Bases of Quantum Group Algebras in Terms of Lyndon Words

Eremey Valetov

BASES OF QUANTUM GROUP ALGEBRAS IN TERMS OF LYNDON WORDS

EREMEY VALETOV

ABSTRACT. We have reviewed some results on quantized shuffling, and in particular, the grading and structure of this algebra. In parallel, we have summarized certain details about classical shuffle algebras, including Lyndon words (primes) and the construction of bases of classical shuffle algebras in terms of Lyndon words. We have explained how to adapt this theory to the construction of bases of quantum group algebras in terms of Lyndon words. This method has a limited application to the specific case of the quantum group parameter being a root of unity, with the requirement that specialization to the root of unity is non-restricted. As an additional, applied part of this work, we have implemented a Wolfram Mathematica package with functions for quantum shuffle multiplication and constructions of bases in terms of Lyndon words.

CONTENTS

Date: September 22, 2016.
2000 *Mathematics Subject Classification.* 17B37, 81R50.
Physics and Astronomy Classification Scheme. 02.20.Uw.
Key words and phrases. quantum group algebras, quantized shuffling, bases, Lyndon words.

1. Introduction

In [24], D. Radford has developed the classical shuffle algebra, proposed a method of constructing its bases in terms of Lyndon words (primes), and explained how this can be applied to commutative pointed irreducible Hopf algebras.

A common object of shuffle algebras is a tensor space $T(V) = \oplus_{n=0}^{+\infty} V^{\otimes n}$, where V is a module. Consider an element $v_a = v_{x_1} \otimes \cdots \otimes v_{x_n}$ of this tensor space. Let $\{v_x | x \in X\}$ be an indexed basis of V and $S = (X)$ the free semigroup generated by X. We establish a notation for the a in v_a that is bijective to the vector $(x_1, \cdots, x_n)$ by setting $a = x_1 \cdots x_n \in S$. This a is called a word, and may be viewed as a nonempty string of characters.

If the set X is totally ordered with some relation $\leq$, we can extend it to S as a lexicographic order. Lexicographic order has multiple applications; for example, a variant of lexicographical order is used the set of real numbers $\mathbb{R}$ in decimal notation, and strings in computer science are commonly lexicographically compared.

In 1954, R. Lyndon has investigated a special type of words called standard lexicographic sequences or regular words [19], which were later also named Lyndon words and primes. If $a \in S$, then a is called a Lyndon word if for any its factorization $uv = a$ with $u, v \in S$ we have $v < a$. Any word in S can be factorized into Lyndon words, and this factorization is unique.

Shuffle algebras use a special multiplication operation called shuffle multiplication. Shuffle multiplication of v_a and v_b, where $a, b \in S$, is defined as the sum of elements of the tensor space that correspond to a special type of permutation that may be called a $(m_0, \cdots, m_r)$-shuffle applied to a and b. We will cover this in detail later on.

To construct bases of $T(V)$ in terms of Lyndon words, we define X_a, which is a shuffle multiplication of elements corresponding to Lyndon words in the unique prime factorization of a. The X_a's form a linear basis of $T(V)$.

M. Rosso has introduced the quantum shuffle algebra [25], which can be viewed as a quantized version of the classical shuffle algebra. Rosso described the construction of its bases in terms of Lyndon words. A quantum shuffle algebra is constructed from the cotensor Hopf algebra of a Hopf bimodule, and this applies to the Hopf subalgebra $U_q^+(\mathfrak{g})$ of a quantum group algebra $U_q(\mathfrak{g})$.

In the case of quantum shuffle algebras, the quantum deformation manifests itself through permutations of the form $s(v \otimes w) = w \otimes v$ being replaced by diagonal braiding of the form $\sigma(v \otimes w) = q_{ij}(w \otimes v)$ in the implementation of $(m_0, \cdots, m_r)$-shuffles.

In the same paper [25], Rosso has discussed how the quantum shuffle algebra theory can be applied to the Hopf bimodules $U_q^+(\mathfrak{g})$. This application may not be immediately obvious to a reader.

We would like to illuminate the path of familiarization with the method of bases construction in terms of Lyndon words for classical shuffle algebras, quantum shuffle algebras, and how this method can be applied to quantum group algebras. Along the way, we wish to implement quantum shuffle multiplication and the corresponding method of bases construction as a Wolfram Mathematica package (function library).

We recognize that an important issue in research is setting priorities and specializing in a number of chosen subject matter areas. With shuffle algebras being the subject matter of specialization in this work, we honor this concept by deriving each proof we provide in this paper on our own. On the level of formulations of mathematical propositions, our aim is to preserve precision and legacy.

We will use the terms 'Lyndon word' and 'prime' interchangeably based on our perception of their common usage in various context. In the broad picture, we prefer to use the term 'Lyndon word'[1].

2. Literature review

We consider the papers by Radford and Rosso [24, 25] mentioned in the introduction to be the primary references for our work, and we will now briefly outline their contents.

In "A natural ring basis for the shuffle algebra and an application to group schemes" [24], Radford (1) defines the shuffle algebra of a set X, including the shuffle multiplication; (2) defines U-graded algebra (coalgebra), with $u(x)$ as the number of x's in the factorization of $a \in S$; (3) shows how commutative pointed irreducible Hopf algebras may be embedded into classical shuffle algebras; (4) details the structure of the Lyndon words of S; (5) discusses prime factorization and shuffles; (6) presents a method of constructing bases of classical shuffle algebras in terms of Lyndon words; and (7) covers some applications and other details.

In "Quantum groups and quantum shuffles" [25], Rosso (1) discusses the Hopf bimodule structure; (2) specifies a braiding in the category of Hopf bimodules that was introduced by Woronowicz [33]; (3) constructs the cotensor Hopf algebra from a Hopf bimodule, including the quantum shuffle multiplication; (4) shows an embedding of a tensor space $T(V)$ in the cotensor Hopf algebra; (5) introduces the quantum symmetric algebra that is a sub-Hopf algebra of the cotensor Hopf algebras; (6) details the universal construction of a quantum shuffle algebra in the braid category; (7) gives examples from abelian group algebras; (8) details the structure of Lyndon words and a method of bases construction of quantum shuffle algebras in terms of Lyndon words; (9)

[1]A trivial paragaph intended for internal audience was deleted here.

covers consequences of growth conditions; and (10) presents a theory for and the applications of the inductive construction of higher rank quantized enveloping algebras.

M. Sweedler's "Hopf algebras" [29] is useful as a review of Hopf algebras in that it provides thorough coverage of relevant concepts such as comodules and coinvariants. "Quantum groups" [13] by C. Kassel introduces crossed modules and modules over the quantum (or, "Drinfel'd") double. Additional references on the quantum double are "Quantum groups" [9] by V. Drinfel'd and "Doubles of quasitriangular Hopf algebras" [20] by S. Majid. For notations and facts about the symmetric group, one may refer to "Groupes et algèbres de Lie" [5] by N. Bourbaki. "Braid groups" [14] by C. Kassel and V. Turaev is a good introduction to the Artin braid groups, which is relevant to the study of quantum shuffle algebras.

Key references used in [25] by Rosso are "Differential calculus on compact matrix pseudogroups (quantum groups)" [33] by S. Woronowicz and "Quantum groups and representations of monoidal categories" [34] by D. Yetter. We found the material in [33] regarding braidings and braid equations to be illuminating. In [34], the discussion of Hopf algebra structure, including comodules and bimodules, somewhat parallels that in [25]. The diagrammatic notation in [34] is a real gem that enables the reader to visually follow through Hopf algebra calculations and evolutions.

For the purposes of coherency, rigor, and broad familiarization with the subject matter, we have reviewed a number of papers on quantum shuffle algebras, including "Quantum quasi-shuffle algebras" [12] by R.-Q. Jian et al., "Quantum symmetric algebras" [7] and "Quantum symmetric algebras II" [8] by D. de Chela and J. Green, and "Dual canonical bases, quantum shuffles and q-characters" by B. Leclerc.

Having understood classical and quantum shuffle algebras, we have turned our attention to quantum group algebras. The following landmark textbooks contain a wealth of information about quantum groups, including basic definitions, universal R-matrices, and braidings: "A guide to quantum groups" [6] by V. Chari and A. Pressley, "Introduction to quantum groups" [18] by G. Lusztig, "Lectures on quantum groups" [11] by J. Jantzen, and "Quantum groups" [13] by C. Kassel.

The paper "A formula for the R-matrix using a system of weight preserving endomorphism" [32] by P. Tingley was useful in finding the form of the standard universal R-matrix of a quantum group algebra. While in general, the universal R-matrix is not unique, "The uniqueness theorem for the universal R-matrix" [15] by S. Khoroshin and V. Tolstoy is a relevant and instructive text.

Next, we have researched the case of quantum groups with the quantum parameter q as a root of unity. We have used the authoritative details in [6] as the main reference for that purpose. "Quantum groups at roots of 1" [17] by G. Lusztig is a historical reference on that topic. The study aid "Quantum groups at root of unity" [28] by B. Singh is a concise overview of the root of unity case.

We have used [18] and "On the automorphisms of $U_q^+(\mathfrak{g})$" [2] by N. Andruskiewitsch and F. Dumas as references to identify that the positive part $U_q^+(\mathfrak{g})$ of a quantum group algebra $U_q(\mathfrak{g})$ is a Nichols algebra with diagonal braiding. In "A survey on Nichols algebras" [30], M. Takeuchi reviews the categorical approach to Nichols algebras and their braided shuffle algebras aspect. We returned to [25] to confirm and validate the conclusions on application of the method of bases construction in terms of Lyndon words to quantum group algebras.

3. Quantum group algebras I

3.1. **Quantum group algebras.** Since the primary objective of this work is to apply the shuffle algebra theory to quantum group algebras, we will begin by defining quantum group algebras and referring to the braiding relations of tensor products of their modules. To some extent, there appears to be a convention to provide a detailed definition of a quantum group algebra in papers on this topic. The purpose of this is not only to remind the reader of the relatively numerous relations, but also to advise about the version or variation of the notation to be used in the specific paper. For example, the generators denoted here as e_i and f_i are also referred to in some papers as X_i^+ and X_i^- respectively.

Definition 1 (Quantum group algebra – in principle)**.** There are numerous related definitions of quantum group algebras. V. Drinfel'd [9] and M. Jimbo have formalized the definition of a quantum group algebra as a Hopf algebra that is a deformation of the universal enveloping algebra of a Kac-Moody algebra.

Historically, the first application of quantum group algebras was the quantum inverse scattering method in statistical mechanics in the first half of the 1980s. Other applications include probability theory, harmonic analysis, and number theory [10].

3.2. **Drinfel'd-Jimbo type quantum group algebras.**

Definition 2 (Quantum group algebra – formal[2])**.** Let $A = (a_{ij})$ be the Cartan matrix of a Kac-Moody algebra and let $q \in \mathbb{C}$ such that $q \notin \{0, 1\}$. Let $\mathfrak{g}$ be a Kac-Moody algebra with the Cartan matrix A. Then the quantum group $U_q(\mathfrak{g})$ is defined as the unital associative algebra with Chevalley generators k_λ, e_i, and f_i as follows:

[2]This definition was obtained from the Wikipedia page "Quantum group" at `https://en.wikipedia.org/wiki/Quantum_group` and carefully compared with [26] and numerous other sources.

- $k_0 = 1$, $k_\lambda k_\mu = k_{\lambda+\mu}$
- $k_\lambda e_i k_\lambda^{-1} = q^{(\lambda,\alpha_i)} e_i$, $k_\lambda f_i k_\lambda^{-1} = q^{-(\lambda,\alpha_i)} f_i$
- $[e_i, f_j] = \delta_{ij} \frac{k_i - k_i^{-1}}{q_i - q_j^{-1}}$
- if $i \neq j$, then $\sum_{n=0}^{1-a_{ij}} (-1)^n \frac{[1-a_{ij}]_{q_i}!}{[1-a_{ij}-n]_{q_i}![n]_{q_i}!} e_i^n e_j e_i^{1-a_{ij}-n} = 0$ and $\sum_{n=0}^{1-a_{ij}} (-1)^n \frac{[1-a_{ij}]_{q_i}!}{[1-a_{ij}-n]_{q_i}![n]_{q_i}!} f_i^n f_j f_i^{1-a_{ij}-n} = 0$ (q-Serre relations)

where λ is an element of the weight lattice, α_i are the simple roots, $(,)$ is an invariant symmetric bilinear form, $k_i = k_{\alpha_i}$, $d_i = (\alpha_i, \alpha_i)/2$ (making $B = \left(d_i^{-1} a_{ij}\right)$ symmetric), $q_i = q^{d_i}$, $[0]_{q_i!} = 1$, $[n]_{q_i}! = \prod_{m=1}^{n} [m]_{q_i}$ for all $n \in \mathbb{N}$ (q-factorial), and $[m]_{q_i} = \frac{q_i^m - q_i^{-m}}{q_i - q_i^{-1}}$ (q-number).

To make it a Hopf algebra, we can define the counit as $\epsilon(k_\lambda) = 1$ and $\epsilon(e_i) = \epsilon(f_i) = 0$ and select a compatible coproduct $\triangle$ and an antipode S.

