Advances in Mathematics 439 (2024) 109482

Contents lists available at ScienceDirect

Advances in Mathematics

journal homepage: www.elsevier.com/locate/aim

Quantum loop groups and shuffle algebras via Lyndon words

Andrei Neguț [a,b,*], Alexander Tsymbaliuk [c]

[a] *MIT, Department of Mathematics, Cambridge, MA, USA*
[b] *Simion Stoilow Institute of Mathematics, Bucharest, Romania*
[c] *Purdue University, Department of Mathematics, West Lafayette, IN, USA*

ARTICLE INFO

Article history:
Received 8 March 2022
Received in revised form 13 November 2023
Accepted 23 December 2023
Available online xxxx
Communicated by A. Kleshchev

Keywords:
Quantum loop group
Shuffle algebra
Lyndon word
Convex order
Wheel condition

ABSTRACT

We study PBW bases of the untwisted quantum loop group $U_q(L\mathfrak{g})$ (in the Drinfeld new presentation) using the combinatorics of loop words, by generalizing the treatment of [26,27,39] in the finite type case. As an application, we prove that Enriquez' homomorphism [9] from the positive half of the quantum loop group to the trigonometric degeneration of Feigin-Odesskii's shuffle algebra [13] associated to $\mathfrak{g}$ is an isomorphism.

1. Introduction

1.1. Let $\mathfrak{g}$ be the Kac-Moody Lie algebra corresponding to a root system of finite type. Associated with a decomposition of the set of roots $\Delta = \Delta^+ \sqcup \Delta^-$, there exists a triangular decomposition:

$$\mathfrak{g} = \mathfrak{n}^+ \oplus \mathfrak{h} \oplus \mathfrak{n}^- \tag{1.1}$$

* Corresponding author.
E-mail addresses: andrei.negut@gmail.com (A. Neguț), sashikts@gmail.com (A. Tsymbaliuk).

https://doi.org/10.1016/j.aim.2023.109482
0001-8708/

where:

$$\mathfrak{n}^+ = \bigoplus_{\alpha \in \Delta^+} \mathbb{Q} \cdot e_\alpha \tag{1.2}$$

and analogously for $\mathfrak{n}^-$. The elements e_α will be called <u>root vectors</u>. Formula (1.1) induces a triangular decomposition[1] of the universal enveloping algebra:

$$U(\mathfrak{g}) = U(\mathfrak{n}^+) \otimes U(\mathfrak{h}) \otimes U(\mathfrak{n}^-) \tag{1.3}$$

Then the PBW theorem asserts that a linear basis of $U(\mathfrak{n}^+)$ is given by the products:

$$U(\mathfrak{n}^+) \ = \bigoplus_{\gamma_1 \geq \dots \geq \gamma_k \in \Delta^+}^{k \in \mathbb{N}} \mathbb{Q} \cdot e_{\gamma_1} \dots e_{\gamma_k} \tag{1.4}$$

and analogously for $U(\mathfrak{n}^-)$, for any total order of the set of positive roots Δ^+ (the set $\mathbb{N}$ will be assumed to include 0). The root vectors (1.2) can be normalized so that we have:

$$[e_\alpha, e_\beta] = e_\alpha e_\beta - e_\beta e_\alpha \in \mathbb{Z}^* \cdot e_{\alpha+\beta} \tag{1.5}$$

whenever α, β and $\alpha + \beta$ are positive roots. Thus we see that formula (1.5) provides an algorithm for constructing, up to scalar multiple, all the root vectors (1.2) inductively starting from $e_i = e_{\alpha_i}$, where $\{\alpha_i\}_{i \in I} \subset \Delta^+$ are the simple roots of $\mathfrak{g}$. The upshot is that all the root vectors e_α, and with them the PBW basis (1.4), can be read off from the combinatorics of the root system.

1.2. The quantum group $U_q(\mathfrak{g})$ is a q-deformation of the universal enveloping algebra $U(\mathfrak{g})$, and we will focus on emulating the features of the previous Subsection. For one thing, there exists a triangular decomposition analogous to (1.3):

$$U_q(\mathfrak{g}) = U_q(\mathfrak{n}^+) \otimes U_q(\mathfrak{h}) \otimes U_q(\mathfrak{n}^-) \tag{1.6}$$

and there exists a PBW basis analogous to (1.4):

$$U_q(\mathfrak{n}^+) \ = \bigoplus_{\gamma_1 \geq \dots \geq \gamma_k \in \Delta^+}^{k \in \mathbb{N}} \mathbb{Q}(q) \cdot e_{\gamma_1} \dots e_{\gamma_k} \tag{1.7}$$

The q-deformed root vectors $e_\alpha \in U_q(\mathfrak{n}^+)$ are defined via Lusztig's braid group action, which requires one to choose a reduced decomposition of the longest element in the Weyl group of type $\mathfrak{g}$. It is well-known ([34]) that this choice precisely ensures that the order $\geq$

[1] Given subalgebras $\{A_k\}_{k=1}^N$ of an algebra A, the decomposition $A = A_1 \otimes \dots \otimes A_N$ will mean that the multiplication in A induces a vector space isomorphism $m \colon A_1 \otimes \dots \otimes A_N \xrightarrow{\sim} A$.

on Δ^+ is convex, in the sense of Definition 2.19. Moreover, the q-deformed root vectors satisfy the following q-analogue of relation (1.5), where α, β and $\alpha + \beta$ are any positive roots that satisfy $\alpha < \alpha + \beta < \beta$ as well as the minimality property (4.15):

$$[e_\alpha, e_\beta]_q = e_\alpha e_\beta - q^{(\alpha,\beta)} e_\beta e_\alpha \in \mathbb{Z}[q, q^{-1}]^* \cdot e_{\alpha+\beta} \tag{1.8}$$

where $(\cdot, \cdot)$ denotes the scalar product corresponding to the root system of type $\mathfrak{g}$. As in the Lie algebra case, we conclude that the q-deformed root vectors can be defined (up to scalar multiple) as iterated q-commutators of $e_i = e_{\alpha_i}$ (with $i \in I$), using the combinatorics of the root system and the chosen convex order on Δ^+.

1.3. There is a well-known incarnation of $U_q(\mathfrak{n}^+)$ due to Green [15], Rosso [38], and Schauenburg [40] in terms of quantum shuffles:

$$U_q(\mathfrak{n}^+) \overset{\Phi}{\hookrightarrow} \mathcal{F} = \bigoplus_{i_1,\dots,i_k \in I}^{k \in \mathbb{N}} \mathbb{Q}(q) \cdot [i_1 \dots i_k] \tag{1.9}$$

where the right-hand side is endowed with the quantum shuffle product (see Definition 4.11). As shown by Lalonde-Ram in [26], there is a one-to-one correspondence between positive roots and <u>standard Lyndon</u> (or Shirshov) words in the alphabet I:

$$\ell \colon \Delta^+ \xrightarrow{\sim} \Big\{ \text{standard Lyndon words} \Big\} \tag{1.10}$$

To this end, we recall that a word in an ordered finite alphabet I is called *Lyndon* if it is lexicographically smaller than all of its cyclic permutations (see Definition 2.4). These words naturally give rise to a basis of the free Lie algebra generated by the alphabet I through the standard bracketing (cf. (2.9)). In [26], a Gröbner basis type approach was used to combinatorially describe a subset of all Lyndon words, called *standard Lyndon* words, that gives rise to a basis of a Lie algebra generated by I (see Definition 2.12(b)). Thus, in the context of (1.10), the notion of standard Lyndon words intrinsically depends on a fixed total order of the indexing set I of simple roots. Furthermore, (1.10) gives rise to a total order on the positive roots:

$$\alpha < \beta \quad \Leftrightarrow \quad \ell(\alpha) < \ell(\beta) \text{ lexicographically} \tag{1.11}$$

It was shown in [39], see [27, Proposition 26], that this total order is convex, and hence can be applied to obtain root vectors $e_\alpha \in U_q(\mathfrak{n}^+)$ for any positive root α, as in (1.8). Moreover, [27] shows that the root vector e_α is uniquely characterized (up to a scalar multiple) by the property that $\Phi(e_\alpha)$ is an element of Im Φ whose leading order term $[i_1 \dots i_k]$ (in the lexicographic order) is precisely $\ell(\alpha)$. We would also like to mention [4] which contains alternative proofs of some of the results of [27], particularly leading into a generalization to quantum supergroups.

1.4. The motivation of the present paper is to extend the discussion of Subsection 1.3 to affine root systems. This would yield a combinatorial description of PBW bases inside the positive half of the Drinfeld-Jimbo affine quantum group. But there is an important problem with this program: the root spaces are no longer one-dimensional in the affine case (because of the imaginary roots), which creates various technical difficulties. We will therefore not take this route, and instead take an "orthogonal" approach. We start from Drinfeld's new presentation of quantum loop groups as:

$$U_q(L\mathfrak{g}) = U_q(L\mathfrak{n}^+) \otimes U_q(L\mathfrak{h}) \otimes U_q(L\mathfrak{n}^-)$$

where $U_q(L\mathfrak{n}^+)$ is a q-deformation of the universal enveloping algebra of $\mathfrak{n}^+[t, t^{-1}]$. The latter Lie algebra has the property that all its root spaces are one-dimensional, so we are able to adapt many of the results mentioned in the previous Subsection. To do so, we introduce the loop version $\mathcal{F}^L$ of the algebra $\mathcal{F}$ in Sections 4.27–4.32:

$$\mathcal{F}^L = \bigoplus_{\substack{i_1,\dots,i_k \in I \\ d_1,\dots,d_k \in \mathbb{Z}}}^{k\in\mathbb{N}} \mathbb{Q}(q) \cdot \left[i_1^{(d_1)} \dots i_k^{(d_k)}\right]$$

The algebra structure on $\mathcal{F}^L$ is defined by the following shuffle product:

$$\left[i_1^{(d_1)} \dots i_k^{(d_k)}\right] * \left[j_1^{(e_1)} \dots j_l^{(e_l)}\right] =$$

$$\sum_{\substack{\{1,\dots,k+l\}=A\sqcup B \\ |A|=k,|B|=l}} \left(\sum_{\substack{\pi_1+\dots+\pi_{k+l}=0 \\ \pi_1,\dots,\pi_{k+l}\in\mathbb{Z}}} \gamma_{A,B,\pi_1,\dots,\pi_{k+l}} \cdot \left[s_1^{(t_1+\pi_1)} \dots s_{k+l}^{(t_{k+l}+\pi_{k+l})}\right] \right)$$

where if $A = \{a_1 < \dots < a_k\}$ and $B = \{b_1 < \dots < b_l\}$, we write:

$$s_c = \begin{cases} i_\bullet & \text{if } c = a_\bullet \\ j_\bullet & \text{if } c = b_\bullet \end{cases}, \qquad t_c = \begin{cases} d_\bullet & \text{if } c = a_\bullet \\ e_\bullet & \text{if } c = b_\bullet \end{cases}$$

and the coefficients $\gamma_{A,B,\pi_1,\dots,\pi_{k+l}}$ are explicitly given in (4.52). In fact, one actually needs to work with an appropriate completion above, see (4.55)–(4.56), in order for the shuffle product to be well-defined (as it contains infinitely many summands).

