circ (\Delta \otimes \Delta) \circ (\Psi^{-1} \otimes \Psi^{-1}) \\ &= (\sqcup^{\text{qs}} \otimes \sqcup^{\text{qs}}) \circ \Psi^{\otimes 4} \circ (\text{id} \otimes \tau \otimes \text{id}) \circ (\Delta \otimes \Delta) \circ (\Psi^{-1} \otimes \Psi^{-1}) \\ &= (\sqcup^{\text{qs}} \otimes \sqcup^{\text{qs}}) \circ (\text{id} \otimes \tau \otimes \text{id}) \circ \Psi^{\otimes 4} \circ (\Delta \otimes \Delta) \circ (\Psi^{-1} \otimes \Psi^{-1}) \\ &= (\sqcup^{\text{qs}} \otimes \sqcup^{\text{qs}}) \circ (\text{id} \otimes \tau \otimes \text{id}) \circ (\Delta \otimes \Delta) \circ (\Psi \otimes \Phi) \circ (\Psi^{-1} \otimes \Psi^{-1}) \\ &= (\sqcup^{\text{qs}} \otimes \sqcup^{\text{qs}}) \circ (\text{id} \otimes \tau \otimes \text{id}) \circ (\Delta \otimes \Delta), \end{aligned}$$

where τ denotes the flip homomorphism determined by $\tau(\mathbf{a} \otimes \mathbf{b}) := \mathbf{b} \otimes \mathbf{a}$ for all $\mathbf{a}, \mathbf{b} \in \text{Comp}$. \square

6 Conclusions and outlook

We have used free Lyndon generators, ideas from \mathbf{B}_∞ -algebras, and a novel two-parameter Hoffman's exponential to provide three different classes of isomorphisms between the two-parameter shuffle and quasi-shuffle algebra. In particular, we have provided a Hopf algebraic connection to the (classical, one-parameter) shuffle algebra over the extended alphabet of connected matrix compositions.

- 1 The here suggested machinery should be useful also for [10, 21] since it provides free generators and an underlying Hopf algebra structure for two-parameter mapping space signatures. In particular, it is now possible to manage all coefficients that are algebraically dependent through shuffling. This is one of the primary reasons to consider log signatures in the one-parameter setting.
- 2 Already in [9, Sec. 6] we addressed the issue to generalize our work for $p > 2$ parameters. The new strategy applied in Section 5.2 should allow us to work around elementary block-tensor arithmetic and prevent us from notational clutter.

- 3 The unsolved question from [9, Sec. 6] regarding the computational complexity of the two-parameter sums signature, taken at an arbitrary matrix composition, can now be reduced to a set of free generators introduced in this article. For example Theorem 3.12 provides the relation

$$\begin{bmatrix} 1 & \varepsilon \\ \varepsilon & 1 \end{bmatrix} = \frac{1}{2} [1] \overset{\text{qs}}{\sqcup} [1] - \begin{bmatrix} \varepsilon & 1 \\ 1 & \varepsilon \end{bmatrix} - \begin{bmatrix} 1 \\ 1 \end{bmatrix} - \begin{bmatrix} 1 & 1 \end{bmatrix} - \frac{1}{2} [1 \star 1]$$

which allows us to compute for every eventually zero $Z : \mathbb{N}^2 \rightarrow \mathbb{K}^d$ the matrix

$$\left(\langle \text{SS}_{0_2;t}(Z), \begin{bmatrix} \varepsilon & 1 \\ 1 & \varepsilon \end{bmatrix} \rangle \right)_{\substack{1 \leq t_1 \leq T_1 \\ 1 \leq t_2 \leq T_2}} \in \mathbb{K}^{T_1 \times T_2}$$

in linear time $O(T_1 T_2)$. So far, the (iteratively) chained coefficients from [9, Thm 4.5] and the algebraic relations according to quasi-shuffles do not yield linear complexity algorithms for all coefficients of the two-parameter signature. *Can we understand which coefficients are not computable in linear time via chaining or even other approaches?*

- 4 The isomorphisms due to Sections 3, 4 and 5 are all different from each other. While the Lyndon isomorphisms of algebras (Corollary 3.13) do not respect the underlying coproduct Δ dual to diagonal concatenation, the way we define the isomorphism of Hopf algebras Φ inspired by Hoffman (Definition 4.2) seems independent of the explicit Δ . *Does Φ respect other coproducts such as deconcatenation along the antidiagonal? Can we make the isomorphism Φ unique up to certain conditions? Can we find a natural isomorphism from one-parameter to two-parameter shuffles which does not depend on Δ using theory related to cumulants?*