Example (Common definition of coproduct)**.** The coproduct of a quantum group algebra $U_q(\mathfrak{g})$ is often defined by

- $\triangle(k_\lambda) = k_\lambda \otimes k_\lambda$
- $\triangle(e_i) = 1 \otimes e_i + e_i \otimes k_i$
- $\triangle(f_i) = k_i^{-1} \otimes f_i + f_i \otimes 1$

Other definitions are possible and used.

The limit of $q \to 1$. In the $q \to 1$ limit, the quantum group algebra $U_q(\mathfrak{g})$ relations approach universal enveloping algebra $U(\mathfrak{g})$ relations, with

- $k_\lambda \to 1$
- $\frac{k_\lambda - k_{-\lambda}}{q_i - q_i^{-1}} \to t_\lambda$

where t_λ are elements of the Cartan subalgebra and $(t_\lambda, h) = \lambda(h)$ for all elements h in the Cartan subalgebra.

Triangular decomposition. Quantum group algebra $U_q(\mathfrak{g})$ has a triangular decomposition into negative U^+, neutral U^0, and positive U^+ parts [30, p. 109]:

$$U_q(\mathfrak{g}) = U^- \otimes U^0 \otimes U^+$$

3.3. **Representations of $U_q(\mathfrak{g})$.**

Isomorphism of $U_q(\mathfrak{g})$-modules [11, 6, 18]**.** While for $U(\mathfrak{g})$-modules V and W the functorial isomorphism between $V \otimes W$ and $W \otimes V$ is a flip map $P : v \otimes w \mapsto w \otimes v$, for $U_q(\mathfrak{g})$ it is, in general, not an isomorphism. However, $U_q(\mathfrak{g})$ is nearly quasitriangular, i.e. there exists an infinite formal sum that plays the role of an R-matrix, which may be called the quasi R-matrix [18]. Commonly, an alternative construction called universal R-matrix is used [31, 6]. A functorial isomorphism $R_{V,W}$ between $V \otimes W$ and $W \otimes V$ for $U_q(\mathfrak{g})$-modules V and W is defined as $R_{V,W} : v \otimes w \mapsto R(w \otimes v)$.

Action of a braid group on $U_q(\mathfrak{g})$-rep [6, p. 276]**.** If V is a $U_q(\mathfrak{g})$-module, action of the universal R-matrix on $V^{\otimes 3}$ satisfies the Yang-Baxter equation

$$(R \otimes 1)(1 \otimes R)(R \otimes 1) = (1 \otimes R)(R \otimes 1)(1 \otimes R)$$

But this is also the braiding equation for the action of a braid group B_n on $V^{\otimes n}$. The R-matrix defines the representation of the braid group B_n that acts on $V^{\otimes n}$ as functorial isomorphisms.

4. Common framework

In this section, we will lay out the common foundation for classical and quantum shuffle algebras. Having this done, we will only need to address the details specific to each case in the subsequent sections.

4.1. **Tensor space $T(V)$.**

Definition 3 (Tensor space $T(V)$)**.** For a context-specific vector space V and $n \in \mathbb{N}$, we define tensor space $T(V)$ as

$$T(V) = \oplus_{k=0}^{+\infty} V^{\otimes k}$$

In [24], the classical shuffle algebra is defined such that it is $T(V)$ as a vector space. However, the bases in terms of Lyndon words are constructed for its subspace generated by V [24, p. 446], as well as the whole space $T(V)$ by adding an appropriately defined Lyndon word of zero length or the multiplicative identity element of the underlying field of V.

A similar situation holds true quantum shuffle algebras. A quantum shuffle algebra is an algebra and coalgebra structure defined on the tensor space $T(V)$. The bases in terms of Lyndon words are constructed for the subalgebra of $T(V)$ generated by V, denoted as $S_\sigma(V)$ and called quantum symmetric algebra or bialgebra (or Hopf algebra) of type one [25, p. 407], as well as for the whole tensor space $T(V)$.

This naturally follows from starting with and intending to use the bases of V to construct shuffle algebras.

Definition 4 (Braiding on $T(V)$ [12, 8])**.** Consider an arbitrary braiding $\tau \in End(V \otimes V)$. Then τ satisfies the quantum Yang-Baxter braiding equation (or, "braiding equation") on $V^{\otimes 3}$

$$(1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \tau) = (\tau \otimes 1) \circ (1 \otimes \tau) \circ (\tau \otimes 1)$$

A vector space V with braiding τ that satisfies these conditions is called "braided vector space". The braiding τ induces an action of the Artin braid group B_n on $V^{\otimes n} \subset T(V)$ for all $n \in \mathbb{N}$.

The standard generators of B_n are denoted as $\sigma_1, \cdots, \sigma_{n-1}$. For all $i \in [[1, n-1]]$, the generator σ_i is defined as $1^{\otimes(i-1)} \otimes \tau \otimes 1^{\otimes(n-i-1)}$ and can be written as $(i \mapsto i+1)$ [14]. Its inverse σ_i^{-1} can be written as $(i+1 \mapsto i)$. The generator σ_i acts on $V^{\otimes n}$ as follows:

$$\sigma_i : \otimes_{j=1}^{n} V_{(j)} \mapsto \left(\otimes_{j=1}^{i-1} V_{(j)}\right) \otimes \tau\left(V_{(i)} \otimes V_{(i+1)}\right) \otimes \left(\otimes_{j=i+1}^{n} V_{(j)}\right)$$

4.2. **Symmetric and braid group notations.** We use the following symmetric and braid group notations [25, p. 401]:

- $\sum_n$: the symmetric group of $\{1, 2, \cdots, n\}$
- s_i: transposition $(i, i+1)$
- B_n: Artin braid group on n strands
- σ_i (or $(i \mapsto i+1)$) for $i \in [[1, n-1]]$: the i-th generator of B_n
- $(l_1, \cdots, l_r)$-shuffle for $l_1 + \cdots + l_r = n$: the set of permutations w such that

$$w(1) < w(2) < \cdots < w(l_1)$$

$$w(l_1+1) < w(l_1+2) < \cdots < w(l_1+l_2)$$

$$\cdots$$

$$w(l_1 + \cdots + l_{r-1} + 1) < \cdots < w(n)$$

- $\sum_{(l_1, \cdots, l_r)}$ for $l_1 + \cdots + l_r = n$: the set of $(l_1, \cdots, l_r)$-shuffles
- $\sum_{l_1, n-l_1}$ for $l_1 \leq n$: the set of $(l_1, n-l_1)$-shuffles
- $l(w)$: the length of the reduced expression of permutation w in terms of standard generators s_i
- T_w for $w \in \sum_n$: the lift of w in B_n, also known as "Matsumoto section" [21], and defined as $w = s_{i_1} \cdots s_{i_{l(w)}} \mapsto T_w = \sigma_{i_1} \cdots \sigma_{i_{l(w)}}$
- $\mathscr{B}_{(l_1, \cdots, l_r)} = \sum_{w \in \sum_{(l_1, \cdots, l_r)}} T_w$
- $\tilde{\mathscr{B}}_{(l_1, \cdots, l_r)} = \sum_{w \in \sum_{(l_1, \cdots, l_r)}} T_w^{-1}$

4.3. **Matsumoto section.** Symmetric group $\sum_n$ is generated by $n-1$ transpositions $s_j = (j, j+1)$, where $j \in [[1, n-1]]$. Likewise, braid group B_n is generated by $n-1$ generators of $\sigma_j = (j \mapsto j+1)$, where

$j \in [[1, n-1]]$. While verbs 'transpose' and 'permute' are defined for symmetric groups, there is no universally recognized verb usage that fully expresses respective braiding operations for braid groups. To remedy this, we will extend this symmetric group terminology to braid groups. We will say that the generators of B_n transpose a pair of elements by analogy with the symmetric group, with the caveat that $\sigma_j \neq \sigma_j^{-1}$ for all $j \in [[1, n-1]]$. We will say that elements of B_n permute elements of a tensor space (or a string) by the same analogy. For any $s_j \in \sum_n$, we can define its lift in B_n (or, "Matsumoto section") as $T_{s_j} = \{\sigma_j, \sigma_j^{-1}\}$, but only $T_{s_j} = \sigma_j$ applies for shuffle algebra purposes by their construction. For a reduced expression on $w = s_1 \cdot \cdots \cdot s_{l(w)} \in \sum_n$, we define T_w as $T_w = T_{s_1} \cdot \cdots \cdot T_{s_{l(w)}}$.

4.4. **Shuffle product on tensor space $T(V)$.**

Proposition 5 (Shuffle product on $T(V)$ [25, 24])**.**

Assume that braid groups $B_n, n \in \mathbb{N}$ act on $T(V)$. Let $x_1, \cdots, x_n$ be in V. We define an associative algebra structure on $T(V)$, given by the shuffle product

$$(x_1 \otimes \cdots \otimes x_p) \cdot (x_{p+1} \otimes \cdots \otimes x_n) = \sum_{w \in \sum_{p,n-p}} T_w (x_1 \otimes \cdots \otimes x_n)$$

4.5. **Gradings of $T(V)$.** Let $(X, \leq)$ be a totally ordered set. Let $S = (X)$ be the free semigroup generated by X.

Definition 6 (Grading of S [24])**.** Let $U = N^{(X)}$ be the additive semigroup of all functions from X to the natural numbers $N = \{0\} \cup \mathbb{N}$ which have finite support. For $u \in U$ let $S(u) \subseteq S$ bet the set of all $a = \prod_{j=1}^{k} x_j \in S$ such that $u(x)$ is the number of x's in the factorization of a for all $x \in X$. We note that $S(u)$ is finite.

Definition 7 (U-graded coalgebra (bialgebra) [24])**.** If U is any commutative (resp. additive) semigroup, a coalgebra (resp. bialgebra) A is U-graded if for each $u \in U$ there exists a subspace $A(u)$ such that (a)-(c) (resp. (a)-(d)) from the following are satisfied:

(1) $A = \oplus_{u \in U} A(u)$, where $A(0) = k$;
(2) $\epsilon(A(u)) = 0$ if $u \neq 0$;
(3) $\Delta A(u) \subseteq \sum_{v+w=u} A(v) \otimes A(w)$;
(4) $A(u) A(v) \subseteq A(u+w)$ for all $u, v \in U$; and
(5) $A(u)$ is finite-dimensional for all $u \in U$.

An element $a \in A$ can uniquely decomposed as $a = \oplus a_u$, where $a_u \in A(u)$ for all $u \in U$.

U-grading was used in [24] for classical shuffle algebras but not in [25] for quantum shuffle algebras. While it may not be essential for shuffle algebras, we find it to be useful for understanding the structure of shuffle algebras and for their construction. We decided to use U-grading for both classical and quantum shuffle algebras in this work, and we found the application of U-grading to quantum shuffle algebras to be an interesting exercise.

Proposition 8 (Gradings of $T(V)$ [25, 24])**.**

(1) *$T(V)$ is naturally graded with $T^k V$ being the k-grade subspace.*
(2) *Let $T(V)(u)$ be the linear span of v_a's where $a \in S(u)$. This defines U-grading of $T(V)$.*

These gradings are compatible with shuffle multiplication and with universal construction of a shuffle algebra.

4.6. **Ordering and Lyndon words in S.**

Definition 9 (Total ordering of S [25, 24])**.**

(1) A total ordering $\leq$ on the set S is defined by lexicographic ordering, with the convention that $a \cdot b \leq a$ for any $a, b \in S$.

(2) We call an element $p \in S$ a prime (or, a "Lyndon word") if, for any splitting $p = a \cdot b$ with $a, b \in S$, we have $b < p$. We denote the set of primes in S as P.

Definition 10 (Prime factorization in S)**.** Let $a \in S$. We will call a factorization $\prod_{j=1}^{k} p_j = a$ a prime factorization of a if each p_j is a prime but cannot itself be factorized into two or more primes.

Proposition 11 (Existence of prime factorization in S)**.** *Any $a \in S$ has a prime factorization.*

Proof. Let $a \in S$. Consider the factorization $\prod_{j=1}^{k} x_j = a$, where $x_j \in X$ for all j. Each x_j is a prime because $X \subset P$ by definition of a prime. We can use the following iterative method with $\prod_{j=1}^{k} x_j = a$ as the initially considered factorization:

(1) If the currently considered factorization $\prod_{j=1}^{k} p_j = a$ is a prime factorization, stop, as we have achieved the objective.
(2) Otherwise, there must be a prime $p = \prod_{j=j_1}^{j_2} p_j$ that prevents $\prod_{j=1}^{k} p_j = a$ from satisfying the definition of a prime factorization. We replace the currently considered factorization of a by $\prod_{j=1}^{j_1-1} p_j \cdot p \cdot \prod_{j=j_2+1}^{k} p_j$, decreasing the length of factorization by at least one.
(3) Go to step 1.

□

Since k is finite, this iterative method completes in a finite number of steps, yielding a prime factorization of a.

Proposition 12 (Unique prime factorization in S [25, 24])**.** *Prime factorization of any $a \in S$ is unique.*

Proof. Let $a \in S$ and suppose that $\prod_{j=1}^{k} p_j$ and $\prod_{j=1}^{r} p'_j$ are prime factorizations of a. We need to prove that $k = r$ and $p_i = p'_i$ for all i.

Indeed:

(1) The case $r = k = 1$ is trivial.