Theorem 1.5. *There exists an injective algebra homomorphism:*

$$U_q(L\mathfrak{n}^+) \xhookrightarrow{\Phi^L} \mathcal{F}^L$$

Fix a total order of I, which induces the following total order on the set $\{i^{(d)}\}_{i\in I}^{d\in\mathbb{Z}}$:

$$i^{(d)} < j^{(e)} \quad \textit{if} \quad \begin{cases} d > e \\ \ \textit{or} \\ d = e \ \textit{and} \ i < j \end{cases} \tag{1.12}$$

This induces the lexicographic order on the words $[i_1^{(d_1)} \dots i_k^{(d_k)}]$ *with respect to which we may define the notion of* <u>*standard Lyndon loop words*</u> *by analogy with [26] (see Subsections 2.22–2.27 for details). Then, there exists a 1-to-1 correspondence:*

$$\ell \colon \Delta^+ \times \mathbb{Z} \xrightarrow{\sim} \Big\{ \textit{standard Lyndon loop words} \Big\} \tag{1.13}$$

The lexicographic order on the right-hand side induces a convex order on the left-hand side, with respect to which one can define elements:

$$e_{\ell(\alpha,d)} \in U_q(L\mathfrak{n}^+) \tag{1.14}$$

for all $(\alpha, d) \in \Delta^+ \times \mathbb{Z}$*. We have the following analogue of the PBW theorem:*

$$U_q(L\mathfrak{n}^+) \ = \bigoplus_{\ell_1 \geq \dots \geq \ell_k \ \textit{standard Lyndon loop words}}^{k \in \mathbb{N}} \mathbb{Q}(q) \cdot e_{\ell_1} \dots e_{\ell_k} \tag{1.15}$$

There are also analogues of the constructions above with $+ \leftrightarrow -$ *and* $e \leftrightarrow f$*.*

By analogy with the previous paragraph, the total order on $\Delta^+ \times \mathbb{Z}$ given by:

$$(\alpha, d) < (\beta, e) \quad \Leftrightarrow \quad \ell(\alpha, -d) < \ell(\beta, -e) \text{ lexicographically} \tag{1.16}$$

is convex; this fact will be proved in Proposition 2.34. As such, this order comes from a certain reduced word in the affine Weyl group associated to $\mathfrak{g}$ (= the Coxeter group associated to $\widehat{\mathfrak{g}}$), in accordance with Theorem 3.14. Therefore, the root vectors (1.14) exactly match (up to constants) the classical construction of [2,5,29,30], once we pass it through the "affine to loop" isomorphism (4.45).

We note that our notion of standard Lyndon loop words, as well as the order (1.16) on $\Delta^+ \times \mathbb{Z}$, are not the same as the similarly named notions of [19]. In general, our order between (α, d) and (β, e) is not determined by the order between α and β, as was the case in [19].

1.6. There exists another shuffle algebra construction in the theory of quantum loop groups, with its origins in the elliptic algebras defined by Feigin-Odesskii [13]. In the setting at hand, the construction is due to Enriquez [9], who constructed an algebra homomorphism:

$$U_q(L\mathfrak{n}^+) \xrightarrow{\Upsilon} \mathcal{A}^+ \subset \bigoplus_{\mathbf{k} = (k_i)_{i \in I} \in \mathbb{N}^I} \mathbb{Q}(q)(\dots, z_{i1}, \dots, z_{ik_i}, \dots)^{\mathrm{Sym}}$$

where the direct sum is made into an algebra using the multiplication (5.2) (we refer the reader to Definition 5.2 for the precise definition of the inclusion $\subset$ above in terms of pole and wheel conditions). In the present paper, we prove that:

Theorem 1.7. *The map Υ is an isomorphism.*

In type A_n, this result follows immediately from the type $\widehat{A}_n$ case proved in [33] (see also [42] for the rational, super, and two-parameter generalizations), but the methods of [33] are difficult to generalize to our current setup. Instead, we use the framework of the preceding Subsection to prove Theorem 1.7. To this end, in Subsection 5.20, we construct an algebra homomorphism:

$$\mathcal{A}^+ \stackrel{\iota}{\hookrightarrow} \mathcal{F}^L$$

given explicitly by (5.25), such that

$$\Phi^L = \iota \circ \Upsilon$$

according to (5.29). Extending all algebras by adding Cartan elements, we obtain:

$$U_q(L\mathfrak{b}^+) \xrightarrow{\Upsilon} \mathcal{A}^{\geq} \stackrel{\iota}{\hookrightarrow} \mathcal{F}^{L,\mathrm{ext}}$$

see (5.15), (5.27), which are bialgebra homomorphisms by Propositions 5.13, 5.21. Furthermore, in Proposition 5.15, we construct a bialgebra pairing

$$\mathcal{A}^{\geq} \otimes U_q(L\mathfrak{b}^-) \longrightarrow \mathbb{Q}(q)$$

which is non-degenerate in the first argument by Proposition 5.17. To establish the surjectivity of the embedding Υ, we filter $U_q(L\mathfrak{n}^+)$ by $U_q(L\mathfrak{n}^+)_{\leq w}$ and $\mathcal{A}$ by $\mathcal{A}_w$, so that

$$\Upsilon(U_q(L\mathfrak{n}^+)_{\leq w}) \subset \mathcal{A}^+_{\leq w} \quad \text{for any loop word} \quad w$$

Using the non-degeneracy of the aforementioned pairing, we then obtain:

$$\#\Big\{\text{good loop words } \leq w\Big\} = \dim U_q(L\mathfrak{n}^+)_{\leq w} \leq$$
$$\dim \mathcal{A}^+_{\leq w} \leq \dim U_q(L\mathfrak{n}^-)^{\leq w} = \#\Big\{\text{standard loop words } \leq w\Big\}$$

with the dimension count understood in the sense of restriction to each $Q^+ \times \mathbb{Z}$-graded component. Evoking Proposition 4.41, we then conclude that both inequalities $\leq$ above must be equalities. This implies the surjectivity of Υ as $\mathcal{A}^+ = \cup_w \mathcal{A}^+_{\leq w}$.

The homomorphism ι can be construed as connecting the two (a priori) different instances of shuffle algebras that appear in the study of quantum loop groups.

1.8. Many of the things discussed in the present paper are connected to existing literature. Besides the strong inspiration from the finite type case studied in [26,27,39] that we already mentioned, we encounter the following concepts:

- Theorems on convex PBW bases of affine quantum groups [2,5,23,29] inspired by the constructions of [24,28,37] for quantum groups of finite type.
- Shuffle algebra incarnations of quantum groups [15,38,40], which we generalize to quantum loop groups, obtaining the algebra $\mathcal{F}^L$ that features in Theorem 1.5.
- Feigin-Odesskii shuffle algebras [13] and their trigonometric versions [9], which have recently had numerous applications to mathematical physics, cf. survey [12].

The combinatorics of Lyndon words for finite types was connected with representations of KLR algebras in [25]. It would be very interesting if the combinatorics of Lyndon loop words had such an interpretation. A priori, the setting of [25] generalizes to affine types, which differs from our approach by the isomorphism (4.45).

1.9. The structure of the present paper is the following:

- In Section 2, we study the Lie algebras $\mathfrak{g}$ and $L\mathfrak{g}$, recall the notion of standard Lyndon words for the former, and extend this notion to the latter.
- In Section 3, we show that the order (1.16) on $\Delta^+ \times \mathbb{Z}$ corresponds to a certain reduced decomposition in the extended affine Weyl group of $\mathfrak{g}$.
- In Section 4, we study the quantum groups $U_q(\mathfrak{g})$ and $U_q(L\mathfrak{g})$, and their PBW bases defined with respect to standard Lyndon (loop) words. We construct the objects featuring in Theorem 1.5.
- In Section 5, we recall the trigonometric degeneration of the Feigin-Odesskii shuffle algebra, and prove Theorem 1.7 using the results of Theorem 1.5.

The interested reader may find self-contained proofs of Theorem 4.8 ([27]) and Theorem 4.25 ([11], which plays a key role in our proof of Theorem 1.5), as well as a list of standard Lyndon loop words for the classical types in Section 5 and the Appendix (respectively) of the arχiv version of the present paper.

1.10. We would like to thank Pavel Etingof and Boris Feigin for their help and numerous stimulating discussions over the years. We also thank Alexander Kleshchev and Weiqiang Wang for their interesting remarks on a draft of the present paper. We are indebted to the anonymous referee for useful suggestions on the exposition.

A.N. would like to gratefully acknowledge NSF grants DMS-1760264 and DMS-1845034, as well as support from the Alfred P. Sloan Foundation and the MIT Research Support Committee. A.T. would like to gratefully acknowledge NSF grants DMS-2037602 and DMS-2302661.

2. Lie algebras and Lyndon words

It is a classical result that the free Lie algebra on a set of generators $\{e_i\}_{i\in I}$ has a basis indexed by Lyndon words (see Definition 2.4) in the alphabet I. If we impose a certain collection of relations among the e_i's, then [26] showed that a basis of the resulting Lie algebra is given by standard Lyndon words (see Definition 2.12), and determined the latter in the particular case of the maximal nilpotent subalgebra of a simple Lie algebra. In the present Section, we will extend the treatment of [26] to the situation of loops into simple Lie algebras.

We start with the exposition of the relevant classical results in Subsections 2.1–2.18.