References

- [1] I. P. Arribas, C. Salvi, and L. Szpruch, *Sig-SDEs model for quantitative finance*, Proceedings of the First ACM International Conference on AI in Finance, ICAIF '20, Association for Computing Machinery, 2021.
- [2] P. Cartier and F. Patras, *Classical Hopf algebras and their applications*, Springer, 2021.
- [3] E. Celledoni, P. E. Lystad, and N. Tapia, *Signatures in Shape Analysis: An efficient approach to Motion Identification*, GSI 2019: Geometric Science of Information (Cham) (F. Nielsen and F. Barbaresco, eds.), Lecture Notes in Computer Science, no. 11712, Springer International Publishing, 2019, pp. 21–30.
- [4] K.-T. Chen, *Iterated integrals and Exponential homomorphisms*, *Proc. London Math. Soc. (3)* **4** (1954), 502–512.
- [5] I. Chevyrev and A. Kormilitzin, *A primer on the Signature method in Machine Learning*, 2016, [arXiv:1603.03788](https://arxiv.org/abs/1603.03788) [stat.ML].
- [6] J. Diehl, K. Ebrahimi-Fard, and N. Tapia, *Time-warping invariants of multidimensional time series*, *Acta Applicandae Mathematicae* **170** (2020), no. 1, 265–290.
- [7] ———, *Tropical time series, iterated-sums signatures, and quasisymmetric functions*, *SIAM Journal on Applied Algebra and Geometry* **6** (2022), no. 4, 563–599.
- [8] J. Diehl and R. Krieg, *FRUITS: Feature Extraction Using Iterated Sums for Time Series classification*, 2023, [arXiv:2311.14549](https://arxiv.org/abs/2311.14549) [stat.ML].
- [9] J. Diehl and L. Schmitz, *Two-parameter sums signatures and corresponding quasisymmetric functions*, 2023, [arXiv:2210.14247](https://arxiv.org/abs/2210.14247) [math.CO].
- [10] C. Giusti, D. Lee, V. Nanda, and H. Oberhauser, *A topological approach to mapping space signatures*, 2022, [arXiv:2202.00491](https://arxiv.org/abs/2202.00491) [math.FA].
- [11] D. Grinberg and V. Reiner, *Hopf algebras in combinatorics*, 2020, [arXiv:1409.8356](https://arxiv.org/abs/1409.8356) [math.CO].
- [12] L. G. Gyurkó, T. Lyons, M. Kontkowski, and J. Field, *Extracting information from the signature of a financial data stream*, 2013, [arXiv:1307.7244](https://arxiv.org/abs/1307.7244) [q-fin.ST].
- [13] M. E. Hoffman, *Quasi-shuffle products*, *Journal of Algebraic Combinatorics* **11** (2000), 49–68.
- [14] M. E. Hoffman and K. Ihara, *Quasi-shuffle products revisited*, *Journal of Algebra* **481** (2017), 293–326.

- [15] L. Jin, T. Lyons, H. Ni, and W. Yang, *Rotation-free online handwritten character recognition using dyadic path signature features, hanging normalization, and deep neural networks*, 23rd International Conference on Pattern Recognition (ICPR), IEEE, 2016.
- [16] P. Kidger, P. Bonnier, I. Perez Arribas, C. Salvi, and T. Lyons, *Deep signature transforms*, Advances in Neural Information Processing Systems (H. Wallach, H. Larochelle, A. Beygelzimer, F. Alché-Buc, E. Fox, and R. Garnett, eds.), vol. 32, Curran Associates, Inc., 2019.
- [17] D. McLeod and T. Lyons, *Signature methods in Machine Learning*, 2022, [arXiv:2206.14674](https://arxiv.org/abs/2206.14674) [stat.ML].
- [18] J. W. Milnor and J. C. Moore, *On the structure of Hopf algebras*, *Annals of Mathematics, Second Series* **81** (1965), no. 2, 211–264.
- [19] D. E. Radford, *A natural ring basis for the shuffle algebra and an application to group schemes*, *Journal of Algebra* **58** (1979), no. 2, 432–454.
- [20] W. Yang, T. Lyons, H. Ni, C. Schmid, and L. Jin, *Developing the path signature methodology and its application to landmark-based human action recognition*, Stochastic Analysis, Filtering, and Stochastic Optimization: A Commemorative Volume to Honor Mark H. A. Davis's Contributions (G. Yin and T. Zariphopoulou, eds.), Springer International Publishing, Cham, 2022, pp. 431–464.
- [21] S. Zhang, G. Lin, and S. Tindel, *Two-dimensional signature of images and texture classification*, *Proceedings of the Royal Society A* **478** (2022), no. 2266, 20220346.

Index

- *-nilpotent, 18
- α -decomposable, 16
- len-compatible, 6
- $a \cdot e_i$ with $a, i \in \mathbb{N}$, 11
- \mathcal{B} , 6
- block shuffle action matrix, 4
- block shuffle product, 4
- \sqcup , 4
- bSH, 4
- \mathcal{B}^m , 7
- C , 11
- Chen-Fox-Lyndon (CFL) factorization, 7
- cols, 2
- Comp_{con} , 2
- $\text{Comp}_{\text{con}}^*$, 2
- composition, 11
- Comp, 2
- Δ , 2
- $\widetilde{\Delta}$, 16
- diag, 2
- e, 2
- ϵ , 18
- ε , 2
- \mathfrak{e} , 18
- Eulerian idempotent, 18
- eval, 14
- evaluation, 14
- factorial, 11, 12
- fuse, 11
- graded lexicographic order, 6
- $<_{\text{grlex}}$, 6
- H, 2
- \mathbb{K} , 2
- $\mathbb{K}\langle \text{Comp}_{\text{con}} \rangle$, 2
- \mathcal{Q} , 6
- leading monomial, 7
- $\text{len} : C(n) \rightarrow \mathbb{N}_0$, 11
- length, 2, 11
- $\text{len} : \text{Comp}_{\text{con}}^* \rightarrow \mathbb{N}_0$, 2
- \leq_{lex} , 6
- lexicographic order, 6
- lm, 7
- Lyndon word, 6
- \mathfrak{M}_d , 2
- monomial order, 6
- μ , 18
- \mathbb{N} , 2
- \mathbb{N}_0 , 2
- permutations, 3
- Φ , 11
- π , 17
- \mathbb{Q} , 2
- QSH, 5
- qsh, 5
- $\overset{\text{qs}}{\sqcup}$, 5
- rows, 2
- $\mathfrak{S}_{u,v}^a$, 16
- SH, 3
- sh, 3
- \sqcup , 3
- Σ_n , 3
- size, 2
- splittings, 16
- \star , 2
- $*$, 18
- two-parameter quasi-shuffle product, 5
- two-parameter shuffle product, 3