(2) Suppose that $r > 1$ or $k > 1$. We will prove that $p_n = p'_n$ for $n = 1$. Suppose $p_1 \neq p'_1$. Then either $p_1 = \left(\prod_{j=1}^{m} p'_j\right) \cdot s$ or $p'_1 = \left(\prod_{j=1}^{m} p_j\right) \cdot s$ for some $m \in \mathbb{N}$ and $s \in S$ such that s is shorter or equal in length to p'_{m+1} or p_{m+1} respectively. Without the loss of generality, let $p_1 = \left(\prod_{j=1}^{m} p'_j\right) \cdot s$ for some $s \in S$. By definition of s, $s \geq p'_{m+1}$. Because p_1 is a prime, $p_1 > s$ and therefore, $p'_1 > p_1 > s \geq p'_{m+1}$. This contradicts $p'_1 \cdot \dots \cdot p'_r$ being a prime factorization. We can use the proof of Proposition 13 here to justify this contradiction because it doesn't use the uniqueness property of prime factorization.

(3) Applying the method of mathematical induction on n with item 2 of this proof as its base case and a trivial inductive step, we get $p_n = p'_n$ for all $n \leq \max(\{r, k\})$.

(4) Now suppose that $r \neq k$. Without the loss of generality, suppose $r > k$. Then

$$a = \prod_{j=1}^{k} p_j = \prod_{j=1}^{k} p_j \cdot \prod_{j=k+1}^{r} p'_j$$

But by definition of total ordering $<$,

$$\prod_{j=1}^{k} p_j > \prod_{j=1}^{k} p_j \cdot \prod_{j=k+1}^{r} p'_j$$

Contradiction.

We have proved that $r = k$ and $p_i = p'_i$ for all i. □

Proposition 13 (Form of unique prime factorization [25, 24])**.** *For any $a \in S$, its unique prime factorization has the form $a = \prod_{j=1}^{k} p_j^{n_j}$, where $p_j < p_{j+1}$ for all $1 \leq j \leq k-1$ and $n_j \in \mathbb{N}$ for all $1 \leq j \leq k$.*

Proof. Indeed, suppose that $p_{j_0} \geq p_{j_0+1}$ for some $1 \leq j_0 \leq k-1$. Then one of the following is true:

(1) $p_{j_0} = p_{j_0+1}$. Then the prime factorization can be rewritten as $a = \prod_{j=1}^{j_0-1} p_j^{n_j} \cdot p_{j_0}^{n_{j_0}+n_{j_0+1}} \cdot \prod_{j=j_0+2}^{k} p_j^{n_j}$, where we omit any terms p_j for $j \leq 0$ or $j \geq k+1$.

(2) $p_{j_0} > p_{j_0+1}$. Then a contains the term $p_{j_0} \cdot p_{j_0+1}$, where $p_{j_0} > p_{j_0+1}$, but then by definition of prime, $p_{j_0} \cdot p_{j_0+1}$ itself is a prime, and there is a contradiction with $a = \prod_{j=1}^{k} p_j^{n_j}$ being a prime factorization.

□

Theorem 14 (Relation between $T_w(a)$ and a [25, 24])**.** *Suppose $a \in S$ has prime factorization $a = \prod_{i=1}^{s} p_i^{n_i}$. Then*

(1) *$T_w(a) \geq a$ for $w \in \sum_{(l_1,\cdots,l_s)}$, where l_i is the length of p_i.*

(2) *Let $w \in \sum_{(l_1,\cdots,l_s)}$. Then $T_w(a) = a$ if and only if w is in the subgroup $\sum_{n_1} \times \cdots \times \sum_{n_s}$ of "block permutations", permuting only p_i's among themselves for each i.*

Proof. We note that for $a = p_1$, we have $T_w(a) = T_w(p_1) = p_1 = a$ because $T_{\sum_{(l_1)}} = \{Id\}$, so *a forteriori* $T_w(a) \geq a$. However, we will use the fact that item (1) is true for $s = 0$ vacuously and see that this makes sense as we use it. Now suppose that $a = \prod_{i=1}^{s} p_j^{n_i}$ for $s = r \geq 2$. Decompose $p_i = \prod_{j=1}^{l_i} x_{ij}$ for all $1 \leq i \leq s$. Also, we denote the decomposition of any $z \in S$ in X as $z = \prod_j z_j$. By definition of prime and definition of prime decomposition, we have $x_{s1} > x_{ji}$ for all j and i such that $(i,j) \neq (1,s)$. Let $\lambda_a(x)$ be the set of indices $\{i\}$ such that $a_i = x$. Then by definition of a $(l_1,\cdots,l_s)$-shuffle, we then have that $\lambda_a(x_{s1}) \subseteq \{1, l_1, \cdots, \sum_{t=1}^{s} n_t l_t - l_s + 1\}$. We note that the restriction of w to $w^{-1}\left(\left[1, \min\left(\lambda_{T_w(a)}(x_{s1})\right) - 1\right]\right)$ is equivalent to the restriction of some $u \in \sum_{(l_1,\cdots,l_s-1)}$ to the same set. There are two possibilities:

(1a): $i_0 := \min\left(\lambda_{T_w(a)}(x_{s1})\right) < \lambda_a(x_{s1})$. Supposing that item (1) of this Theorem is true for $s = r - 1 \geq 1$, we have that

$\prod_{i=1}^{i_0-1} T_w(a)_i \geq \prod_{i=1}^{i_0-1} a_i$, and because $x_{s1} > x_{ji}$ for all j and i such that $(i,j) \neq (1,s)$, we have that $T_w(a)_{i_0} > a_{i_0}$. Therefore, $T_w(a) > a$.

(1b): $i_0 := \min\left(\lambda_{T_w(a)}(x_{s1})\right) \geq \lambda_a(x_{s1})$. Then $\lambda_{T_w(a)}(x_{s1}) = \lambda_a(x_{s1})$. Suppose $l = w^{-1}\left(\max\left(\lambda_{T_w(a)}(x_{s1})\right)\right)$. Applying the definition of a $(l_1, \cdots, l_s)$-shuffle, we have

$$w(l) < \cdots < w(l + l_s - 1)$$

and therefore for the interval $I = [[l, l + l_s - 1]]$ we have $w(I) = [[\sum_{t=1}^{s} n_t l_t - l_s + 1, \sum_{t=1}^{s} n_t l_t]]$. Iteratively applying this reasoning, we have that $\prod_{i=\sum_{t=1}^{s-1} n_t l_t + 1}^{\sum_{t=1}^{s} n_t l_t} w(a)_i = \prod_{i=\sum_{t=1}^{s-1} n_t l_t + 1}^{\sum_{t=1}^{s} n_t l_t} a_i$, i.e. $w \in \sum_{(l_1, \cdots, l_{s-1})} \times \sum_{n_s}$. Now, supposing that item (1) of this Theorem is true for $s = r - 1 \geq 0$, we have that $\prod_{i=1}^{\sum_{t=1}^{s-1} n_t l_t} T_w(a)_i \geq \prod_{i=1}^{\sum_{t=1}^{s-1} n_t l_t} a_i$. Therefore, $T_w(a) \geq a$.

From discussion in case 1b see that $T_w(a) = a$ if and only if case 1b applies to the last block of $a = \prod_{i=1}^{r} p_j^{n_i}$ for all $1 \leq r \leq s$, i.e. if and only if $w \in \sum_{n_1} \times \cdots \times \sum_{n_s}$. □

5. Classical shuffle algebras

Considering that classical shuffle algebras can be obtained as the $q \to 1$ limit of quantum shuffle algebras and that our objective in this section is to summarize some facts about classical shuffle algebras, we will be concise here and refer the reader to Quantum Shuffle Algebras section (or to [24]) for proofs.

5.1. **Definition and notes.**

Definition 15 (Classical shuffle algebra [24])**.** A classical shuffle algebra $Sh(V)$ of V is a commutative strictly graded pointed irreducible Hopf algebra with shuffle product:

for $x_1, \cdots, x_n$ in V,

$$(x_1 \otimes \cdots \otimes x_p) \cdot (x_{p+1} \otimes \cdots \otimes x_n) = \sum_{w \in \sum_{p,n-p}} T_w (x_1 \otimes \cdots \otimes x_n)$$

As a vector space, $Sh(V) = T(V)$.

In classical shuffle algebras, the T_w's are actually $(l_1, \cdots, l_r)$-shuffles. The lift T_w of $(l_1, \cdots, l_r)$-shuffle w to the braid group represents an increase in the structure complexity with the purpose of implementing a quantum deformation in quantum shuffle algebras. Viewing the classical shuffle algebras as quantum shuffle algebras in the limit $q \to 1$, for consistent notation between classical and quantum shuffle algebras, we may either (1) by abuse of notation, formally set $T_w = w$; or (2) use the braiding relation $\sigma(v \otimes w) = w \otimes v$ in the classical shuffle algebras – these two options are practically equivalent.

Proposition 16 (Embedding bialgebras into the classical shuffle algebra [24])**.**

(1) *Let A be a sub-bialgebra of $Sh(V)$ for some vector space V over a field k. Then A is a commutative pointed irreducible Hopf algebra. If* $\operatorname{char} k = p > 0$, *then $x^p = 0$ for $x \in A^+$.*

(2) *Let $V = P(A)$ be the space of primitives of a commutative pointed irreducible Hopf algebra A. If* $\operatorname{char} k = 0$ *or* $\operatorname{char} k = p > 0$ *and $x^p = 0$ for $x \in A^+$, then A is isomorphic to a sub-Hopf algebra of $Sh(V)$.*

5.2. **Bases in terms of Lyndon words.** Here we continue where we left off in the previous section.

Lemma 17 (The α_{aa} coefficient in X_a (see Proposition 18))**.** *Let $a \in S$, and let $p_1^{n_1} \cdots p_s^{n_s} = a$ be its prime factorization ($p_1 < \cdots < p_s$). Then the number of σ's in $\mathscr{B}_{(l_1, \cdots, l_s)}$ such that $\sigma(a) = a$ is $n_1! \cdots n_s!$.*

Proof. Trivial. The method of mathematical induction may be used. See Quantum Shuffle Algebras II section or [24, p. 445] for details. □

Theorem 18 (Bases of classical shuffle algebras in terms of Lyndon words [24])**.** *Assume* char $k = 0$. *Let $a \in S(u)$ and $a = \prod_{i=1}^{s} p_i^{n_i}$ be its unique prime factorization. We define $X_a = \prod_{i=1}^{s} v_{p_i}^{n_i}$, where quantum multiplication is used between the terms of the form v_{p_i}. Then:*

1. *$X_a, a \in S(u)$ form a basis of $T(V)(u)$; and*
2. *the change of basis with respect to a is triangular, i.e. there exist $\alpha_{ab} \in k$ such that $X_a = \sum_{a \leq b} \alpha_{ab} v_b$;*
3. *setting for $1 \leq i \leq s$ $p_i = \prod_{j=1}^{l_i} x_{ij}$, we have $\alpha_{aa} = \prod_{j=1}^{s} (n_j!) \neq 0$;*
4. *the X_a's, $a \in S$, form a linear basis of $T(V)$;*
5. *the v_p's, $p \in P$, form a polynomial basis for $T(V)$;*
6. *$X_a \cdot X_b = X_{a \cdot b}$ for $a, b \in S$.*

Proof. See the Proposition 37 or [24, p. 446]. □

A similar theorem has been formulated in [24, p. 447] for the case char $k = p > 0$.

Point 5 in Theorem 18 elucidates the reason why we call this construction of bases in terms of Lyndon words. While any $v_a, a \in S$ has a unique prime factorization of a in terms of Lyndon words, the resulting v_p components compose v_a using tensor multiplication, but for a polynomial basis, the operation that should be used is multiplication. This is satisfied with shuffle multiplication in Theorem 18.

6. Quantum shuffle algebras

We will follow the fundamental work of Rosso [25] towards the definition of a quantum shuffle algebra. Afterwards, we will provide formulations and our proofs for construction of bases of quantum shuffle algebras in terms of Lyndon words.

6.1. **Hopf bimodules.** We will first define Hopf bimodules and provide an overview of their relevant structure.

Definition 19 (Hopf bimodule [25, p. 401])**.** Let H be a k-Hopf algebra. A Hopf bimodule over H is a k-vector space M given with an H-bimodule structure, a H-bicomodule structure (i.e. left and right coactions $\delta_L : M \to H \otimes M$, $\delta_R : M \to M \otimes H$ which commute in the following sense: $(\delta_L \otimes Id)\,\delta_R = (Id \otimes \delta_R)\,\delta_L$, and such that δ_L and δ_R are morphisms of H-bimodules.

Taking tensor products over Hopf algebra H, Hopf bimodules form a tensor category $\mathscr{E}$ [25, 23].

Definition 20 (Left and coinvariants of a Hopf bimodule [25, p. 402])**.**

(1) The left coinvariant subspace M^L of M is defined as

$$M^L = \{m \in M | \delta_L(m) = 1 \otimes m\}$$

It is a sub-right comodule of M and inherits a structure of right H-module by

$$m \cdot h = \sum S\left(h_{(1)}\right) m h_{(2)}$$

where $m \in M$ and $h \in H$.