2.1. Let us consider a root system of finite type:

$$\Delta^+ \sqcup \Delta^- \subset Q$$

(where Q denotes the root lattice) associated to the symmetric pairing:

$$(\cdot,\cdot)\colon Q\otimes Q \longrightarrow \mathbb{Z}$$

Let $\{\alpha_i\}_{i\in I}\subset \Delta^+$ denote a choice of <u>simple roots</u>. The Cartan matrix $(a_{ij})_{i,j\in I}$ and the symmetrized Cartan matrix $(d_{ij})_{i,j\in I}$ of this root system are:

$$a_{ij} = \frac{2(\alpha_i,\alpha_j)}{(\alpha_i,\alpha_i)} \qquad \text{and} \qquad d_{ij} = (\alpha_i,\alpha_j) \tag{2.1}$$

Definition 2.2. To the root system above, one associates the Lie algebra:

$$\mathfrak{g} = \mathbb{Q}\Big\langle e_i, f_i, h_i\Big\rangle_{i\in I}\Big/\text{relations (2.2)–(2.4)}$$

where we impose the following relations for all $i,j\in I$:

$$\underbrace{[e_i,[e_i,[\dots,[e_i,e_j]\dots]]]}_{1-a_{ij}\text{ Lie brackets}} = 0, \quad \text{if } i\neq j \tag{2.2}$$

$$[h_j,e_i] = d_{ji}e_i, \qquad\qquad [h_i,h_j]=0 \tag{2.3}$$

as well as the opposite relations with e's replaced by f's, and finally the relation:

$$[e_i,f_j] = \delta_i^j h_i \tag{2.4}$$

We will consider the triangular decomposition (1.1), where $\mathfrak{n}^+$, $\mathfrak{h}$, $\mathfrak{n}^-$ are the Lie subalgebras of $\mathfrak{g}$ generated by the e_i, h_i, f_i, respectively. We will write:

$$Q^\pm \subset Q$$

for the monoids generated by $\pm\alpha_i$. The Lie algebra $\mathfrak{g}$ is graded by Q, if we let:

$$\deg e_i = \alpha_i, \quad \deg h_i = 0, \quad \deg f_i = -\alpha_i$$

The subalgebras $\mathfrak{n}^\pm$ are graded by $Q^\pm$ accordingly.

2.3. We will now recall the construction of [26], which describes positive roots in terms of the combinatorics of words:

$$[i_1 \dots i_k] \tag{2.5}$$

for various $i_1, \dots, i_k \in I$. Let us fix a total order on the set I of simple roots, which induces the following total lexicographic order on the set of all words:

$$[i_1 \dots i_k] < [j_1 \dots j_l] \quad \text{if} \begin{cases} i_1 = j_1, \dots, i_a = j_a, i_{a+1} < j_{a+1} \text{ for some } a \geq 0 \\ \text{ or} \\ i_1 = j_1, \dots, i_k = j_k \text{ and } k < l \end{cases}$$

Definition 2.4. A word $\ell = [i_1 \dots i_k]$ is called Lyndon (such words were also studied independently by Shirshov) if it is smaller than all of its cyclic permutations:

$$[i_1 \dots i_{a-1} i_a \dots i_k] < [i_a \dots i_k i_1 \dots i_{a-1}]$$

for all $a \in \{2, \dots, k\}$.

The following is an elementary exercise, that we leave to the interested reader.

Claim 2.5. *If $\ell_1 < \ell_2$ are Lyndon, then $\ell_1\ell_2$ is also Lyndon, and so $\ell_1\ell_2 < \ell_2\ell_1$.*

Given a word $w = [i_1 \dots i_k]$, the subwords:

$$w_{a|} = [i_1 \dots i_a] \qquad \text{and} \qquad w_{|a} = [i_{k-a+1} \dots i_k]$$

with $0 \leq a \leq k$ will be called a prefix and a suffix of w, respectively. Such a prefix or a suffix is called proper if $a \notin \{0, k\}$. It is straightforward to show that a word w is Lyndon iff it is smaller than all of its proper suffixes, i.e. $w < w_{|a}$ for all $0 < a < k$.

Proposition 2.6 *(see [26, §1] for a survey). Any Lyndon word ℓ has a factorization:*

$$\ell = \ell_1 \ell_2 \tag{2.6}$$

defined by the property that ℓ_2 is the longest proper suffix of ℓ which is also a Lyndon word. Under these circumstances, ℓ_1 is also a Lyndon word.

Proposition 2.7. *Any word w has a* <u>*canonical factorization*</u> *as a concatenation:*

$$w = \ell_1 \dots \ell_k \tag{2.7}$$

where $\ell_1 \geq \dots \geq \ell_k$ are all Lyndon words.

2.8. For any word $w = [i_1 \dots i_k]$, we define:

$$_w e = e_{i_1} \dots e_{i_k} \in U(\mathfrak{n}^+) \tag{2.8}$$

On the other hand, Propositions 2.6 and 2.7 yield the following construction.

Definition 2.9. For any word w, define $e_w \in U(\mathfrak{n}^+)$ inductively by $e_{[i]} = e_i$ and:

$$e_\ell = [e_{\ell_1}, e_{\ell_2}] \in \mathfrak{n}^+ \tag{2.9}$$

if ℓ is a Lyndon word with factorization (2.6), and:

$$e_w = e_{\ell_1} \dots e_{\ell_k} \in U(\mathfrak{n}^+) \tag{2.10}$$

if w is an arbitrary word with the canonical factorization $\ell_1 \dots \ell_k$, as in (2.7).

Remark 2.10. Because $[e_\alpha, e_\beta] \in \mathbb{Q}^* \cdot e_{\alpha+\beta}$ for all positive roots α, β such that $\alpha + \beta$ is also a root ([20, Proposition 8.4(d)]), then choosing a different factorization (2.6) for various Lyndon words will in practice produce bracketings (2.9) which are non-zero multiples of each other. Thus various choices will simply lead to PBW bases (1.4) which are renormalizations of each other.

It is well-known that the elements (2.8) and (2.10) both give rise to bases of $U(\mathfrak{n}^+)$, and indeed are connected by the following triangularity property:

$$e_w = \sum_{v \geq w} c_w^v \cdot {}_v e \tag{2.11}$$

for various integer coefficients c_w^v such that $c_w^w = 1$.

2.11. If $\mathfrak{n}^+$ were a free Lie algebra, then it would have a basis given by the elements (2.9), as ℓ goes over all Lyndon words (and similarly, $U(\mathfrak{n}^+)$ would have a basis given by the elements (2.10) as w goes over all words). But since we have to contend with the relations (2.2) between the generators $e_i \in \mathfrak{n}^+$, we must restrict the set of Lyndon words which appear. The following definition is due to [26].

Definition 2.12. (a) A word w is called <u>standard</u> if $_w e$ cannot be expressed as a linear combination of $_v e$ for various $v > w$, with $_w e$ as in (2.8).

(b) A Lyndon word ℓ is called standard Lyndon if e_ℓ cannot be expressed as a linear combination of e_m for various Lyndon words $m > \ell$, with e_ℓ as in (2.9).

The following Proposition is non-trivial, and it justifies the above terminology.

Proposition 2.13 *([26]). A Lyndon word is standard iff it is standard Lyndon.*

According to [26, §2.1], $\mathfrak{n}^+$ has a basis consisting of the e_ℓ's, as ℓ goes over all standard Lyndon words. Since the Lie algebra $\mathfrak{n}^+$ is Q^+-graded by $\deg e_i = \alpha_i$, it is natural to extend this grading to words as follows:

$$\deg[i_1 \dots i_k] = \alpha_{i_1} + \dots + \alpha_{i_k} \tag{2.12}$$

Because of the decomposition (1.2) of $\mathfrak{n}^+$, and the fact that the basis vectors $e_\alpha \in \mathfrak{n}^+$ all live in distinct degrees $\alpha \in Q^+$, we conclude that there exists a bijection:

$$\ell \colon \Delta^+ \xrightarrow{\sim} \Big\{\text{standard Lyndon words}\Big\} \tag{2.13}$$

such that $\deg \ell(\alpha) = \alpha$, for all $\alpha \in \Delta^+$.

2.14. The following explicit description of the bijection (2.13) was proved in [27, Proposition 25], and allows one to inductively construct the bijection ℓ:

$$\ell(\alpha) \ = \max_{\substack{\gamma_1+\gamma_2=\alpha,\ \gamma_k\in\Delta^+ \\ \ell(\gamma_1)<\ell(\gamma_2)}} \Big\{\text{concatenation } \ell(\gamma_1)\ell(\gamma_2)\Big\} \tag{2.14}$$

We also have the following simple property of standard words.

Proposition 2.15 *([26, §2.4]). Any subword of a standard word is standard.*

Combining Propositions 2.7, 2.13, 2.15, we conclude that any standard word can be uniquely written in the form (2.7), where $\ell_1 \geq \dots \geq \ell_k$ are all standard Lyndon words. The converse also holds (by a dimension count argument, see [26, §2.8]).

Proposition 2.16 *([26]). A word w is standard if and only if it can be written (uniquely) as $w = \ell_1 \dots \ell_k$, where $\ell_1 \geq \dots \geq \ell_k$ are standard Lyndon words.*

Remark 2.17. The results of Propositions 2.13, 2.15, 2.16 hold for any finite dimensional Lie algebra, according to [26]. In particular, we shall be applying them to Lie algebras $L^{(s)}\mathfrak{n}^+$ of (2.22), generalizing $L^{(0)}\mathfrak{n}^+ \simeq \mathfrak{n}^+$.

Thus we obtain the following reformulation of (1.4):

$$U(\mathfrak{n}^+) = \bigoplus_{\ell_1 \geq \dots \geq \ell_k \text{ standard Lyndon words}}^{k \in \mathbb{N}} \mathbb{Q} \cdot e_{\ell_1} \dots e_{\ell_k} \tag{2.15}$$

By the triangularity property (2.11), we could also get a basis of $U(\mathfrak{n}^+)$ by replacing $e_w = e_{\ell_1} \dots e_{\ell_k}$ in (2.15) by ${}_w e$, for any standard word w.

2.18. The bijection (2.13) yields a total order on the set of positive roots Δ^+, induced by the lexicographic order of standard Lyndon words, see (1.11). As observed in [27,39], this order is convex, in the following sense.

Definition 2.19. A total order on the set of positive roots Δ^+ is called convex if:

$$\alpha < \alpha + \beta < \beta \tag{2.16}$$

for all $\alpha < \beta \in \Delta^+$ such that $\alpha + \beta$ is also a root.

It is well-known ([34]) that convex orders of the positive roots are in 1-to-1 correspondence with reduced decompositions of the longest element of the Weyl group associated to our root system. We will consider this issue, and its affine version, in more detail in Section 3.

Proposition 2.20 *([27, Proposition 26]). The order (1.11) on Δ^+ is convex.*

We will prove the loop version of the Proposition above in Proposition 2.34.