(2) The right coinvariant subspace M^R of M is defined as

$$M^R = \{m \in M | \delta_R(m) = m \otimes 1\}$$

It is a sub-left comodule of M and inherits a structure of left H-module by

$$h \cdot m = \sum h_{(1)} m S\left(h_{(2)}\right)$$

where $m \in M$ and $h \in H$.

Proposition 21 (Properties of the right coinvariant [25, p. 402])**.**

(1) *The right coinvariant M^R of a Hopf bimodule M over H is a crossed module over H in the sense of Yetter.*
(2) *If H and M are finite-dimensional, it is a module over the quantum double.*
(3) *A morphism of Hopf bimodules induces on the space of right coinvariants a morphism of crossed modules.*

6.2. **Braidings in the category of Hopf bimodules.** Here we establish that the right coinvariant space M^R of a Hopf bimodule M has a naturally defined braiding $\sigma(v \otimes w) \mapsto w \otimes v$, where $v, w \in M^R$. This braiding is a foundation for construction of a quantum shuffle algebra.

Proposition 22 (Braiding in the category of Hopf bimodules [25, p. 403])**.** *Let M and N be H-Hopf bimodules.*

(1) *There exists a unique morphism of H-bimodules $\sigma_{M,N} : M \otimes N \to N \otimes M$ such that, for $\omega \in M^L$ and $\eta \in M^R$ we have $\omega_{M,N}(\omega \otimes \eta) = \eta \otimes \omega$.*
(2) *Furthermore, $\omega_{M,N}$ is an invertible morphism of bicomodules and satisfies the following braid equation (where M, N, and P are Hopf bimodules):*

$$(I_P \otimes \omega_{M,N})(\omega_{M,P} \otimes I_N)(I_M \otimes \omega_{N,P}) =$$
$$= (\omega_{N,P} \otimes I_M)(I_N \otimes \omega_{M,P})(\omega_{M,N} \otimes I_P)$$

(1) This makes $\mathscr{E}$ a braided tensor category [25, 13, 22].
(2) $\sigma_{M,M}$ sends $M^R \otimes M^R$ into itself, acting as

$$\sigma(x \otimes y) = \delta_L(x)(y \otimes 1)$$

and defines a representation T of the braid group B_n in $\left(M^R\right)^{\otimes n}$.

Proposition 23 (Equivalence between $\mathscr{E}$ and the category of crossed modules [25, p. 403])**.** *The functor sending M to M^R is an equivalence* *of braided tensor categories between $\mathscr{E}$ and the category of crossed modules.*

6.3. **The cotensor Hopf algebra.** We recall that a classical shuffle algebra is, on one level, a commutative strictly graded pointed irreducible Hopf algebra, and, on another level, a tensor space $T(V)$ with shuffle multiplication. Construction of a quantum shuffle algebra features a similar duality (in the philosophical sense of the word). The technical part with the tensor space $T(V)$, where $V = M^R$, is endowed with conceptual meaning as quantum shuffle algebra using cotensor Hopf algebra. A nontrivial isomorphism between the cotensor Hopf algebra and $T(V)$ is a key link in this construction.

Definition 24 (Cotensor product and cotensor coalgebra [25, p. 403])**.**

(1) Let M and N be H-Hopf bimodules. Their cotensor coproduct $M \sqcup N$ is the kernel of

$$\delta_R \otimes I_N - I_M \otimes \delta_L : M \otimes N \to M \otimes H \otimes N$$

(2) The cotensor coalgebra is constructed on M is

$$T_H^c(M) = H \oplus \oplus_{n \geq 1} M^{\sqcup n}$$

The following applies to the structure of tensor algebra

$$T_H(M) = H \oplus \oplus_{n \geq 1} M^{\otimes_H n}$$

(1) If A is an H-bimodule, $h \in H$, and a and $b \in A$, then

$$h(ab) = \sum h_{(1)}(a)\, h_{(2)}(b)$$

(2) If f and $g : M \to A$ are two H-bimodule maps, the map $f \cdot g : M \otimes_H M \to A$ is defined for $m \in M$ and $n \in M$ as

$$f \cdot g : m \otimes_H n \mapsto f(m)\, f(n)$$

Proposition 25 (Power of the sum of two bimodule maps [25, p. 404])**.** *Let A be an H-bimodule algebra and f and $g : M \to A$ two bimodule maps. Assume that $g \cdot f = (f \cdot g) \circ \sigma$. Then the map $(f+g)^n : M^{\otimes_H n} \to A$ is given by*

$$(f+g)^n = \sum_{k=0}^{n} \left(f^k \cdot g^{n-k}\right) \circ \tilde{\mathscr{B}}_{k,n-k}$$

Lemma 26 (Relation between coactions and braiding [25, p. 404])**.**

$$\delta_l \cdot \delta_R = (\delta_R \cdot \delta_R) \circ \sigma$$

Proposition 27 (Coproduct on $T(M)$ [25, p. 404])**.** *The coproduct on $T_H(M)$ is given by: for $(x_1, \cdots, x_n) \in M^{\otimes_H n}$,*

$$\triangle (x_1, \cdots, x_n) = \sum_{k=0}^{n} \left(\delta_R^k \cdot \delta_L^{n-k}\right) \circ \tilde{\mathscr{B}}_{k,n-k}$$

Definition 28 (Universal property of $T_H^c(M)$ [25, p. 405])**.** The product on $T_H^c(M)$ is a unique coalgebra map

$$T_H^c(M) \otimes T_H^c(M) \to T_H^c(M)$$

induced by the product on H and by left or right coaction on $H \otimes M + M \otimes H$.

We denote $V = M^R$ for simplicity.

Proposition 29 (Shuffle multiplication and structure of $T(V)$ [25, p. 405])**.**

(1) *There is an associative algebra structure on $T(V)$, given by: for $x_1, \cdots, x_n$ in V,*

$$(x_1 \otimes \cdots \otimes x_p) \cdot (x_{p+1} \otimes \cdots \otimes x_n) = \sum_{w \in \sum_{p,n-p}} T_w (x_1 \otimes \cdots \otimes x_n)$$

We call this "shuffle multiplication" or, more formally, "quantum shuffle multiplication". In other publications, it is also called *"quantum shuffle product" and "braided shuffle product"* [30, p. 107].

(2) *The diagonal coaction on H on each $V^{\otimes n}$ gives $T(V)$ an H-comodule structure $\delta_L : T(V) \to H \otimes T(V)$, and δ_L is an algebra homomorphism.*

(3) *For the diagonal action of H on each $V^{\otimes n}$, $T(V)$ is an H-module algebra, and $T(V) \otimes H$ inherits the crossed product algebra structure.*

(4) *The following defines a coalgebra structure on $T(V) \otimes H$: for $(v_1, \cdots, v_n)$ in V and h in H,*

$$\triangle((v_1, \cdots, v_n) \otimes h) = \\ = \sum_{k=0}^{n} \left[(v_1, \cdots, v_k) \otimes v_{k+1(-1)} \cdots v_{n(-1)} h_{(1)}\right] \\ \otimes \left[\left(v_{k+1(0)}, \cdots, v_{n(0)}\right) \otimes h_{(2)}\right]$$

(5) *The algebra structure of 3 and coalgebra structure of 4 are compatible and make $T(V) \otimes H$ a Hopf algebra.*

Proposition 30 (Embedding of $T(V)$ in $T_H^c(M)$ [25, p. 406])**.**

(1) *There is a natural embedding of ϕ of $T(V)$ in $T_H^c(M)$ given on homogenous elements of degree n by:*

$$\phi\left(v^1, \cdots, v^n\right) = \\ = \sum v^1 v^2_{(-1)} \cdots v^n_{(-n+1)} \otimes v^2_{(0)} v^3_{(-1)} \cdots v^n_{(-n+2)} \otimes \cdots \otimes v^n_{(0)}$$

whose image is the subspace of right coinvariants.

(2) *There is an isomorphism of right module and comodule* $\tilde{\phi}$: $T(V) \otimes H \to T_H^c(M)$

$$\tilde{\phi}\left[\left(v^1, \cdots, v^n\right) \otimes h\right] =$$
$$= \sum v^1 v^2_{(-1)} \cdots v^n_{(-n+1)} h_{(1)}$$
$$\otimes v^2_{(0)} v^3_{(-1)} \cdots v^n_{(-n+2)} h_{(2)} \otimes \cdots \otimes v^n_{(0)} h_{(n)}$$

(3) *The subspace of right coinvariants is a subalgebra of* $T_H^c(M)$.

Theorem 31. *The map* $\tilde{\phi}$ *is a Hopf algebra isomorphism.* [25, p. 405]

Below, we will show bases construction in terms of Lyndon words for $T(V)$.

6.4. **Quantum symmetric algebra.** The term "quantum symmetric algebra" was introduced by Rosso [25] and refers in part to quantization $\sigma(v \otimes w) = q_{vw} w \otimes v$ of the action $\sigma(v \otimes w) = w \otimes v$ of a symmetric group on a tensor space.

Definition 32 (Quantum symmetric algebra [25, p. 407])**.** The sub-Hopf algebra $S_H(M)$ of $T_H^c(M)$ generated by M and H is a Hopf bimobule, and its subspace of right coinvariants is isomorphic, via ϕ, to the subalgebra of $T(V)$ generated by V. We will call this a "quantum symmetric algebra" and denote it by $S_\sigma(V)$.

Quantum symmetric algebra is also known as "Nichols algebra" by N. Andruskiewitsch and H.-J. Schneider [3] and "bialgebras of type one" by W. Nichols [23].

In general, braided shuffle algebras naturally satisfy the quantum Serre relations [30, p. 108].

The braiding on $S_\sigma(V)$ is induced by the diagonal braiding in $V \times V$ given by $\sigma(e_i \otimes e_j) = q_{ij}(e_j \otimes e_i)$ and is encoded in the $N \times N$ matrix (q_{ij}).

Since the braiding on $S_\sigma(V)$ is diagonal, we can extend the method of construction of bases in terms of Lyndon words for classic shuffle algebras to $S_\sigma(V)$ almost verbatim.

6.5. **Universal construction in braid category.** Assume that we have used the braid group generator σ to construct a representation of the braid group B_n in $V^{\otimes n}$. If we define a graded multiplication sh as in Proposition 33, or, more specifically, a shuffle multiplication, on the tensor space $T(V)$ generated by V, we may wish to ensure that algebra and coalgebra structures on $T(V)$ are compatible. To that end, we can (1) use the coproduct definition from Proposition 27 with trivial coactions, and (2) change the product in $T(V)\otimes T(V)$.

Proposition 33 (Associative algebra structure on $T(V)\otimes T(V)$ [25, p. 407-408])**.** *Let (V,σ) be a braided space.*

(1) *The following defines an associative algebra structure on $T(V)\otimes T(V)$: for p and q two positive integers, let $w_{p,q}$ be the permutation:*
$$\begin{pmatrix} 1 & 2 & \cdots & q & q+1 & \cdots & p+q \\ p+1 & p+2 & \cdots & p+q & 1 & \cdots & p \end{pmatrix}$$
and let $T_{w_{p,q}}$ be the associative element in the braid group B_{p+q}: it acts in $V^{\otimes p+q}$ and can be seen as a "generalized flip" from $V^{\otimes p}\otimes V^{\otimes q}$ to $V^{\otimes q}\otimes V^{\otimes p}$. Then the product sends $(V^{\otimes n}\otimes V^{\otimes p})\otimes(V^{\otimes q}\otimes V^{\otimes m})$ to $V^{\otimes n+q}\otimes V^{\otimes p+m}$ and it is the composition: $(sh\otimes sh)\circ\left(Id\otimes T_{w_{p,q}}\otimes Id\right)$ where sh denotes the product on $T(V)$ defined above.

(2) *Then $\Delta : T(V)\to T(V)\otimes T(V)$ is an algebra homomorphism.*

Proposition 34 (Shuffle algebra [25, p. 408])**.**

(1) *The shuffle algebra $\mathscr{S}$ in $\mathscr{B}$ is, as an object, the direct sum of all objects n.*

(2) *The product is given by the direct sum of its "homogenous components": for all n and m in $\mathbb{N}$, one has a component in*

$$Mor\,(n \otimes m, n+m)$$

which is the sum $T_w \in B_{n+m}$, w ranging in the set of (n,m)-shuffles of $\sum_{n+m}$.

(3) *The coalgebra structure is also given by the direct sum of its "homogenous components": for all n, p, q in $\mathbb{N}$ such that $p+q = n$, the component in $Mor\,(n, p \otimes q)$ is the canonical morphism $n \to p \otimes q$.*

(4) *These product and coproduct are compatible if we give $\mathscr{S} \otimes \mathscr{S}$ the algebra structure deduced from the one on $\mathscr{S}$ by first twisting the braiding:*

$$\left(Id \otimes T_{w_{p,q}} \otimes Id\right) : (n+p) \otimes (q+m) \to (n+q) \otimes (p+m)$$

6.6. **Block permutation of Lyndon words.** In classical shuffle algebras, the number of all possible block permutation of p's in $p^n \in S$ is trivially computed as $n!$. In case of diagonal braiding $\sigma\,(v \otimes w) = q_{vw} w \otimes v$, this is a bit more complicated. We address this with a lemma and a corollary on block permutation on Lyndon words.