2.21. We will now extend the description above to the Lie algebra of loops into $\mathfrak{g}$:

$$L\mathfrak{g} = \mathfrak{g}[t, t^{-1}] = \mathfrak{g} \otimes_{\mathbb{Q}} \mathbb{Q}[t, t^{-1}]$$

where the Lie bracket is simply given by:

$$[x \otimes t^m, y \otimes t^n] = [x, y] \otimes t^{m+n} \tag{2.17}$$

for all $x, y \in \mathfrak{g}$ and $m, n \in \mathbb{Z}$. The triangular decomposition (1.1) extends to a similar decomposition at the loop level, and our goal is to describe $L\mathfrak{n}^+$ along the lines of Subsections 2.11–2.14. To this end, we think of $L\mathfrak{n}^+$ as being generated by:

$$e_i^{(d)} = e_i \otimes t^d$$

$\forall\, i \in I, d \in \mathbb{Z}$. Associate to $e_i^{(d)}$ the letter $i^{(d)}$, and call d the exponent of $i^{(d)}$. We fix a total order on I, which induces the total order (1.12) on the letters $\{i^{(d)}\}_{i \in I}^{d \in \mathbb{Z}}$. Any word in these letters will be called a loop word:

$$\left[i_1^{(d_1)} \dots i_k^{(d_k)}\right] \tag{2.18}$$

We have the total lexicographic order on loop words (2.18) induced by (1.12). All the results of Subsection 2.3 continue to hold in the present setup, so we have a notion of Lyndon loop words. Since $L\mathfrak{n}^+$ is $Q^+ \times \mathbb{Z}$-graded by:

$$\deg e_i^{(d)} = (\alpha_i, d)$$

it makes sense to extend this grading to loop words as follows:

$$\deg \left[i_1^{(d_1)} \dots i_k^{(d_k)}\right] = (\alpha_{i_1} + \dots + \alpha_{i_k}, d_1 + \dots + d_k) \tag{2.19}$$

The obvious generalization of (1.2) is:

$$L\mathfrak{n}^+ = \bigoplus_{\alpha \in \Delta^+} \bigoplus_{d \in \mathbb{Z}} \mathbb{Q} \cdot e_\alpha^{(d)} \tag{2.20}$$

with $e_\alpha^{(d)} = e_\alpha \otimes t^d$. If $\deg x = (\alpha, d) \in Q^+ \times \mathbb{Z}$, then we will use the notation:

$$\operatorname{hdeg} x = \alpha \qquad \text{and} \qquad \operatorname{vdeg} x = d \tag{2.21}$$

and call these two notions the <u>horizontal</u> and the <u>vertical</u> degree, respectively. While obviously infinite-dimensional, $L\mathfrak{n}^+$ still has one-dimensional $Q^+ \times \mathbb{Z}$-graded pieces, which is essential for the treatment of [26] to carry through.

The aim of Subsections 2.22–2.27 is to obtain a notion of standard (Lyndon) loop words. This is a non-trivial task as the alphabet $\{i^{(d)}\}_{i \in I}^{d \in \mathbb{Z}}$ is infinite. To do so, we shall consider a filtration by finitely generated Lie algebras $L^{(s)}\mathfrak{n}^+$ of (2.22), corresponding to the finite alphabets $\{e_i^{(d)} | i \in I, -s \leq d \leq s\}$. We then establish some basic properties of the corresponding standard Lyndon loop words for $L^{(s)}\mathfrak{n}^+$ in Propositions 2.23, 2.25, 2.26, 2.28. The latter result implies that the notion of "standard Lyndon loop word" does not depend on the particular $L^{(s)}\mathfrak{n}^+$ with respect to which it is defined, thus establishing the loop analogue (2.35) of the bijection (2.13).

2.22. We now wish to extend Definition 2.12 in order to obtain a notion of standard (Lyndon) loop words, but here we must be careful, because the alphabet $\{i^{(d)}\}_{i \in I}^{d \in \mathbb{Z}}$ is infinite. In particular, the key assumption "for any word v, there are only finitely many words u of the same length and $> v$ in the lexicographical order" of [26, §2] clearly does not hold. To deal with this issue, we consider the increasing filtration:

$$L\mathfrak{n}^+ = \bigcup_{s=0}^{\infty} L^{(s)}\mathfrak{n}^+$$

defined with respect to the finite-dimensional Lie subalgebras:

$$L\mathfrak{n}^+ \supset L^{(s)}\mathfrak{n}^+ = \bigoplus_{\alpha\in\Delta^+} \bigoplus_{d=-s|\alpha|}^{s|\alpha|} \mathbb{Q}\cdot e_\alpha^{(d)} \tag{2.22}$$

where $|\alpha|$ denotes the height of a root, i.e.

$$|\alpha| = \sum_{i\in I} k_i$$

if $\alpha = \sum_{i\in I} k_i\alpha_i$.

As a Lie algebra, $L^{(s)}\mathfrak{n}^+$ is generated by $\{e_i^{(d)}|i \in I, -s \leq d \leq s\}$. Therefore, we may apply Definition 2.12 to yield a notion of standard (Lyndon) loop words with respect to the finite-dimensional Lie algebras $L^{(s)}\mathfrak{n}^+$, where the corresponding words will only be made up of the symbols $i^{(d)}$ with $i \in I, d \in \{-s, \dots, s\}$.

Proposition 2.23. *There exists a bijection:*

$$\ell\colon \Big\{(\alpha, d) \in \Delta^+ \times \mathbb{Z}, |d| \leq s|\alpha|\Big\} \xrightarrow{\sim} \Big\{\textit{standard Lyndon loop words for } L^{(s)}\mathfrak{n}^+\Big\} \tag{2.23}$$

explicitly determined by $\ell(\alpha_i, d) = \left[i^{(d)}\right]$ *and the following property:*

$$\ell(\alpha, d) \;=\; \max_{\substack{(\gamma_1,d_1)+(\gamma_2,d_2)=(\alpha,d)\\ \gamma_k\in\Delta^+,\ |d_k|\leq s|\gamma_k|\\ \ell(\gamma_1,d_1)<\ell(\gamma_2,d_2)}} \Big\{\textit{concatenation } \ell(\gamma_1, d_1)\ell(\gamma_2, d_2)\Big\} \tag{2.24}$$

In view of Proposition 2.16 (see Remark 2.17), this also gives a parametrization of standard loop words for $L^{(s)}\mathfrak{n}^+$. We note that both the property (2.24), as well as the main idea of the subsequent proof, are direct adaptations of the analogous results in [27] (cf. (2.14)).

Proof of Proposition 2.23. Because the root spaces of $L^{(s)}\mathfrak{n}^+$ are one-dimensional, as in (2.22), then for any Lyndon loop word ℓ of degree $(\alpha, d) \in Q^+ \times \mathbb{Z}$ with $|d| \leq s|\alpha|$, we have:

$$e_\ell \in \mathbb{Q}\cdot e_\alpha^{(d)} \tag{2.25}$$

The right-hand side is 0 if $\alpha \notin \Delta^+$. By Definition 2.12(b), a word ℓ is standard Lyndon if and only if it is the maximal Lyndon loop word of its given degree, with the property that $e_\ell \neq 0$. Together with the fact [26, §2.1] that $\{e_\ell|\ell - \text{standard Lyndon}\}$ is a basis of $L^{(s)}\mathfrak{n}^+$, this establishes the existence of a bijection (2.23).

Let us now prove that this bijection takes the form (2.24). Consider any $\gamma_1, \gamma_2 \in \Delta^+$ such that $\gamma_1 + \gamma_2 \in \Delta^+$, and any integers d_1, d_2 such that $|d_k| \leq s|\gamma_k|$ for all $k \in \{1, 2\}$. Let us write $\ell_k = \ell(\gamma_k, d_k)$ for all $k \in \{1, 2\}$ and $\ell = \ell(\gamma_1 + \gamma_2, d_1 + d_2)$; we may assume without loss of generality that $\ell_1 < \ell_2$. We have:

$$e_{\ell_k} = \sum_{v_k \geq \ell_k} c_{\ell_k}^{v_k} \cdot {}_{v_k}e \tag{2.26}$$

$\forall\, k \in \{1,2\}$, due to property (2.11) (which holds in $L^{(s)}\mathfrak{n}^+$ as it did in $\mathfrak{n}^+$). Thus:

$$e_{\ell_1} e_{\ell_2} = \sum_{v \geq \ell_1 \ell_2} x_v \cdot {}_v e \tag{2.27}$$

for various coefficients x_v.[2] As a consequence of Claim 2.5, we have an analogue of formula (2.27) when the indices 1 and 2 are swapped in the left-hand side. Hence we obtain the following formula for the commutator:

$$[e_{\ell_1}, e_{\ell_2}] = \sum_{v \geq \ell_1 \ell_2} y_v \cdot {}_v e \tag{2.28}$$

for various coefficients y_v. Furthermore, we may restrict the sum above to standard v's since, by the very definition of this notion, any ${}_v e$ can be inductively written as a linear combination of ${}_u e$'s for standard $u \geq v$ (this uses the fact that there exist finitely many words of any given degree, as we use a finite alphabet $\{i^{(d)}\}_{i\in I}^{-s\leq d\leq s}$). By this very same reason, we may restrict the right-hand side of (2.11) to standard v's, and conclude that $\{e_w | w - \text{standard}\}$ yield a basis which is upper triangular in terms of the basis $\{{}_w e | w - \text{standard}\}$. With this in mind, (2.28) implies:

$$[e_{\ell_1}, e_{\ell_2}] = \sum_{\substack{v \geq \ell_1 \ell_2 \\ v-\text{standard}}} z_v \cdot e_v \tag{2.29}$$

for various coefficients z_v.

However, $[e_{\gamma_1}, e_{\gamma_2}] \in \mathbb{Q}^* \cdot e_{\gamma_1+\gamma_2}$ implies $[e_{\gamma_1}^{(d_1)}, e_{\gamma_2}^{(d_2)}] \in \mathbb{Q}^* \cdot e_{\gamma_1+\gamma_2}^{(d_1+d_2)}$, so that:

$$[e_{\ell_1}, e_{\ell_2}] \in \mathbb{Q}^* \cdot e_\ell \tag{2.30}$$

As $\{e_v | v - \text{standard}\}$ is a basis of $U(L^{(s)}\mathfrak{n}^+)$ ([26, §2.2]), comparing (2.29) and (2.30), we conclude that $\ell \geq \ell_1 \ell_2$. This proves the inequality $\geq$ in (2.24). As for the opposite inequality $\leq$, it follows from the fact that $\ell(\alpha, d)$ admits a factorization (2.6) $\ell(\alpha, d) = \ell_1 \ell_2$ (with $\ell_1 < \ell(\alpha, d) < \ell_2$), and Propositions 2.13, 2.15 (see Remark 2.17) imply that $\ell_k = \ell(\gamma_k, d_k)$ for some decomposition $(\alpha, d) = (\gamma_1, d_1) + (\gamma_2, d_2)$. $\square$

Since standard Lyndon loop words give rise to bases of the finite-dimensional Lie algebra $L^{(s)}\mathfrak{n}^+$, then the analogue of property (2.15) gives us:

[2] Here we are using the fact that if $v_1 \geq \ell_1$ and $v_2 \geq \ell_2$, then $v_1 v_2 \geq \ell_1 \ell_2$; this fact is not true for arbitrary words v_1 and v_2, because we could have $v_1 = \ell_1 u$ for some word $u < \ell_2$. However, such counterexamples are not allowed because the words v_k which appear in (2.26) have the same number of letters as ℓ_k, for degree reasons.

$$U(L^{(s)}\mathfrak{n}^+) \;=\; \bigoplus^{k\in\mathbb{N}}_{\substack{\ell_1\geq\dots\geq\ell_k \text{ standard Lyndon loop} \\ \text{words with all exponents in } \{-s,\dots,s\}}} \mathbb{Q}\cdot e_{\ell_1}\dots e_{\ell_k} \tag{2.31}$$

By the triangularity property (2.11), we could also get a basis of $U(L^{(s)}\mathfrak{n}^+)$ by replacing $e_w = e_{\ell_1}\dots e_{\ell_k}$ in (2.31) by ${}_we$, for any standard loop word w with all exponents in $\{-s,\dots,s\}$.