Lemma 35 (Block permutation of two equal primes)**.** *Let $a \in S$ and $a = p^2$ its prime factorization. We denote the string decomposition of p as $\prod_{j=1}^{L} e_j$, where L is its length. Let w be in $\sum_2$, a subgroup of "block permutations" that permutes the p's among themselves. Whenever we speak of "block permutations", we will express w and T_w in terms of permutations and braidings that are applied to the "blocks". Let the braiding in $V \otimes V$ be given by $\sigma\,(e_i \otimes e_j) = q_{ij}\,(e_j \otimes e_i)$, and let $Q = \prod_{k,l \in [[1,L]]} q_{kl}$. Then either*

(1) *$w = Id$ and $T_w\,(v_a) = v_a$;*

(2) *$w = s_1$, $T_w = \sigma_1 = (1 \mapsto 2)$, and $T_w\,(v_a) = Qv_a$; or*

(3) $w = s_1$, $T_w = \sigma_1^{-1} = (2 \mapsto 1)$, *and* $T_w(v_a) = Q^{-1}v_a$ *(N/A).*

Proof. (1) Trivial. (2) We will first consider the case when the rightmost p is transposed to the left. In that case, T_w permutes each of the elements v_{x_j} composing the p's such that they interchange position. To do this, it is sufficient to permute each v_{x_j} from the rightmost p sequentially toward their respective place in the beginning of the construction, starting from the leftmost one. Each v_{x_j} of the rightmost p is thus transposed with one v_{x_k} for all $k \in [[1, L]]$ in the process. Thus, permutation of each v_{x_j} multiplies the construction by $\prod_{k\in[[1,L]]} q_{x_j x_k}$. Overall, for permutation of the p's we have $T_w(X_a) = QX_a$. (3) In case the rightmost p is transposed to the right, T_w is, as a whole and component-wise, an inverse of the the one in the first case, so $T_w(X_a) = Q^{-1}X_a$. □

Only cases 1 and 2 in Lemma 35 are applicable to shuffle multiplication or construction of bases in terms of Lyndon words by definition of shuffle multiplication (case 3 is not applicable).

Corollary 36 (Block permutation of n equal primes). *Let $a \in S$ and $a = p^n$ its prime factorization. Let w be in $\sum_n$, a subgroup of "block permutations" that permutes the p's among themselves. (Whenever we speak of "block permutations", we express w and T_w in terms of permutations and braidings that are applied to "blocks".) Let the braiding in $V \otimes V$ be given by $\sigma(e_i \otimes e_j) = q_{ij}(e_j \otimes e_i)$, and let $Q = \prod_{k,l\in[[1,L]]} q_{kl}$. Let T_w be the permutation of p's that is a lift of $(j_2, j_1, j_1 + 1, \cdots, j_2 - 1)$, where j_1 and j_2 correspond to p's in positions j_1 and j_2 respectively such that $j_1 < j_2$. Then, considering the Lemma 35 and that its item 3 is not applicable, we have*

$$T_w(v_a) = Q^{(j_2 - j_1)}v_a$$

Proof. Trivial, using the method of mathematical induction. □

6.7. **Bases in terms of Lyndon words.** For the case of quantum shuffle algebras, we need to only make a small adjustment to Proposition 18, replacing factorials by Mahonian numbers [4].

Proposition 37 (Bases of quantum shuffle algebras in terms of Lyndon words). *Let $a \in S(u)$ and $a = \prod_{i=1}^{s} p_i^{n_i}$ be its unique prime factorization. We define $X_a = \prod_{i=1}^{s} v_{p_i}^{n_i}$, where quantum multiplication is used between the terms of the form v_{p_i}. Then:*

1. *$X_a, a \in S(u)$ form a basis of $T(V)(u)$; and*
2. *the change of basis with respect to a is triangular, i.e. there exist $\alpha_{ab} \in k$ such that $X_a = \sum_{a \leq b} \alpha_{ab} v_b$;*
3. *setting for $1 \leq i \leq s$ $p_i = \prod_{j=1}^{l_i} x_{ij}$ and $Q_i = \prod_{k,l \in [[1,l_i]]} q_{x_k x_l}$, we have $\alpha_{aa} = \prod_{j=1}^{s} \left([n_j]_{Q_j}!\right) \neq 0$ for all $Q_i \in k$ being different from unity, or Q_i's indeterminate;*
4. *the X_a's, $a \in S$, form a linear basis of $T(V)$;*
5. *the v_p's, $p \in P$, form a polynomial basis for $T(V)$;*
6. *$X_a \cdot X_b = X_{a \cdot b}$ for $a, b \in S$.*

Proof. Let l_i be the length of p_i. By definition of shuffle multiplication, we have $X_a = \mathscr{B}_{(l_1,\cdots,l_s)}(v_a)$, where $v_a = \otimes_{i=1}^{s} v_{p_i}^{n_i}$.

First we will prove (2).

Indeed, we have $X_a = \mathscr{B}_{(l_1,\cdots,l_s)}(v_a) = \sum_{w \in \sum_{(l_1,\cdots,l_s)}} T_w(v_a)$. By Lemma 1, $T_w(a) \geq a$ for all $w \in \sum_{(l_1,\cdots,l_s)}$, so $X_a = \sum_{b \geq a} \alpha_{ab} v_b$, where $\alpha_{ab} = 0$ if $b \notin S(u)$.

Now we will prove (3).

We note that braiding in $V \otimes V$ is given by $\sigma(e_i \otimes e_j) = q_{ij}(e_i \otimes e_j)$.

We will rewrite $[n_j]_{Q_j}!$ as

$$[n_j]_{Q_j}! = \prod_{i=1}^{n_j} [i]_{Q_j} = \prod_{i=1}^{n_j} \frac{1 - Q_j^i}{1 - Q_j^1} = \prod_{i=1}^{n_j} \sum_{m=0}^{i-1} Q_j^m$$

We note that the expanded form of the Mahonian number formula

$$[n_j]_{Q_j}! = \prod_{i=1}^{n_j} \sum_{m=0}^{i-1} Q_j^m$$

is valid even if $Q_j = 1$.

From Theorem 14, we know that if $w \in \sum_{(l_1,\cdots,l_s)}$, then $T_w(a) = a$ if and only if w is in the subgroup $\sum_{n_1} \times \cdots \times \sum_{n_s}$ of "block permutations", permuting only p_i's among themselves for each i.

Therefore, it is sufficient to prove (3) for the case $s = 1$, i.e. $a = p_1^{n_1}$, with the decomposition $p_1 = \prod_{j=1}^{l_1} x_{1j}$.

We will use the method of mathematical induction.

Step 1. We will prove the formula

$$\alpha_{aa} = [n_1]_{Q_1}!$$

is valid for the case $n_1 = 1$. Indeed, then $\sum_{n_1} = \sum_1$ consists only of the identity element and

$$\alpha_{aa} = 1 = [n_1]_{Q_1}!$$

as in that case $[n_1]_{Q_1}! = \prod_{i=1}^{1} \sum_{m\in\{0\}} Q_1^m = 1$.

Step 2. We will prove that if the formula

$$\alpha_{aa} = [n_1]_{Q_1}!$$

is valid for $n_1 = r \in \mathbb{N}$, it is valid for $n_1 = r + 1$. We note the natural inclusion $\iota : B_r \to B_{r+1}$. For the permutations T_{w_1} of the first r p_1's among themselves

$$[r]_{Q_1}! = \prod_{i=1}^{r} \sum_{m=0}^{i-1} Q_1^m$$

In case of $n_1 = r + 1$, to obtain the permutations T_w of all p's among themselves, we take compositions $T_w = T_{w_2} \circ T_{w_1}$ of permutations T_{w_1} of the first r p_1's among themselves and the additional permutations T_{w_2} of the last p_i to each possible position relative to the first r p_i's. By

Lemma 35, if T_w permutes the p in position $r+1$ to position $1 \le i \le r$, then $T_w(X_a) = Q^{2t} X_a$. We note that T_w is then already written in terms of reduced expressions by construction. Adding these factors and multiplying by $[r]_{Q_1}!$, we get

$$T_w(X_a) = [r]_{Q_1}! \sum_{m=0}^{r} Q_1^m X_a = [r+1]_{Q_1}! X_a$$

and

$$\alpha_{aa} = [n_1]_{Q_1}!$$

is valid for $n_1 = r+1$.

By definition of a Mahonian number, assuming that $Q_1 \neq 1$,

$$\alpha_{aa} = [n_1]_{Q_1}! \neq 0$$

Now we will prove (1).

Consider the basis $\left\{ v_a | a = \prod_{j=1}^{k} x_j \in S(u), k \in \mathbb{N} \right\}$of $S(u)$. Since $\alpha_{aa} \neq 0$, the matrix (α_{ab}) has a nonzero determinant, and therefore $X_a, a \in S(u)$ form a basis of $T(V)(u)$.

Item (4) follows from Definition 7 with exclusion of $0 \in U$ (as it does not correspond to an element of V), i.e.

$$\oplus_{k=1}^{+\infty} V^{\otimes k} = \oplus_{0 \neq u \in U} T(V)(u)$$

Item (5) follows from (4) and from the fact that $X_a = \prod_{i=1}^{s} v_{p_i}^{n_i}$ can be expressed as a monomial in v_p's. Item (6) follows by definition of X_a: indeed, for $X_a = \prod_{i=1}^{s} v_{p_i}^{n_i}$ and $X_b = \prod_{i=1}^{s'} v_{p'_i}^{n'_i}$ we have $X_a \cdot X_b = \prod_{i=1}^{s} v_{p_i}^{n_i} \cdot \prod_{i=1}^{s'} v_{p'_i}^{n'_i}$, but that is $X_{a \cdot b}$ by definition. □

Notes on α_{aa}. As mentioned earlier, when constructing bases in terms of Lyndon words for quantum shuffle algebras and quantum group algebras, we only use σ and not σ^{-1}.

(1) If all $Q_i \in k$ are different from unity or indeterminate, then $[n_j]_{Q_j}!$ is the Mahonian number such that

$$[n]_q! = \prod_{j=1}^{n} \sum_{i=0}^{j-1} q^i = \prod_{j=1}^{n} \frac{1-q^j}{1-q}$$

(2) If some $Q_i \in k$ are unity, then we can't use the geometric series formula for Mahonian numbers $[n_j]_{Q_j}!$, and use the expanded form instead:

$$[n]_q! = \prod_{j=1}^{n} \sum_{i=0}^{j-1} q^i = \prod_{j=1}^{n} j = n!$$

Special alternative case. If we (1) use both σ and σ^{-1}, (2) consider both permutations and braidings in the sense of circular permutations and braidings and not in the sense of linear arrangements, (3) continue use the reduced expressions for permutations, (4) use symmetry considerations in case of an ambiguity, and (5) set $Q_i^2 = \prod_{k,l\in[[1,l_i]]} q_{x_k x_l}$, then

(1) If all $Q_i \in k$ are different from a square root of unity unity or indeterminate, then $[n_j]_{Q_j}!$ has the standard quantum group algebra definition

$$[n]_q! = \prod_{i=1}^{n} [i]_q = \prod_{i=1}^{n} \frac{q^i - q^{-i}}{q - q^{-1}} = \prod_{i=1}^{n} \sum_{m\in M_i} q_j^m$$

where $M_i = \{m| -i+1 \le m \le i-1 \wedge m+i-1 \in 2\mathbb{Z}\}$, i.e. $M_i = \{-i+1, -i+3, \cdots, i-1\}$.

(2) If some $Q_i \in k$ are square roots of unity, then we can't use the formula $[i]_q = \frac{q^i - q^{-i}}{q-q^{-1}}$, thus we have

$$[n]_q! = \prod_{i=1}^{n} \sum_{m\in M_i} q_j^m$$

7. Implementation in Mathematica

We have implemented a Wolfram Mathematica package with functions for quantum shuffle algebra and bases construction in terms of Lyndon words. Since using a generic totally ordered set X would have added a layer of abstraction that is not necessarily essential for our purposes, we have used $S = (\mathbb{N})$ for convenience.