2.24. Property (2.24) will allow us to deduce some facts about the bijection (2.23).

Proposition 2.25. *For any positive root $\alpha\in\Delta^+$ and integer $d\in\mathbb{Z}$, we have:*

$$\ell(\alpha,d) < \ell(\alpha,d-1) \tag{2.32}$$

where ℓ is the function of (2.23), which a priori depends on a natural number s (so we implicitly need $d-1,d\in\{-s|\alpha|,\dots,s|\alpha|\}$ in order for (2.32) to make sense).

Proof. Let us prove (2.32) by induction on $|\alpha|$, the base case $|\alpha| = 1$ being trivial. According to (2.24), there exist decompositions $\alpha = \gamma_1+\gamma_2$, $d = d_1+d_2$ such that:

$$\ell(\alpha,d) = \ell(\gamma_1,d_1)\ell(\gamma_2,d_2)$$

with $\ell(\gamma_1,d_1) < \ell(\gamma_2,d_2)$. Note that $\gamma_1\neq\gamma_2$ as $\gamma_1+\gamma_2$ is a root. Because we assume $d > -s|\alpha|$, then at least one of the following two options holds:

- $d_1 > -s|\gamma_1|$, in which case the induction hypothesis implies $\ell(\gamma_1,d_1-1) > \ell(\gamma_1,d_1)$. Then we either have $\ell(\gamma_1,d_1-1) < \ell(\gamma_2,d_2)$, in which case:

$$\ell(\alpha,d-1) \geq \ell(\gamma_1,d_1-1)\ell(\gamma_2,d_2) > \ell(\gamma_1,d_1)\ell(\gamma_2,d_2) = \ell(\alpha,d)$$

  or $\ell(\gamma_1,d_1-1) > \ell(\gamma_2,d_2)$, in which case:

$$\ell(\alpha,d-1) \geq \ell(\gamma_2,d_2)\ell(\gamma_1,d_1-1) > \ell(\gamma_2,d_2)\ell(\gamma_1,d_1) > \ell(\gamma_1,d_1)\ell(\gamma_2,d_2) = \ell(\alpha,d)$$

- $d_2 > -s|\gamma_2|$, in which case the induction hypothesis implies $\ell(\gamma_2,d_2-1) > \ell(\gamma_2,d_2)$, and so $\ell(\gamma_2,d_2-1) > \ell(\gamma_1,d_1)$. Then we have:

$$\ell(\alpha,d-1) \geq \ell(\gamma_1,d_1)\ell(\gamma_2,d_2-1) > \ell(\gamma_1,d_1)\ell(\gamma_2,d_2) = \ell(\alpha,d)$$

In all chains of two or three inequalities above, the first inequality is due to (2.24), while the third inequality uses Claim 2.5. $\square$

Next, we estimate the exponents of letters in the standard Lyndon loop words for $L^{(s)}\mathfrak{n}^+$.

Proposition 2.26. *For all $\alpha \in \Delta^+$ and $d \in \{-sk, \dots, sk\}$ with $k = |\alpha|$, we have:*

$$\ell(\alpha, d) = \left[i_1^{(d_1)} \dots i_k^{(d_k)}\right] \quad \textit{for various} \quad d_1, \dots, d_k \in \left\{\left\lfloor \frac{d}{k} \right\rfloor, \left\lceil \frac{d}{k} \right\rceil\right\} \tag{2.33}$$

Proof. We will prove (2.33) by induction on k, the base case $k = 1$ being trivial.

If $\frac{d}{k} = t \in \mathbb{Z}$, then we must show that all exponents of $\ell(\alpha, d)$ are equal to t. Indeed, pick a decomposition $\alpha = \gamma_1 + \gamma_2$ into positive roots, and assume without loss of generality that $\ell(\gamma_1, t|\gamma_1|) < \ell(\gamma_2, t|\gamma_2|)$ (otherwise, swap their order). Then:

$$\ell(\alpha, d) \geq \ell(\gamma_1, t|\gamma_1|)\ell(\gamma_2, t|\gamma_2|)$$

by (2.24). By the induction hypothesis, the word on the right has all exponents equal to t, which implies that the first letter of $\ell(\alpha, d)$ has exponent $\leq t$. But because the first letter of a Lyndon loop word is its smallest one, this implies that all letters of $\ell(\alpha, d)$ have exponent $\leq t$. Because $\text{vdeg } \ell(\alpha, d) = d = tk$ is also the sum of the exponents of $\ell(\alpha, d)$, this implies that all letters of $\ell(\alpha, d)$ must have exponent equal to t, as we needed to prove.

If $tk < d < (t + 1)k$ for some $t \in \mathbb{Z}$, then we must show that all exponents of $\ell(\alpha, d)$ are equal to either t or $t + 1$. By a slight modification of the argument in the preceding paragraph, we conclude that the first letter of $\ell(\alpha, d)$ has exponent $= t + 1$, which implies that all letters of $\ell(\alpha, d)$ have exponent $\leq t + 1$. Then assume for the purpose of contradiction that there is some letter of $\ell(\alpha, d)$ with exponent $\leq t - 1$. Consider the factorization (2.6):

$$\ell(\alpha, d) = \ell(\gamma_1, d_1)\ell(\gamma_2, d_2) \tag{2.34}$$

for some decomposition $\alpha = \gamma_1 + \gamma_2$, $d = d_1 + d_2$ with $|d_k| \leq s|\gamma_k|$ for $k \in \{1, 2\}$. Since the first letter of $\ell(\gamma_1, d_1)$ has exponent $t + 1$, the induction hypothesis does not allow $\ell(\gamma_1, d_1)$ to have any letters with exponents $\leq t - 1$. Therefore, the letters with exponents $\leq t - 1$ must lie in $\ell(\gamma_2, d_2)$, and so the induction hypothesis yields:

$$d_1 > t|\gamma_1| \quad \text{and} \quad d_2 < t|\gamma_2|$$

However, if $\ell(\gamma_1, d_1 - 1) < \ell(\gamma_2, d_2 + 1)$ then the word $\ell(\gamma_1, d_1 - 1)\ell(\gamma_2, d_2 + 1)$ would be greater than $\ell(\gamma_1, d_1)\ell(\gamma_2, d_2) = \ell(\alpha, d)$, by Proposition 2.25, thus contradicting the maximality of $\ell(\alpha, d)$ provided by (2.24). The only other possibility is that $\ell(\gamma_1, d_1 - 1) > \ell(\gamma_2, d_2 + 1)$, at which point the same property (2.24) implies that:

$$\ell(\alpha, d) \geq \ell(\gamma_2, d_2 + 1)\ell(\gamma_1, d_1 - 1)$$

However, by the induction hypothesis, all the letters of $\ell(\gamma_2, d_2 + 1)$ have exponents $\leq t$, which contradicts the fact that the first letter of $\ell(\alpha, d)$ has exponent $t + 1$. $\square$

2.27. Property (2.33) has one great advantage: it is independent of s.

Proposition 2.28. *Any loop word w with exponents in $\{-s, \dots, s\}$ is standard (Lyndon) with respect to $L^{(s)}\mathfrak{n}^+$ iff it is standard (Lyndon) with respect to $L^{(s+1)}\mathfrak{n}^+$.*

Proof. Due to Proposition 2.16 (see Remark 2.17), it suffices to consider the case of standard Lyndon loop words. In other words, we must show that if α is a positive root and d is an integer such that $|d| \leq s|\alpha|$, then the Lyndon loop words:

$$\ell = \ell(\alpha, d) \text{ of (2.23) with respect to } L^{(s)}\mathfrak{n}^+$$

$$\ell' = \ell(\alpha, d) \text{ of (2.23) with respect to } L^{(s+1)}\mathfrak{n}^+$$

are equal. We may do so by induction on $|\alpha|$, the base case $|\alpha| = 1$ being trivial. Due to property (2.24), both ℓ and ℓ' are defined as the maximum over various concatenations, but the set of concatenations defining ℓ' is a priori larger. In other words, the only situation in which $\ell \neq \ell'$ would be if:

$$\ell' = \ell(\gamma_1, d_1)\ell(\gamma_2, d_2) > \ell$$

with $\ell(\gamma_1, d_1)$ or $\ell(\gamma_2, d_2)$ having an exponent $\pm(s+1)$. However, this can not happen due to (2.33) applied to ℓ', since it would force $|d| > s|\alpha|$. $\square$

Proposition 2.28 implies that the notion "standard Lyndon loop word" does not depend on the particular $L^{(s)}\mathfrak{n}^+$ with respect to which it is defined. We conclude that there exists a bijection:

$$\ell \colon \Delta^+ \times \mathbb{Z} \xrightarrow{\sim} \Big\{\text{standard Lyndon loop words}\Big\} \tag{2.35}$$

satisfying properties (2.24) and (2.33) (with $s = \infty$).

2.29. Because of the Lie algebra isomorphism:

$$L\mathfrak{n}^+ \xrightarrow{\sim} L\mathfrak{n}^+ \qquad \text{given by} \qquad e_\alpha^{(d)} \mapsto e_\alpha^{(d+|\alpha|)}$$

the procedure:

$$\left[i_1^{(d_1)} \dots i_k^{(d_k)}\right] \rightsquigarrow \left[i_1^{(d_1+1)} \dots i_k^{(d_k+1)}\right] \tag{2.36}$$

preserves the property of a loop word being standard. It obviously also preserves the property of a loop word being Lyndon, hence also of being standard Lyndon, due to Proposition 2.13 (see Remark 2.17). This implies the following result.

Proposition 2.30. *For any $(\alpha, d) \in \Delta^+ \times \mathbb{Z}$, $\ell(\alpha, d+|\alpha|)$ is obtained from $\ell(\alpha, d)$ by adding 1 to all the exponents of its letters, i.e. by the procedure (2.36).*

Therefore, to describe the bijection (2.35), it suffices to specify a finite amount of data, i.e. the standard Lyndon loop words corresponding to (α, d) for all $\alpha \in \Delta^+$ and $d \in \{0, \dots, |\alpha| - 1\}$. The $s = 0$ case of Proposition 2.28 also implies:

Proposition 2.31. *The restriction of* (2.35) *to* $\Delta^+ \times \{0\}$ *matches* (2.13).