7.1. **Function listings.** The package functions include:

(1) Comparison of two elements $a, b \in S$ using the total ordering on S;

```
QSARelation[x_List, y_List] := (
   Module[{rel = 0, i}, (
     For[i = 1, i <= Min[Length[x], Length[y]], i++,
      If[rel == 0 && x[[i]] < y[[i]], rel = -1];
      If[rel == 0 && x[[i]] > y[[i]], rel = 1];
      ];
     If[rel == 0 && Length[x] < Length[y], rel = 1];
     If[rel == 0 && Length[x] > Length[y], rel = -1];
     rel
     )]);
```

(2) Test of whether v_a ($a \in S$) is prime;

```
QSAIsPrime[x_List] := (
   Module[{ans = True, i1}, (
     If[Length[x] > 1, {
       For[i1 = 2, i1 <= Length[x], i1++, {
          If[QSARelation[x[[i1 ;; -1]], x] > -1, ans =
              False]
          }];
       }];
     ans
     )]);
```

(3) Finding the first prime of v_a ($a \in S$) in its unique prime factorization;

```
QSAFirstPrime[x_List] := (
   Module[{ans2 = {}, i2 = 1}, (
     While[
      i2 <= Length[x] &&
       QSAIsPrime[x[[1 ;; i2]]], {ans2 = x[[1 ;; i2]];
           i2++;}];
     ans2
     )]);
```

(4) Unique prime factorization (UPF) of v_a ($a \in S$);

```
QSAUniquePrimeFactorization[x_List] := (
   Module[{remx = x, upf = {}, nextprime}, (
     While[Length[remx] > 0, {
       nextprime = QSAFirstPrime[remx];
       AppendTo[upf, nextprime];
       If[Length[nextprime] < Length[remx],
        remx = remx[[Length[nextprime] + 1 ;; -1]], remx
            = {}];
       }];
     upf
     )]);
```

(5) Partition, permutation, and other auxiliary functions;

```
QSAV[x_List, xi_] := (
   Apply[TensorProduct, Map[Subscript[v, xi[[#]]] &, x]]
   );
QSASumV[x_List, xi_] := (
   Module[{sum = 0}, (
     AddFun[item1_] := (
       If[ListQ[item1[[1]]],
        sum = sum + item1[[2]] QSAV[item1[[1]], xi],
        sum = sum + QSAV[item1, xi]]
       );
     Map[AddFun, x];
     sum
     )]);
QSAIndexToObject[x_, xi_] := (
```

```
   If[ListQ[x[[1]]], Map[xi[[#]] &, x[[;; , 1]]], Map[xi
       [[#]] &, x]]
   );
QSALengthToPartitionIndex[L_List] := (
   Module[{M = {1}, CurM = 1, i3}, (
     For[i3 = 1, i3 <= Length[L], i3++, {
       CurM = CurM + L[[i3]];
       AppendTo[M, CurM];
       }];
     M
     )]);
Permutation[xlist_List, yitem_, aword_, qletter_: q] :=
    (
   Module[{plist, k, i}, (
     plist = {};
     For[k = 1, k <= Length[xlist], k++, {
       For[i = 1, i <= Length[xlist[[k, 1]]] + 1, i++, {
         AppendTo[
          plist, {Insert[xlist[[k, 1]], yitem, i],
           xlist[[k, 2]] Product[
             If[qletter === 1, 1, Subscript[qletter,
                aword[[jj]],
              aword[[Length[xlist[[k, 1]]] + 1]]]], {jj,
                  i,
              Length[xlist[[k, 1]]]}]}]
         }]
       }];
     plist
     )]);
PermuteList[zlist_List, aword_, qletter_: q] := (
   Module[{plist2, i1}, (
     plist2 = {};
     If[Length[zlist] == 1, plist2 = {{zlist, 1}}, {
       plist2 = {{{zlist[[1]]}, 1}};
       For[i1 = 2, i1 <= Length[zlist], i1++, {
         plist2 = Permutation[plist2, zlist[[i1]], aword
             , qletter]
         }];
```

```
        }];
      plist2
      )]);
Complement1[list1_List, list2_List] := (
   Module[{list3, list4 = {}, i}, (
      list3 = Complement[list1[[;; , 1]], list2[[;; ,
          1]]];
      For[i = 1, i <= Length[list1], i++, {
        If[MemberQ[list3, list1[[i, 1]]], AppendTo[list4,
             list1[[i]]]]
        }];
      list4
      )]);
QSAWordToLength[x_List] := (
   Map[Length[#] &, x]
   );
```

(6) Quantum shuffle multiplication $v_a \cdot v_b$ $(a, b \in S)$;

```
QSAGeneratePrimaryShuffles[L_List, aword_, qpar_: True]
    := (
   Module[{ShuffleList = {}, LL = Total[L],
      M = QSALengthToPartitionIndex[L], ShuffleListTemp =
           {}, i4}, (
      For[i4 = 1, i4 < Length[M], i4++, {
        AppendTo[ShuffleListTemp, Range[M[[i4]], M[[i4 +
            1]] - 1]];
        }];
      ShuffleList =
       PermuteList[ShuffleListTemp, Range[Length[
           ShuffleListTemp]],
        If[qpar, Q, 1]];
      For[i4 = 1, i4 <= Length[ShuffleList], i4++, {
        ShuffleList[[i4]] = {Flatten[ShuffleList[[i4,
            1]]],
            ShuffleList[[i4, 2]]};
        }];
      ShuffleList
      )]);
```

```
QSAGenerateShuffles[L_List, aword_, qpar_: True] := (
   Module[{ShuffleList = {}, LL = Total[L],
     M = QSALengthToPartitionIndex[L], i4, item1, plist0
        }, (
     ShuffleListTemp = PermuteList[Range[LL], aword, If[
        qpar, q, 1]];
     AddShuffle[item_] := (
       TestF = True;
       item1 = item[[1]];
       For[i4 = 1, i4 < Length[M], i4++, {
         If[
           Not[OrderedQ[
             Select[item1, # >= M[[i4]] && # < M[[i4 +
                 1]] &]]],
           TestF = False];
         }];
       If[TestF, AppendTo[ShuffleList, item]];
       );
     Map[AddShuffle, ShuffleListTemp];
     plist0 = QSAGeneratePrimaryShuffles[L, aword, qpar
        ];
     ShuffleList = Union[plist0, Complement1[ShuffleList
        , plist0]];
     ShuffleList
     )]);
QSAGenerateSecondaryShuffles[L_List, aword_, qpar_: True
    ] := (
   Complement1[QSAGenerateShuffles[L, aword, qpar],
    QSAGeneratePrimaryShuffles[L, aword, qpar]]
   );
QSAShuffleMultiplication[x_List] :=
  QSASumV[QSAGenerateShuffles[QSAWordToLength[x],
      Flatten[x]],
   Flatten[x]];
```

(7) Calculation of X_a ($a \in S$);

```
QSAX[x_, qpar_: True] :=
  QSASumV[QSAGenerateShuffles[
    QSAWordToLength[QSAUniquePrimeFactorization[x]], x,
       qpar], x];
```

(8) Expression of v_a ($a \in S$) in terms of Lyndon words (primes) .

```
QSAExpressInLyndonWords[x_] := (
   Module[{shuffles, shuffles1, lhs = {}, rhs = {}, eqns
       = {},
     rhs1 = {}, ia, avec, coeffarrays, sol}, (
     shuffles = QSAGenerateShuffles[L, x];
     shuffles1 = QSAIndexToObject[shuffles, a];
     For[ia = 1, ia <= Length[shuffles1], ia++, {
       AppendTo[lhs, Evaluate[Subscript[X, shuffles1[[ia
          ]]]]];
       AppendTo[rhs, QSAX[shuffles1[[ia]]]];
       AppendTo[rhs1, QSAX[shuffles1[[ia]], False]];
       AppendTo[eqns,
        Evaluate[Subscript[X, shuffles1[[ia]]]] ==
         QSAX[shuffles1[[ia]]]];
       }];
     avec = DeleteDuplicates[Flatten[rhs1, 1, Plus]];
     coeffarrays = Normal[CoefficientArrays[eqns, avec
        ]];
     sol = LinearSolve[coeffarrays[[2]], coeffarrays
        [[1]]];
     MapThread[#1 == #2 &, {avec, sol}]
     )]);
```

7.2. **Calculation examples.**

Example 38 (Unique prime factorization)**.** Consider $a = 18{\cdot}19{\cdot}4{\cdot}8{\cdot}5{\cdot}7$. It is written in Mathematica notation using an ordered list as $a = \{18, 19, 4, 8, 5, 7\}$. (Since in this section we are specifically speaking of the Mathematica package, we will disregard the usual notation of curly brackets for an unordered set and use it only for an ordered list in this section.)

Using the function `QSAUniquePrimeFactorization`, we obtain the UPF as an ordered list of two ordered lists $\{\{18\},\{19,4,8,5,7\}\}$, which means that $a = p_1 \cdot p_2$, where primes $p_1$and p_2 are $p_1 = 18$ and $p_2 = 19 \cdot 4 \cdot 8 \cdot 5 \cdot 7$.

Example 39 (Calculation of X_a $(a \in S)$)**.**

Consider again $a = \{18,19,4,8,5,7\}$ in the Mathematica notation for an ordered list. Using the function `QSAX`, we obtain for X_a that

$$
\begin{aligned}
X_a = v_{18} \otimes v_{19} \otimes v_4 \otimes v_8 \otimes v_5 \otimes v_7 + \\
+ Q_{1,2} v_{19} \otimes v_4 \otimes v_8 \otimes v_5 \otimes v_7 \otimes v_{18} + \\
+ q_{4,8} q_{8,5} q_{18,19} q_{19,4} v_{19} \otimes v_4 \otimes v_8 \otimes v_5 \otimes v_{18} \otimes v_7 + \\
+ q_{4,8} q_{18,19} q_{19,4} v_{19} \otimes v_4 \otimes v_8 \otimes v_{18} \otimes v_5 \otimes v_7 + \\
+ q_{18,19} q_{19,4} v_{19} \otimes v_4 \otimes v_{18} \otimes v_8 \otimes v_5 \otimes v_7 + \\
+ q_{18,19} v_{19} \otimes v_{18} \otimes v_4 \otimes v_8 \otimes v_5 \otimes v_7
\end{aligned}
$$

where $\sigma(v_i \otimes v_j) = q_{ij}(v_j \otimes v_i)$ for $i, j \in \mathbb{N}$ and, for conciseness purposes, $\sigma(v_i \otimes v_j) = Q_{ij}(v_j \otimes v_i)$ for $i, j \in P \subset S = (\mathbb{N})$.

Using the function `QSAPrimaryCoefficient`, we obtain $\alpha_{aa} = 1$.

Example 40 (Quantum shuffle multiplication)**.** Consider $b = \{5,10,10\}$ and $c = \{7,4,10\}$. Using the function `QSAShuffleMultiplication`, we obtain for quantum shuffle multiplication $v_b \cdot v_c$ the result in Figure 7.1.

Example 41 (Expression of v_a $(a \in S)$ in terms of X_c's $(c \in S$ and $c \geq a)$)**.** We again consider $a = \{18,19,4,8,5,7\}$. Solving the matrix equation, we express v_a and other summands in X_a in terms of X_c's $(c \geq a)$. The result is shown in Figure 7.2.

$$
\begin{aligned}
&\texttt{Shuffle multiplication } v_b v_c = q_{7,4}\, q_{10,4}\, q_{10,7}^2\, v_5\otimes v_7\otimes v_4\otimes v_{10}\otimes v_{10}\otimes v_{10} + \\
&\quad q_{4,10}\, q_{7,4}\, q_{10,4}\, q_{10,7}^2\, v_5\otimes v_7\otimes v_4\otimes v_{10}\otimes v_{10}\otimes v_{10} + q_{4,10}\, q_{7,4}\, q_{7,10}\, q_{10,4}\, q_{10,7}^2\, v_5\otimes v_7\otimes v_4\otimes v_{10}\otimes v_{10}\otimes v_{10} + \\
&\quad q_{7,4}\, q_{10,7}^2\, v_5\otimes v_7\otimes v_{10}\otimes v_4\otimes v_{10}\otimes v_{10} + q_{4,10}\, q_{7,4}\, q_{10,7}^2\, v_5\otimes v_7\otimes v_{10}\otimes v_4\otimes v_{10}\otimes v_{10} + q_{10,7}^2\, v_5\otimes v_7\otimes v_{10}\otimes v_{10}\otimes v_4\otimes v_{10} + \\
&\quad q_{7,4}\, q_{10,7}\, v_5\otimes v_{10}\otimes v_7\otimes v_4\otimes v_{10}\otimes v_{10} + q_{4,10}\, q_{7,4}\, q_{10,7}\, v_5\otimes v_{10}\otimes v_7\otimes v_4\otimes v_{10}\otimes v_{10} + q_{10,7}\, v_5\otimes v_{10}\otimes v_7\otimes v_{10}\otimes v_4\otimes v_{10} + \\
&\quad v_5\otimes v_{10}\otimes v_{10}\otimes v_7\otimes v_4\otimes v_{10} + q_{5,7}\, q_{7,4}\, q_{10,4}^2\, q_{10,7}^2\, v_7\otimes v_4\otimes v_5\otimes v_{10}\otimes v_{10}\otimes v_{10} + q_{4,10}\, q_{5,7}\, q_{7,4}\, q_{10,4}^2\, q_{10,7}^2\, v_7\otimes v_4\otimes v_5\otimes v_{10}\otimes v_{10}\otimes v_{10} + \\
&\quad q_{4,10}\, q_{5,7}\, q_{7,4}\, q_{7,10}\, q_{10,4}^2\, q_{10,7}^2\, v_7\otimes v_4\otimes v_5\otimes v_{10}\otimes v_{10}\otimes v_{10} + Q_{1,2}\, v_7\otimes v_4\otimes v_{10}\otimes v_5\otimes v_{10}\otimes v_{10} + q_{5,7}\, q_{7,4}\, q_{10,4}\, q_{10,7}^2\, v_7\otimes v_5\otimes v_4\otimes v_{10}\otimes v_{10}\otimes v_{10} + \\
&\quad q_{4,10}\, q_{5,7}\, q_{7,4}\, q_{10,4}\, q_{10,7}^2\, v_7\otimes v_5\otimes v_4\otimes v_{10}\otimes v_{10}\otimes v_{10} + q_{4,10}\, q_{5,7}\, q_{7,4}\, q_{7,10}\, q_{10,4}\, q_{10,7}^2\, v_7\otimes v_5\otimes v_4\otimes v_{10}\otimes v_{10}\otimes v_{10} + \\
&\quad q_{5,7}\, q_{7,4}\, q_{10,7}^2\, v_7\otimes v_5\otimes v_{10}\otimes v_4\otimes v_{10}\otimes v_{10} + q_{4,10}\, q_{5,7}\, q_{7,4}\, q_{10,7}^2\, v_7\otimes v_5\otimes v_{10}\otimes v_4\otimes v_{10}\otimes v_{10} + q_{5,7}\, q_{10,7}^2\, v_7\otimes v_5\otimes v_{10}\otimes v_{10}\otimes v_4\otimes v_{10}
\end{aligned}
$$