Since $U(L\mathfrak{n}^+)$ is the direct limit as $s \to \infty$ of the $U(L^{(s)}\mathfrak{n}^+)$, then (2.31) implies:

$$U(L\mathfrak{n}^+) \ = \bigoplus_{\ell_1 \geq \dots \geq \ell_k \text{ standard Lyndon loop words}}^{k \in \mathbb{N}} \mathbb{Q} \cdot e_{\ell_1} \dots e_{\ell_k} \tag{2.37}$$

By Proposition 2.16 (see Remark 2.17), we then have:

$$U(L\mathfrak{n}^+) \ = \bigoplus_{w \text{ standard loop words}} \mathbb{Q} \cdot e_w \tag{2.38}$$

The following result will be used in Section 4.

Corollary 2.32. *For any loop word w, there exist finitely many standard loop words $\leq w$ in any fixed degree $(\alpha, d) \in Q^+ \times \mathbb{Z}$.*

Proof. Any standard loop word v admits a canonical factorization $v = \ell_1 \dots \ell_k$ where $\ell_1 \geq \dots \geq \ell_k$ are all standard Lyndon loop words. If $v \leq w$, then we note that all the ℓ_r's are bounded from above by w, due to $\ell_r \leq \ell_1 \leq v$. Combining this with (2.33), we see that the exponents which appear among the letters of the ℓ_r's are bounded from below. Therefore, there are only finitely many choices of $\ell_1, \dots, \ell_k$ with a fixed number of letters, whose exponents sum up to precisely d. $\square$

We conclude this Section with a few fundamental properties of the total order (1.16) on $\Delta^+ \times \mathbb{Z}$ induced by (2.35) from the lexicographic order. The loop version of the convexity result from Proposition 2.20 is established in Proposition 2.34. A corollary of the latter implies Proposition 2.38 which is key to the proof of Theorem 4.25.

2.33. The bijection (2.35) gives rise to a total order (1.16) on $\Delta^+ \times \mathbb{Z}$, by transporting the total lexicographic order on loop words. We will now show that this order is convex, a notion which is the direct generalization of Definition 2.19.

Proposition 2.34. *For all $(\alpha, d), (\beta, e), (\alpha + \beta, d + e) \in \Delta^+ \times \mathbb{Z}$, we have:*

$$\ell(\alpha, d) < \ell(\alpha + \beta, d + e) < \ell(\beta, e) \tag{2.39}$$

if $\ell(\alpha, d) < \ell(\beta, e)$.

Proof. We will prove the required statement by induction on $|\alpha+\beta|$, the base case being vacuous. By (2.24), we have:

$$\ell(\alpha+\beta,d+e) \geq \ell(\alpha,d)\ell(\beta,e) > \ell(\alpha,d)$$

Therefore, it remains to show that $\ell(\alpha+\beta,d+e) < \ell(\beta,e)$. Let us assume for the purpose of contradiction that the opposite inequality holds:

$$\ell(\alpha+\beta,d+e) > \ell(\beta,e) > \ell(\alpha,d) \tag{2.40}$$

By (2.24), we have:

$$\ell(\alpha+\beta,d+e) = \ell(\alpha',d')\ell(\beta',e') \tag{2.41}$$

where $\ell(\alpha',d') < \ell(\beta',e')$, for certain positive roots α',β' satisfying $\alpha+\beta=\alpha'+\beta'$ and integers d',e' satisfying $d+e=d'+e'$. Comparing the formulas above, we have two options:

$$\underline{\text{Case 1}}: \quad \ell(\alpha',d') > \ell(\beta,e)$$
$$\underline{\text{Case 2}}: \quad \ell(\alpha',d') < \ell(\beta,e)$$

(note that the equality $(\alpha',d')=(\beta,e)$ would imply $(\alpha,d)=(\beta',e')$, which would contradict various inequalities above). In Case 1, we would have:

$$\ell(\beta',e') > \ell(\alpha',d') > \ell(\beta,e) > \ell(\alpha,d) \tag{2.42}$$

We will use (2.42) to obtain a contradiction, but first we make an elementary claim:

Claim 2.35. *Given positive roots $\alpha,\beta,\alpha',\beta'$ such that $\alpha+\beta=\alpha'+\beta'$, then:*

$$\alpha' = \alpha+\gamma \quad \textit{and} \quad \beta' = \beta-\gamma$$

or:

$$\alpha' = \beta+\gamma \quad \textit{and} \quad \beta' = \alpha-\gamma$$

for some $\gamma \in \Delta \sqcup \{0\}$.

The Claim is proved as follows. Suppose first that $(\alpha,\alpha') > 0$. Then, the reflection $s_\alpha(\alpha') = \alpha' - k\alpha$ is also a root, for some positive integer $k > 0$. This implies that $\alpha'-\alpha$ is either a root or 0, hence $\alpha'-\alpha=\gamma$ for some $\gamma \in \Delta \sqcup \{0\}$, thus proving the claim. The analogous argument applies if $(\alpha,\beta') > 0$, $(\beta,\alpha') > 0$, or $(\beta,\beta') > 0$. However, one of the aforementioned 4 inequalities must hold, or else $0 \geq (\alpha+\beta,\alpha'+\beta') = (\alpha+\beta,\alpha+\beta)$, a contradiction.

Using Claim 2.35, we conclude that there exist $\gamma \in \Delta \sqcup \{0\}$ and $x \in \mathbb{Z}$ such that:

$$(\alpha', d') = (\alpha + \gamma, d + x) \quad \text{and} \quad (\beta', e') = (\beta - \gamma, e - x) \tag{2.43}$$

or:

$$(\alpha', d') = (\beta + \gamma, e + x) \quad \text{and} \quad (\beta', e') = (\alpha - \gamma, d - x) \tag{2.44}$$

(one just needs to pick the integer x such that the equalities above hold). First of all, we cannot have $\gamma = 0$, as Proposition 2.25 and the chain of inequalities (2.42) would simultaneously require $x > 0$ and $x < 0$. If $\gamma \neq 0$, then the induction hypothesis of (2.39) contradicts the chain of inequalities in (2.42), as per the following:

- If (2.43) holds and $\gamma \in \Delta^+$, the contradiction arises from the fact that $\ell(\gamma, x)$ would have to be simultaneously bigger than $\ell(\alpha', d')$ and smaller than $\ell(\beta, e)$.
- If (2.43) holds and $\gamma \in \Delta^-$, the contradiction arises from the fact that $\ell(-\gamma, -x)$ would have to be simultaneously bigger than $\ell(\beta', e')$ and smaller than $\ell(\alpha, d)$.
- If (2.44) holds and $\gamma \in \Delta^+$, the contradiction arises from the fact that $\ell(\gamma, x)$ would have to be simultaneously bigger than $\ell(\alpha', d')$ and smaller than $\ell(\alpha, d)$.
- If (2.44) holds and $\gamma \in \Delta^-$, the contradiction arises from the fact that $\ell(-\gamma, -x)$ would have to be simultaneously bigger than $\ell(\beta', e')$ and smaller than $\ell(\beta, e)$.

In Case 2, the only situation when (2.40) and (2.41) are compatible would be if:

$$\ell(\beta, e) = \ell(\alpha', d')w \tag{2.45}$$

for some loop word w, which would need to satisfy:

$$\ell(\beta', e') > w > \ell(\beta, e)$$

(the first inequality is a consequence of (2.40) and (2.41), while the second inequality is a consequence of the fact that $\ell(\beta, e)$ is Lyndon). However, being a suffix of a standard loop word, w is also standard and hence admits a canonical factorization:

$$w = \ell(\gamma_1, f_1) \dots \ell(\gamma_k, f_k)$$

for various $(\gamma_r, f_r) \in \Delta^+ \times \mathbb{Z}$ which satisfy $\ell(\gamma_r, f_r) \leq \ell(\gamma_1, f_1) \leq w < \ell(\beta', e')$ for all $1 \leq r \leq k$. However, (2.45) implies:

$$(\beta, e) = (\alpha', d') + \sum_{r=1}^{k} (\gamma_r, f_r) \quad \Rightarrow \quad (\beta', e') = (\alpha, d) + \sum_{r=1}^{k} (\gamma_r, f_r)$$

Because $\alpha, \gamma_1, \dots, \gamma_k, \beta'$ are all positive roots, we claim that there exist positive roots $\epsilon_1, \dots, \epsilon_k$ and a permutation $\sigma \in S(k)$ such that:

$$\epsilon_r = \alpha + \gamma_{\sigma(1)} + \cdots + \gamma_{\sigma(r)} \quad \forall\, r \in \{1, \ldots, k\} \tag{2.46}$$

Since $\ell(\alpha, d)$ and all the $\ell(\gamma_r, f_r)$ are $< \ell(\beta', e')$, then the induction hypothesis of (2.39) implies (inductively in r) that:

$$\ell(\epsilon_r, d + f_{\sigma(1)} + \cdots + f_{\sigma(r)}) < \ell(\beta', e')$$

However, $(\epsilon_k, d + f_1 + \cdots + f_k) = (\beta', e')$, which provides the required contradiction.

It remains to prove (2.46), which we will do by induction on k, the base case $k = 1$ being trivial. If $(\alpha, \gamma_r) < 0$ for some r, then the reflection $s_\alpha(\gamma_r) = \gamma_r + p\alpha$ is also a root, for some positive integer $p > 0$. This implies that $\alpha + \gamma_r$ is a root, hence we can apply the induction hypothesis for the collection of positive roots $(\alpha+\gamma_r, \gamma_1, \ldots, \gamma_{r-1}, \gamma_{r+1}, \ldots, \gamma_k, \beta')$. The analogous argument applies if $(\beta', \gamma_r) > 0$ for some r, in which case we can apply the induction hypothesis for the collection of positive roots $(\alpha, \gamma_1, \ldots, \gamma_{r-1}, \gamma_{r+1}, \ldots, \gamma_k, \beta' - \gamma_r)$. Hence the only situation when we could not prove the claim via the argument above would be if:

$$(\alpha, \gamma_r) \geq 0 \geq (\beta', \gamma_r) \quad \forall r \qquad \Rightarrow \qquad (\alpha, \beta' - \alpha) \geq 0 \geq (\beta', \beta' - \alpha)$$

But this would imply $(\beta' - \alpha, \beta' - \alpha) \leq 0$, which is impossible since $\beta' - \alpha \neq 0$. $\square$

Remark 2.36. We note that such "lexicographic order on Lyndon words are convex" results are well-known in representation theory, see e.g. [1] for slightly different (but more systematic and general) setting from ours.

Corollary 2.37. *Consider any $k, k' \geq 1$ and any:*

$$(\gamma_1, d_1), \ldots, (\gamma_k, d_k), (\gamma'_1, d'_1), \ldots, (\gamma'_{k'}, d'_{k'}) \in \Delta^+ \times \mathbb{Z}$$

such that:

$$(\gamma_1, d_1) + \cdots + (\gamma_k, d_k) = (\gamma'_1, d'_1) + \cdots + (\gamma'_{k'}, d'_{k'}) \tag{2.47}$$

Then we have:

$$\min\Big\{\ell(\gamma_1, d_1), \ldots, \ell(\gamma_k, d_k)\Big\} \leq \max\Big\{\ell(\gamma'_1, d'_1), \ldots, \ell(\gamma'_{k'}, d'_{k'})\Big\} \tag{2.48}$$

Proof. Proposition 2.34 is simply the $(k, k') \in \{(1, 2), (2, 1)\}$ case of the Corollary. Let us prove the Corollary by induction on $\min(k, k')$, and to break ties, by $k + k'$. This means that we must start with the case $\min(k, k') = 1$, and we will show how to deal with the $k' = 1$ case (as the $k = 1$ case is an analogous exercise that we leave to the interested reader). The assumption implies that $\gamma_1 + \cdots + \gamma_k \in \Delta^+$, in which case (2.46) shows that we can relabel indices such that $\gamma_1 + \gamma_2 \in \Delta^+$. Then the induction hypothesis shows that:

$$\min\left\{\ell(\gamma_1+\gamma_2,d_1+d_2),\ell(\gamma_3,d_3),\dots,\ell(\gamma_k,d_k)\right\}\le\ell(\gamma_1+\dots+\gamma_k,d_1+\dots+d_k)$$

Then Proposition 2.34 for (γ_1,d_1) and (γ_2,d_2) implies that the left-hand side is $\geq$ the minimum of all the $\ell(\gamma_s,d_s)$'s, as we needed to prove.

Let us now assume that $k,k'>1$. Since:

$$\gamma_1+\dots+\gamma_k=\gamma'_1+\dots+\gamma'_{k'}$$

there exist s,s' such that $(\gamma_s,\gamma'_{s'})>0$. Let us relabel indices such that $s=s'=1$. As we saw in the proof of Claim 2.35, this implies that:

$$(\gamma'_1,d'_1)=(\gamma_1,d_1)+(\epsilon,x)$$

for some $\epsilon\in\Delta\sqcup\{0\}$ and some $x\in\mathbb{Z}$. Then (2.47) implies:

$$(\gamma_2,d_2)+\dots+(\gamma_k,d_k)=(\gamma'_2,d'_2)+\dots+(\gamma'_{k'},d'_{k'})+(\epsilon,x)$$

If $\epsilon\in\Delta^+$, then the induction hypothesis gives us:

$$\min\left\{\ell(\gamma_1,d_1),\ell(\epsilon,x)\right\}\le\ell(\gamma'_1,d'_1)$$
$$\min\left\{\ell(\gamma_2,d_2),\dots,\ell(\gamma_k,d_k)\right\}\le\max\left\{\ell(\epsilon,x),\ell(\gamma'_2,d'_2),\dots,\ell(\gamma'_{k'},d'_{k'})\right\}$$

which implies (2.48). If $\epsilon\in\Delta^-$, then the induction hypothesis gives us:

$$\ell(\gamma_1,d_1)\le\max\left\{\ell(-\epsilon,-x),\ell(\gamma'_1,d'_1)\right\}$$
$$\min\left\{\ell(-\epsilon,-x),\ell(\gamma_2,d_2),\dots,\ell(\gamma_k,d_k)\right\}\le\max\left\{\ell(\gamma'_2,d'_2),\dots,\ell(\gamma'_{k'},d'_{k'})\right\}$$

which also implies (2.48). Finally, if $\epsilon=0$ and $x\le 0$, then Proposition 2.25 implies that $\ell(\gamma_1,d_1)\le\ell(\gamma'_1,d'_1)$, which easily yields (2.48). If $\epsilon=0$ and $x>0$, then:

$$\min\left\{\ell(\gamma_2,d_2),\dots,\ell(\gamma_k,d_k)\right\}\le\min\left\{\ell(\gamma_2,d_2-x),\ell(\gamma_3,d_3),\dots,\ell(\gamma_k,d_k)\right\}\le$$
$$\le\max\left\{\ell(\gamma'_2,d'_2),\dots,\ell(\gamma'_{k'},d'_{k'})\right\}$$

where the first inequality is due to (2.32) and the second inequality holds because of the induction hypothesis. The chain of inequalities above implies (2.48). $\square$

Proposition 2.38. *If $\ell_1<\ell_2$ are standard Lyndon loop words such that $\ell_1\ell_2$ is also a standard Lyndon loop word, then we cannot have:*

$$\ell_1<\ell'_1<\ell'_2<\ell_2$$

for standard Lyndon loop words ℓ'_1, ℓ'_2 *such that* $\deg \ell_1 + \deg \ell_2 = \deg \ell'_1 + \deg \ell'_2$.

Proof. Assume such ℓ'_1, ℓ'_2 existed. Then by (2.24), we would have:

$$\ell'_1 \ell'_2 \leq \ell_1 \ell_2 \tag{2.49}$$

The only way this is compatible with $\ell_1 < \ell'_1$ is if:

$$\ell'_1 = \ell_1 w$$

for some loop word w, which must be standard due to Proposition 2.15 (or more precisely, its straightforward loop generalization). However, (2.49) then implies:

$$w \ell'_2 \leq \ell_2 \tag{2.50}$$

If we consider the canonical factorization (2.7) of $w = u_1 \dots u_k$ for standard Lyndon loop words $u_1 \geq \dots \geq u_k$, then (2.50) implies that:

$$u_k \leq \dots \leq u_1 < \ell_2$$

Together with the assumption that $\ell'_2 < \ell_2$, this violates Corollary 2.37 since:

$$\deg u_1 + \dots + \deg u_k + \deg \ell'_2 = \deg w + \deg \ell'_2 = \deg \ell'_1 - \deg \ell_1 + \deg \ell'_2 = \deg \ell_2 \quad \square$$

3. Lyndon words and Weyl groups

In the present Section, we will show that the lexicographic order (1.16) on $\Delta^+ \times \mathbb{Z}$ induced by (2.35) is closely related to the construction of [35,36] applied to a reduced decomposition of a certain translation element in the extended affine Weyl group associated to $\mathfrak{g}$. The reader who is interested in quantum groups, and prepared to accept the proof of Theorem 3.14, may skip ahead to Section 4.

3.1. Let us consider the affine root system of type $\mathfrak{g}$:

$$\widehat{\Delta} = \widehat{\Delta}^+ \sqcup \widehat{\Delta}^- \subset \widehat{Q}$$

The affine root system has one more simple root α_0 besides the simple roots $\{\alpha_i\}_{i \in I}$ of the finite root system. Therefore, we may use formulas (2.1) for I replaced by:

$$\widehat{I} = I \sqcup 0$$

which lead to the affine Cartan matrix $(a_{ij})_{i,j \in \widehat{I}}$ and the affine symmetrized Cartan matrix $(d_{ij})_{i,j \in \widehat{I}}$. There is a natural identification:

$$\widehat{Q} \xrightarrow{\sim} Q \times \mathbb{Z} \qquad \text{with} \qquad \alpha_i \mapsto (\alpha_i, 0) \quad \forall\, i \in I, \quad \alpha_0 \mapsto (-\theta, 1) \tag{3.1}$$

where $\theta \in \Delta^+$ is the highest root of the finite root system. Note that $(0, 1) \in Q \times \mathbb{Z}$ is the minimal imaginary root of the affine root system. With this in mind, we have the following explicit description of the affine root system in terms of finite roots:

$$\widehat{\Delta}^+ = \left\{\Delta^+ \times \mathbb{Z}_{\geq 0}\right\} \sqcup \left\{0 \times \mathbb{Z}_{>0}\right\} \sqcup \left\{\Delta^- \times \mathbb{Z}_{>0}\right\} \tag{3.2}$$

$$\widehat{\Delta}^- = \left\{\Delta^- \times \mathbb{Z}_{\leq 0}\right\} \sqcup \left\{0 \times \mathbb{Z}_{<0}\right\} \sqcup \left\{\Delta^+ \times \mathbb{Z}_{<0}\right\} \tag{3.3}$$

where $\mathbb{Z}_{\geq 0}$, $\mathbb{Z}_{>0}$, $\mathbb{Z}_{\leq 0}$, $\mathbb{Z}_{<0}$ denote the obvious subsets of $\mathbb{Z}$.

Definition 3.2. Let $\widehat{\mathfrak{g}}$ be as in Definition 2.2, but using $\widehat{I}$ instead of I.

As opposed from the non-degenerate pairing on finite type root systems, the pairing on affine type root systems has a 1-dimensional kernel, which is spanned by the imaginary root. Explicitly, this implies the fact that:

$$(\alpha_0 + \theta, -) = 0 \quad \Leftrightarrow \quad d_{0j} + \sum_{i \in I} \theta_i d_{ij} = 0$$

for all $j \in I$, where the positive integers $\{\theta_i\}_{i \in I}$ (called the "labels" of the corresponding extended Dynkin diagram) are defined via:

$$\theta = \sum_{i \in I} \theta_i \alpha_i \tag{3.4}$$

Using formula (2.3), this implies that the Cartan element:

$$c = h_0 + \sum_{i \in I} \theta_i h_i \tag{3.5}$$

is central in $\widehat{\mathfrak{g}}$. Furthermore, we have the following relation between $\widehat{\mathfrak{g}}$ and $L\mathfrak{g}$.

Lemma 3.3. *There exists a Lie algebra isomorphism:*

$$\widehat{\mathfrak{g}}/(c) \xrightarrow{\sim} L\mathfrak{g}$$

determined by the formulas:

$$\begin{aligned} e_i &\mapsto e_i \otimes t^0 & \qquad e_0 &\mapsto f_\theta \otimes t^1 \\ f_i &\mapsto f_i \otimes t^0 & \qquad f_0 &\mapsto e_\theta \otimes t^{-1} \\ h_i &\mapsto h_i \otimes t^0 & \qquad h_0 &\mapsto -\sum_{i \in I} \theta_i h_i \otimes t^0 \end{aligned}$$

for all $i \in I$, where e_θ (resp. f_θ) is a root vector of degree θ (resp. $-\theta$).