FIGURE 7.1. Result in Mathematica for quantum shuffle multiplication $v_b \cdot v_c$ in Example 40.

$$\{v_{18}\otimes v_{19}\otimes v_4\otimes v_8\otimes v_5\otimes v_7 == -X_{\{18,19,4,8,5,7\}} + X_{\{19,18,4,8,5,7\}}\, q_{18,19} + X_{\{19,4,18,8,5,7\}}\, q_{18,19}\, q_{19,4} + X_{\{19,4,8,18,5,7\}}\, q_{4,8}\, q_{18,19}\, q_{19,4} + X_{\{19,4,8,5,18,7\}}\, q_{4,8}\, q_{8,5}\, q_{18,19}\, q_{19,4} + X_{\{19,4,8,5,7,18\}}\, Q_{1,2},\ v_{19}\otimes v_4\otimes v_8\otimes v_5\otimes v_7\otimes v_{18} == -X_{\{19,4,8,5,7,18\}},$$

$$v_{19}\otimes v_4\otimes v_8\otimes v_5\otimes v_{18}\otimes v_7 == -X_{\{19,4,8,5,18,7\}},\ v_{19}\otimes v_4\otimes v_8\otimes v_{18}\otimes v_5\otimes v_7 == -X_{\{19,4,8,18,5,7\}},$$

$$v_{19}\otimes v_4\otimes v_{18}\otimes v_8\otimes v_5\otimes v_7 == -X_{\{19,4,18,8,5,7\}},\ v_{19}\otimes v_{18}\otimes v_4\otimes v_8\otimes v_5\otimes v_7 == -X_{\{19,18,4,8,5,7\}}\}$$

FIGURE 7.2. Result in Mathematica for expression of v_a in terms of Lyndon words in Example 41.

8. Quantum group algebras II

8.1. **Idea and underlying principles.** We can adapt the construction of bases of quantum shuffle algebras in terms of Lyndon words to quantum group algebras by noting the following:

(1) Braiding is defined on $T(V)$ for a $U_q(\mathfrak{g})$-module V by the universal R-matrix and on $S_\sigma\left(M^R\right)$ by an $N \times N$ matrix (q_{ij}).
(2) Specifying a $U_q(\mathfrak{g})$-module $T(V)$, where $V = \mathfrak{g}$, we can define an associative structure on $T(V)$, for $x_1, \cdots, x_n$ in V,

$$(x_1 \otimes \cdots \otimes x_p) \cdot (x_{p+1} \otimes \cdots \otimes x_n) = \sum_{w \in \sum_{p,n-p}} T_w (x_1 \otimes \cdots \otimes x_n)$$

Proof of the associativity is the same as in case of quantum shuffle algebras.
(3) If case the quantum group parameter q is unity, the R-matrix is $R = 1 \otimes 1$, and braiding is trivial: $\sigma(v \otimes w) = w \otimes v$.
(4) One should keep in mind that generators of $U_q(\mathfrak{g})$ are not the linear basis of V.
(5) Failing to adapt the bases construction method for quantum group algebras as a whole, we will use the same idea and principles for subalgebras of quantum group algebras.

8.2. **Braiding and the universal R-matrix.** If $v \in V$ and $w \in W$, then

$$\sigma(v \otimes w) = \tau(R(v \otimes w))$$

where τ is the flip $\tau : v \otimes w \mapsto w \otimes v$ and R is the universal R-matrix of the form [13, p. 175]

$$R = \sum_i s_i \otimes t_i$$

i.e.

$$\sigma(v \otimes w) = \sum_i t_i w \otimes s_i v$$

Proposition 42 (Block permutation of two equal primes)**.** *Let $a \in S$ and $a = p^2$ its prime factorization. We denote the string decomposition of p as $\prod_{j=1}^{L} e_j$, where L is its length. Let w be in $\sum_2$, a subgroup of "block permutations" that permutes the p's among themselves. Let the braiding in $V \otimes V$ be given by $\sigma(e_i \otimes e_j) = \tau(R(e_i \otimes e_j))$, where R is the universal R-matrix. Then either*

(1) *$w = Id$ and $T_w(v_a) = v_a$;*

(2) *$w = s_1$, $T_w = \sigma_1 = (1 \mapsto 2)$, and*

$$T_w(v_a) = \left(\sum_{i_1,\cdots,i_L} t_{i_1}\cdots t_{i_L}\right) v_p \otimes \left(\sum_{i_1,\cdots,i_L} s_{i_1}\cdots s_{i_L}\right) v_p;$$

(3) *$w = s_1$ and $T_w = \sigma_1^{-1} = (2 \mapsto 1)$ (N/A).*

Proof. This is trivial application of the expression of the universal R-matrix in terms of elements s_i and t_i to the framework we have developed above. □

To apply the same method of construction of bases in terms of Lyndon words for the quantum group algebra as for quantum shuffle algebras, we need the universal R-matrix to be diagonal, which corresponds to diagonal braiding. We will assume that this is the case. For that, it is sufficient that all t_i and s_i in the expression for the universal R-matrix are elements of the Cartan subalgebra.

For a highest weight module of a quantum group algebra, it is useful to write the weight vector expression as

$$k_\lambda \cdot v = d_\lambda v = c_\lambda q^{(\lambda,v)} v$$

where ν is an element of the weight lattice. [11, p. 72]

Accordingly, we consider the specific form of the diagonal universal R-matrix

$$R = q^{\sum_i d_{ij} \tilde{k}_{\lambda_i} \otimes \tilde{k}_{\mu_i}}$$

where Cartan subalgebra generators k_i are formally identified with $q^{\tilde{k}_i}$ [15]. It is one of the possible functions f as described, for example, in [11, ch. 3,7]. Setting $q^{\tilde{k}_{\lambda_i}} e_j = q^{\alpha_{ij}} e_j$, and $q^{\tilde{k}_{\mu_i}} e_j = q^{\beta_{ij}} e_j$, it acts on an element $v \otimes w \in V \otimes W$ as

$$R \cdot (v \otimes w) = q^{\sum_k d_{ij} \alpha_{ki} \beta_{kj}} (v \otimes w)$$

We now state the following trivial propositions:

Proposition 43 (Diagonal braiding on $V \otimes V$)**.**

(1) *If all elements t_i and s_i in the expression $R = \sum_i s_i \otimes t_i$ of the universal R-matrix are elements of the Cartan subalgebra, then braiding in $V \otimes V$ is diagonal (i.e. given by $\sigma(e_i \otimes e_j) = q_{ij}(e_j \otimes e_i)$).*

(2) *If additionally V is a highest weight module, $q^{\tilde{k}_{\lambda_i}} e_j = q^{\alpha_{ij}} e_j$, and $q^{\tilde{k}_{\mu_i}} e_j = q^{\beta_{ij}} e_j$ for all i and j, then*

$$\sigma(e_i \otimes e_j) = q^{\sum_k d_{ij} \alpha_{ki} \beta_{kj}} (e_j \otimes e_i)$$

8.3. **Bases in terms of Lyndon words.**

Proposition 44 (Block permutation of two equal primes in case of a diagonal universal R-matrix)**.** *Let $a \in S$ and $a = p^2$ its prime factorization. We denote the string decomposition of p as $\prod_{j=1}^{L} e_j$, where L is its length. Let w be in $\sum_2$, a subgroup of "block permutations" that permutes the p's among themselves. Let the braiding in $V \otimes V$ be given by $\sigma(e_i \otimes e_j) = q_{ij}(e_j \otimes e_i)$, and let $Q = \prod_{k,l \in [[1,L]]} q_{kl}$. Then either*

(1) *$w = Id$ and $T_w(v_a) = v_a$;*

(2) *$w = s_1$, $T_w = \sigma_1 = (1 \mapsto 2)$, and $T_w(v_a) = Q v_a$;*

(3) *$w = s_1$, $T_w = \sigma_1^{-1} = (2 \mapsto 1)$, and $T_w(v_a) = Q^{-1} v_a$ (N/A).*

Assuming that the universal R-matrix is diagonal (i.e. we have diagonal braiding) for quantum group algebra (or its subalgebra), we can apply Proposition 37 used for quantum shuffle algebras to the quantum group algebra (resp. its subalgebra) verbatim. Even though the proposition's formulation is the same as that of Proposition 37 (as can be expected), will restate it here for text structure and reference purposes.

Proposition 45 (Bases of quantum group algebras in terms of Lyndon words)**.** *Let $a \in S(u)$ and $a = \prod_{i=1}^{s} p_i^{n_i}$ be its unique prime factorization. We define $X_a = \prod_{i=1}^{s} v_{p_i}^{n_i}$, where quantum multiplication is used between the terms of the form v_{p_i}. Then:*

1. *$X_a, a \in S(u)$ form a basis of $T(V)(u)$; and*
2. *the change of basis with respect to a is triangular, i.e. there exist $\alpha_{ab} \in k$ such that $X_a = \sum_{a \leq b} \alpha_{ab} v_b$;*
3. *setting for $1 \leq i \leq s$ $p_i = \prod_{j=1}^{l_i} x_{ij}$ and $Q_i = \prod_{k,l \in [[1,l_i]]} q_{x_k x_l}$, we have $\alpha_{aa} = \prod_{j=1}^{s} \left([n_j]_{Q_j}!\right) \neq 0$ for all $Q_i \in k$ being different from unity, or Q_i's indeterminate;*
4. *the X_a's, $a \in S$, form a linear basis of $T(V)$;*
5. *the v_p's, $p \in P$, form a polynomial basis for $T(V)$;*
6. *$X_a \cdot X_b = X_{a \cdot b}$ for $a, b \in S$.*

Notes on α_{aa}. As mentioned earlier, when constructing bases in terms of Lyndon words for quantum shuffle algebras and quantum group algebras, we only deal with σ and not σ^{-1}.

1. If all $Q_i \in k$ are different from unity or indeterminate, then $[n_j]_{Q_j}!$ is the Mahonian number such that

$$[n]_r! = \prod_{j=1}^{n} \sum_{i=0}^{j-1} r^i = \prod_{j=1}^{n} \frac{1 - r^j}{1 - r}$$

2. If some $Q_i \in k$ are unity, then can't use the geometric series formula and have for respective Mahonian numbers $[n_j]_{Q_j}!$ that

$$[n]_r! = \prod_{j=1}^{n} \sum_{i=0}^{j-1} r^i = \prod_{j=1}^{n} j = n!$$

(3) If the quantum group parameter q is unity, then we have a nondeformed universal enveloping algebra module, and all Q_i's are unity.

(4) The case of q being a root of unity (other than $q = 1$) has to be addressed separately.

Algorithm for bases construction in terms of Lyndon words. Similarly to classical quantum algebras and the general case of quantum group algebras, Proposition 45 implicitly gives a method of bases construction in terms of Lyndon words. In Example 41, we have expressed one $v_a, a \in S$ in terms of X_c's, which is equivalent to expression as a polynomial of v_p's, where $p \in P$. Suppose that we have a linear basis of $T(V)$ or its subspace as a set of v_a's, where $a \in S$. Then we can express that basis using a polynomial basis of Lyndon words as follows: (1) following Proposition 45, express each v_a in the linear basis of $T(V)$ using shuffle multiplication in terms of primes $v_p, p \in P$; and (2) take the union of the sets of applicable v_p's, remembering to delete any duplicates during the process.

$U_q(\mathfrak{g})$ **structure and quantum shuffle multiplication.** The quantum shuffle multiplication is based on the natural representation of the braid group on quantum group algebra on $T(V)$, where V is a quantum group algebra module. It is an additional structure that is, as a multiplication, not compatible with the quantum group algebra's coproduct. If we wish, can can define an additional coproduct on the quantum group algebra that is compatible with the quantum shuffle multiplication – for example, by using the approach of universal construction in the braid category.

Application of the Mathematica function package. Continuing to consider the case where the braiding is given in $V \otimes V$ by $\sigma(e_i \otimes e_j) = q_{ij}(e_j \otimes e_i)$, where V is a quantum group algebra module, we can directly apply the Mathematica program discussed above to quantum shuffle multiplication and construction of bases in terms of Lyndon words for quantum group algebras.

Scope of applicability to quantum group algebras. The diagonal universal R-matrix condition is quite restrictive, and we expect it to apply only to exceptional types of quantum group algebras. This can be seen from the expression for the standard universal R-matrix for $U_q(\mathfrak{g})$ with assumption that $\mathfrak{g}$ is of finite type:

$$R_q = exp\left(q\sum_{i,j}\left(B^{-1}\right)_{ij} k_i \otimes k_j\right)\prod_{\beta} exp_{q_\beta}\left[\left(1-q_\beta^{-2}\right)e_\beta \otimes f_\beta\right]$$

where the product is over all the positive roots of $\mathfrak{g}$, and the order of the terms is such that β_r appears to the left of β_s if $r \geq s$. [6, Theorem 8.3.9]

Applicability to positive and negative parts of quantum group algebras. Continuing to assume that $\mathfrak{g}$ is if finite type, the positive part $U_q^+(\mathfrak{g})$ of the quantum group algebra is a Nichols algebra. Restriction of the universal R-matrix of $U_q(\mathfrak{g})$ to $U_q^+(\mathfrak{g})$ satisfies the diagonality condition, i.e. the braiding in $U_q^+(\mathfrak{g})$ is diagonal [2, 30]. Fundamental results on this include [25] and, in form an implicit discussion, [18]. This diagonal braiding is given by $q_{ij} = q^{d_i a_{ij}}$ [25, 2, 30]. Moreover, keeping in mind that the universal R-matrix and the corresponding braiding are not unique, the results of constructing bases of $U_q^+(\mathfrak{g})$ in terms of Lyndon words as described in this section and in [25] are equivalent. Same applies to the negative part $U_q^-(\mathfrak{g})$.

Specialized and non-specialized quantum group algebras. The non-restricted specialization of $U_q(\mathfrak{g})$ is obtained by using a specific value of q instead of the indeterminate. For q not being a root of unity, the restricted and non-restricted specializations coincide. While the standard universal R-matrix obtained for a non-specialized $U_q(\mathfrak{g})$ using [6, Theorem 8.3.9] gives a well-defined endomorphism for the specialized case when q is not a root of unity, it does not give an element of $U_q \otimes U_q$ due to fractional powers of q and due to the expression being an infinite sum. This issue is not substantial for our purposes and can be addressed as described in [6, pp. 327-331].

8.4. **A PBW-type basis analogy for $T(V)$.** Parts (4) and (5) of Proposition 45 can be restated to resemble a PBW-type bases theorem.

Definition 46 ($(T^j)^i$ notation)**.** Define $(T^j)^i$ as $(j \mapsto j - i) \in B_n$ that permutes the $p \in P$ (or respective $v_p \in T(V)$) from position j in a (v_a resp.) to position $j - i$. In the same context, let $I = [[1, n]]$.

Corollary 47 (A PBW-type basis analogy for $T(V)$)**.**

(1) *The set of elements of $T(V)(u)$ of the form $T^{\gamma_1} \cdots T^{\gamma_k} v_a$ where $a \in S(u)$, with γ_j being a monotonically increasing sequence of k elements of I, i.e.*

$$\gamma_1 \leq \cdots \leq \gamma_k$$

and with k any non-negative integer, is a linear basis of $T(V)(u)$.

(2) *The set of elements of $T(V)$ of the form $T^{\gamma_1} \cdots T^{\gamma_k} v_p$ where $p \in P$, with γ_j being a monotonically increasing sequence of k elements of I, i.e.*

$$\gamma_1 \leq \cdots \leq \gamma_k$$

and with k any non-negative integer, is a polynomial basis of $T(V)$.

8.5. **Case of q as a root of unity.**

8.5.1. *Restricted and non-restricted specializations.* For a quantum group $U_q(\mathfrak{g})$, there are two ways to specialize the group parameter q to a root of unity ϵ: non-restricted and restricted, resulting in different algebras $U_\epsilon(q)$ and $U_\epsilon^{res}(q)$ respectively. It is usually assumed that ϵ is the primitive lth root of unity, where l is odd and $l > d_i$ for all i (d_i are the coprime positive integers such that the matrix $(d_i a_{ij})$ is symmetric). Both $U_\epsilon(\mathfrak{g})$ and $U_\epsilon^{res}(\mathfrak{g})$ are not quasitriangular and do not have a universal R-matrix. [6, p. 327-329]

(1) However, it is possible to obtain matrix-valued solutions of the quantum Yang-Baxter equation (QYBE) on representations of $U_\epsilon(\mathfrak{g})$, where the tensor product is commutative up to an isomorphism. In this subcase, we can directly apply the method of constructing bases in terms of Lyndon words to the solution of the QYBE.

(2) This method of obtaining matrix-valued solutions of QYBE is specific to $U_\epsilon(\mathfrak{g})$ and is not applicable to $U_\epsilon^{res}(\mathfrak{g})$.

8.5.2. *Solutions of QYBE in $U_\epsilon(\mathfrak{g})$.* The following proposition is useful for obtaining matrix-valued QYBE solutions in the non-restricted case of $U_\epsilon(\mathfrak{g})$.

Proposition 48 (Solutions of QYBE in $U_\epsilon(\mathfrak{g})$ [6, pp. 349-359])**.** *Let $\{V(u)\}_{u\in V}$ be a family of representations of a Hopf algebra A, all with the same underlying vector space V and parametrized by the elements v of some set $\mathcal{V}$, such that:*

for all $v_1, v_2 \in \mathcal{V}$, there is an isomorphism of representations

$$I(v_1, v_2) : V(v_1) \otimes V(v_2) \to V(v_2) \otimes V(v_1)$$

for all $v_1, v_2, v_3 \in \mathcal{V}$, the only isomorphisms of representations

$$V(v_1) \otimes V(v_2) \otimes V(v_3) \to V(v_1) \otimes V(v_2) \otimes V(v_3)$$

are the scalar multiples of identity.

Then, if $R = \tau \circ I$, where τ is the interchange of the factors in the tensor product,

$$R_{12}(v_1, v_2) R_{13}(v_1, v_3) R_{23}(v_2, v_3) = cR_{23}(v_2, v_3) R_{13}(v_1, v_3) R_{12}(v_1, v_2)$$

where c is a scalar (possibly depending on v_1, v_2, and v_3).

Since the intertwiners I are only determined up to a scalar multiple, it may be possible to normalize them so that $c = 1$.

9. Discussion

We have derived a method to construct bases of positive (negative) parts $U_q^+(\mathfrak{g})$ ($U_q^-(\mathfrak{g})$ resp.) of quantum group algebras using Lyndon words (primes). We have examined the case of quantum parameter q being a root of unity. A secondary result is that we have developed a Wolfram Mathematica package that performs a number of relevant operations, including quantum shuffle multiplication and construction of bases in terms of Lyndon words for quantum group algebras.

We have founded the bases construction method on classical shuffle algebra [24] and quantum shuffle algebra [25] theory. In this work, we have attempted to balance independent perspective and coherence with these primary references. We found that our end result for quantum group algebras agrees with that in [25]. On the one hand, this limits the novelty of our work, but on the other, it validates it.

The Mathematica package's functionality is limited to the concrete case of $X = \mathbb{N}$, but can be easily extended to the general case of any totally ordered set. The memory requirement of its current implementation is roughly proportional to the factorial of the length of a word, and all calculations are done in random-access memory. To address this issue, one can optimize the source code, perform the calculations piecewise, and/or store interstitial calculation results in a file.

Interesting directions for more specific research include (1) determining whether our bases construction method may have broader applications for specific types of Kac-Moody algebra $\mathfrak{g}$ than as detailed here,

(2) fully developing the approach toward diagonal braiding using the

$$T_w(v_a) = \left(\sum_{i_1,\cdots,i_L} t_{i_1}\cdots t_{i_L}\right) v_p \otimes \left(\sum_{i_1,\cdots,i_L} s_{i_1}\cdots s_{i_L}\right) v_p$$

expression, and (3) researching the case in which q is a root of unity in more depth, including cyclic representations of $U_\epsilon(\mathfrak{g})$. With some extension of functionality, performance optimization, and thorough documentation, the Mathematica package can be shared publicly by means of a repository and accessed by practitioners.

This work details theory of shuffle algebras and bases construction in terms of Lyndon words (primes) for classical and quantum shuffle algebras. We have applied this theory to positive (negative) parts of quantum group algebras, including the case of quantum parameter q being a root of unity.

This thesis (mémoire de stage), along with the Mathematica package, may be useful to graduate students and researchers familiarizing themselves with the topic.

References

1. E. Abe, *Hopf algebras*, vol. 74., Cambridge University Press, Cambridge; New York, 1980.
2. N. Andruskiewitsch and F. Dumas, *On the automorphisms of uq+(g)*, Quantum Groups (B. Enriquez, ed.), IRMA Lectures in Mathematics and Theoretical Physics, vol. 12, European Math Society, 2008, pp. 107–133.
3. N. Andruskiewitsch and H.-J. Schneider, *Finite quantum groups and cartan matrices*, Advances in Mathematics **154** (2000), no. 1, 1–45.
4. M. Bona, *Combinatorics of permutations*, 2nd ed., CRC Press, Boca Raton, FL, 2012.
5. N. Bourbaki, *Groupes et algebres de Lie*, vol. 1349, Hermann, Paris, 1960.
6. V. Chari and A. Pressley, *A guide to quantum groups*, 1st paperback (with corrections) ed., Cambridge University Press, Cambridge, 1995.
7. D. F. de Chela and J. A. Green, *Quantum symmetric algebras*, Algebras and Representation Theory **4** (2001), no. 1, 55–76.

8. ______, *Quantum symmetric algebras II*, Journal of Algebra **269** (2003), no. 2, 610–631.
9. V. Drinfel'd, *Quantum groups*, Proceedings of the ICM (Rhode Island) (A. Gleason, ed.), AMS, 1987, pp. 798–820.
10. P. Etingof, V. Ginzburg, N. Guay, D. Hernandez, and A. Savage, *Twenty-five years of representation theory of quantum groups*, August 2011.
11. J. C. Jantzen, *Lectures on quantum groups*, American Mathematical Society, 1995.
12. R.-Q. Jian, M. Rosso, and J. Zhang, *Quantum quasi-shuffle algebras*, Letters in Mathematical Physics **92** (2010), no. 1, 1–16.
13. C. Kassel, *Quantum groups*, Springer New York, 1995.
14. C. Kassel and V. G. Turaev, *Braid groups*, vol. 247., Springer, New York, 2008.
15. S. M. Khoroshkin and V. N. Tolstoy, *The uniqueness theorem for the universal R-matrix*, Letters in Mathematical Physics **24** (1992), no. 3, 231–244.
16. B. Leclerc, *Dual canonical bases, quantum shuffles and q-characters*, Mathematische Zeitschrift **246** (2004), no. 4, 691–732.
17. G. Lusztig, *Quantum groups at roots of 1*, Geometriae Dedicata **35** (1990), no. 1-3, 90–113.
18. ______, *Introduction to quantum groups*, 1. aufl. ed., Birkhaeuser, Boston, 2010.
19. R. C. Lyndon, *On Burnside's problem*, Transactions of the American Mathematical Society **77** (1954), no. 2, 202–215.
20. S. Majid, *Doubles of quasitriangular Hopf algebras*, Communications in Algebra **19** (1991), no. 11, 3061–3073.
21. H. Matsumoto, *Generateurs et relations des groupes de weyl generalises*, C.R. Acad. Sci. **259** (1964), 3419–3422.
22. S. Montgomery, *Hopf algebras and their actions on rings*, CBMS Regional Conference Series in Mathematics, vol. 82, American Mathematical Society, Providence, RI, 1993.
23. W. D. Nichols, *Bialgebras of type one*, Communications in Algebra **6** (1978), no. 15, 1521–1552.
24. 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.
25. M. Rosso, *Quantum groups and quantum shuffles*, Inventiones mathematicae **133** (1998), no. 2, 399–416.

26. Steven Sam and Peter Tingley, *Quantum groups, combinatorics and geometry seminar*, Lecture notes, Department of Mathematics and Statistics, Loyola University Chicago, Chicago, IL, Spring 2011.
27. W. A. Schnizer, *Roots of unity: Representations of quantum groups*, Communications in Mathematical Physics **163** (1994), no. 2, 293–306.
28. B. Singh, *Quantum groups at root of unity*, http://goo.gl/GU8rkv.
29. M. E. Sweedler, *Hopf algebras*, W. A. Benjamin, New York, 1969.
30. M. Takeuchi, *A survey on Nichols algebras*, Algebraic structures and their representations: XV Coloquio Latinoamericano de Algebra, Cocoyoc, Morelos, Mexico, July 20-26, 2003 (Providence, RI) (J.A. de la Pena, E. Vallejo, and N. Atakishiyev, eds.), Contemporary Mathematics, vol. 376, American Mathematical Society, 2005, pp. 105–117.
31. P. Tingley, *Constructing the R-matrix from the quasi R-matrix.*, goo.gl/H31ICL.
32. P. Tingley, *A formula for the R-matrix using a system of weight preserving endomorphisms*, Representation Theory of the American Mathematical Society **14** (2010), no. 13, 435–445.
33. S. L. Woronowicz, *Differential calculus on compact matrix pseudogroups (quantum groups)*, Communications in Mathematical Physics **122** (1989), no. 1, 125–170.
34. D. N. Yetter, *Quantum groups and representations of monoidal categories*, Mathematical Proceedings of the Cambridge Philosophical Society **108** (1990), no. 2, 261–290.

Faculté de Mathématiques, Université Pierre & Marie Curie (Paris VI), 4 place Jussieu, 75252 Paris CEDEX 05, France. Also at Michigan State University, East Lansing, MI 48824, USA, and at Institut für Kernphysik, Forschungszentrum Jülich, Germany.