3.4. We have already mentioned that convex orders of Δ^+ are in 1-to-1 correspondence with reduced decompositions of the longest element of the finite Weyl group W associated to $\mathfrak{g}$. To define the latter explicitly, consider the coroot lattice:

$$Q^\vee = \bigoplus_{i \in I} \mathbb{Z} \cdot \alpha_i^\vee \tag{3.6}$$

where for any $\alpha \in \Delta^+$ the corresponding coroot $\alpha^\vee$ is defined via:

$$\alpha^\vee = \frac{2\alpha}{(\alpha, \alpha)} \tag{3.7}$$

The finite Weyl group W, i.e. the abstract Coxeter group associated to the Cartan matrix $(a_{ij})_{i,j \in I}$, acts faithfully on the coroot lattice $Q^\vee$ as well as on the root lattice Q:

$$W \curvearrowright Q^\vee \qquad \text{and} \qquad W \curvearrowright Q \tag{3.8}$$

via the following assignments:

$$s_i(\mu) = \mu - (\alpha_i, \mu)\alpha_i^\vee \qquad \text{and} \qquad s_i(\lambda) = \lambda - (\lambda, \alpha_i^\vee)\alpha_i \tag{3.9}$$

$\forall\, i \in I$, $\mu \in Q^\vee$, $\lambda \in Q$.

3.5. We will also encounter the affine Weyl group, which is by definition the semidirect product:

$$\widehat{W} = W \ltimes Q^\vee \tag{3.10}$$

defined with respect to the action (3.8). It is well-known that $\widehat{W}$ is also the Coxeter group associated to the Cartan matrix $(a_{ij})_{i,j \in \hat{I}}$. In other words, the affine Weyl group is generated by the symbols $\{s_i\}_{i \in \hat{I}}$ defined by:

$$\begin{aligned} s_i &= (s_i, 0), \quad \forall\, i \in I \\ s_0 &= (s_\theta, -\theta^\vee) \end{aligned}$$

The affine analogue of the action $W \curvearrowright Q$ from the previous Subsection is:

$$\widehat{W} \curvearrowright \widehat{Q} \tag{3.11}$$

where the generators of the affine Weyl group act by the following formulas:

$$s_i(\lambda, d) = (\lambda - (\lambda, \alpha_i^\vee)\alpha_i, d)\,, \quad \forall\, i \in I \tag{3.12}$$

$$s_0(\lambda, d) = (\lambda - (\lambda, \theta^\vee)\theta, d + (\lambda, \theta^\vee)) \tag{3.13}$$

for all $(\lambda, d) \in Q \times \mathbb{Z} \simeq \widehat{Q}$, see (3.1). An important feature of the affine Weyl group is that it contains a large commutative subalgebra:

$$1 \ltimes Q^\vee \subset \widehat{W}$$

which acts on the affine root lattice $\widehat{Q} \simeq Q \times \mathbb{Z}$ by translations:

$$\widehat{\mu}(\lambda, d) = (\lambda, d - (\lambda, \mu)) \tag{3.14}$$

$\forall\, \mu \in Q^\vee$, $\lambda \in Q$, $d \in \mathbb{Z}$. Here and henceforth, we write $\widehat{\mu}$ for the element $1 \ltimes \mu \in \widehat{W}$, and call it a translation element.

3.6. We will also need to consider the extended affine Weyl group, which is by definition the semidirect product:

$$\widehat{W}^{\text{ext}} = W \ltimes P^\vee \tag{3.15}$$

Above, $P^\vee$ is the coweight lattice:

$$P^\vee = \bigoplus_{i \in I} \mathbb{Z} \cdot \omega_i^\vee \tag{3.16}$$

where the fundamental coweights $\{\omega_i^\vee\}_{i \in I}$ are dual to the simple roots $\{\alpha_j\}_{j \in I}$:

$$(\alpha_j, \omega_i^\vee) = \delta_i^j \tag{3.17}$$

In particular, $Q^\vee$ is a finite index subgroup of $P^\vee$. It is well-known that:

$$\widehat{W}^{\text{ext}} \simeq \mathcal{T} \ltimes \widehat{W} \tag{3.18}$$

where the finite subgroup $\mathcal{T}$ of $\widehat{W}^{\text{ext}}$ is naturally identified with a subgroup of automorphisms of the Dynkin diagram of $\widehat{\mathfrak{g}}$. The semi-direct product (3.18) is such that:

$$\tau s_i = s_{\tau(i)} \tau, \qquad \forall\, \tau \in \mathcal{T}, i \in \widehat{I}$$

Finally, the action (3.11) extends to:

$$\widehat{W}^{\text{ext}} \curvearrowright \widehat{Q} \tag{3.19}$$

via:

$$\tau(\alpha_i) = \alpha_{\tau(i)}, \qquad \forall\, \tau \in \mathcal{T}, i \in \widehat{I}$$

We still have the following formula, akin to (3.14):

$$\widehat{\mu}(\lambda, d) = (\lambda, d - (\lambda, \mu)) \tag{3.20}$$

$\forall\, \mu \in P^\vee$, $\lambda \in Q$, $d \in \mathbb{Z}$, where $\widehat{\mu}$ denotes the translation element $1 \ltimes \mu \in \widehat{W}^{\mathrm{ext}}$.

3.7. Recall that the length of an element $x \in \widehat{W}$, denoted by $l(x) \in \mathbb{N}$, is the smallest number $l \in \mathbb{N}$ such that we can write:

$$x = s_{i_{1-l}} \dots s_{i_0} \tag{3.21}$$

for various $i_{1-l}, \dots, i_0 \in \widehat{I}$. Every factorization (3.21) with $l = l(x)$ is called a reduced decomposition of x. Given such a reduced decomposition, the terminal subset (a priori, a multiset) of the affine root system is:

$$E_x = \left\{ s_{i_0} s_{i_{-1}} \dots s_{i_{k+1}}(\alpha_{i_k}) \Big| 0 \geq k > -l \right\} \subset \widehat{\Delta} \tag{3.22}$$

It is well-known that E_x is independent of the reduced decomposition of x, and consists of the positive affine roots (all with multiplicity one) that are mapped to negative ones under the action of x:

$$E_x = \left\{ \widetilde{\lambda} \in \widehat{\Delta}^+ \Big| x(\widetilde{\lambda}) \in \widehat{\Delta}^- \right\} \tag{3.23}$$

In particular, we get the following description of the length of x:

$$l(x) = \# \left\{ \widetilde{\lambda} \in \widehat{\Delta}^+ \Big| x(\widetilde{\lambda}) \in \widehat{\Delta}^- \right\} \tag{3.24}$$

The aforementioned length function $l \colon \widehat{W} \to \mathbb{N}$ naturally extends to $\widehat{W}^{\mathrm{ext}}$ via:

$$l(\tau w) = l(w), \qquad \forall\, \tau \in \mathcal{T}, w \in \widehat{W}$$

Thus, the length $l(x)$ of $x \in \widehat{W}^{\mathrm{ext}}$ is the smallest number l such that we can write:

$$x = \tau s_{i_{1-l}} \dots s_{i_0} \tag{3.25}$$

for various $i_{1-l}, \dots, i_0 \in \widehat{I}$ and (uniquely determined) $\tau \in \mathcal{T}$. Given a reduced decomposition of $x \in \widehat{W}^{\mathrm{ext}}$ as in (3.25) with $l = l(x)$, define E_x via (3.22). We note that E_x is still described via (3.23) since τ acts by permuting negative affine roots. Therefore, E_x is independent of the reduced decomposition of x and we still have:

$$l(x) = \# \left\{ \widetilde{\lambda} \in \widehat{\Delta}^+ \Big| x(\widetilde{\lambda}) \in \widehat{\Delta}^- \right\} \tag{3.26}$$

Remark 3.8. A restricted case of the discussion above is when $\widehat{W}, \widehat{\Delta}$ are replaced by W, Δ. In this case, applying (3.23) to the longest element $w_0 \in W$ yields $E_{w_0} = \Delta^+$.

Furthermore, choosing a reduced decomposition $w_0 = s_{i_{1-l}} \dots s_{i_0}$ amounts to placing a total order on $E_{w_0} = \Delta^+$ via:

$$\alpha_{i_0} < s_{i_0}(\alpha_{i_{-1}}) < \dots < s_{i_0} s_{i_{-1}} \dots s_{i_{2-l}}(\alpha_{i_{1-l}}) \tag{3.27}$$

According to [34], this total order of Δ^+ is convex (see Definition 2.19), and conversely, any convex order of Δ^+ arises in this way for a certain (unique) reduced decomposition of w_0. We will study the affine version of this picture in Subsection 3.10.

Let us recall the element $\rho \in \frac{1}{2}Q$ defined by:

$$\rho = \frac{1}{2} \sum_{\alpha \in \Delta^+} \alpha$$

The following result is standard ([22, Exercise 6.10]).

Proposition 3.9. *For any $\mu \in P^\vee$ such that $(\alpha_i, \mu) \in \mathbb{N}$ for all $i \in I$:*

$$l(\widehat{\mu}) = (2\rho, \mu)$$

Proof. Applying formula (3.20) for the action of $\widehat{\mu} \in \widehat{W}^{\mathrm{ext}}$ on $\widehat{Q} \simeq Q \times \mathbb{Z}$, we see that the only positive affine roots $\widetilde{\lambda} \in \widehat{\Delta}^+$ that are mapped to negative ones are:

$$\Big\{ (\alpha, d) \Big| \alpha \in \Delta^+, 0 \le d < (\alpha, \mu) \Big\} \tag{3.28}$$

Combining this with formula (3.26), we find

$$l(\widehat{\mu}) = \sum_{\alpha \in \Delta^+} (\alpha, \mu) = (2\rho, \mu) \quad \square$$

3.10. Let us pick any $\mu \in P^\vee$ such that $(\alpha_i, \mu) \in \mathbb{N}$ for all $i \in I$. Let $l = (2\rho, \mu)$ be the length of $\widehat{\mu} \in \widehat{W}^{\mathrm{ext}}$ (Proposition 3.9) and consider any reduced decomposition:

$$\widehat{\mu} = \tau s_{i_{1-l}} s_{i_{2-l}} \dots s_{i_0} \tag{3.29}$$

Extend $i_{1-l}, \dots, i_0$ to a (τ-quasiperiodic) bi-infinite sequence $\{i_k\}_{k \in \mathbb{Z}}$ via:

$$i_{k+l} = \tau(i_k), \qquad \forall\, k \in \mathbb{Z} \tag{3.30}$$

To such a bi-infinite sequence (3.30), one assigns the following bi-infinite sequence of affine roots:

$$\beta_k = \begin{cases} s_{i_1} s_{i_2} \dots s_{i_{k-1}}(-\alpha_{i_k}) & \text{if } k > 0 \\ s_{i_0} s_{i_{-1}} \dots s_{i_{k+1}}(\alpha_{i_k}) & \text{if } k \le 0 \end{cases} \tag{3.31}$$

According to [35,36], the sequences:

$$\beta_1 > \beta_2 > \beta_3 > \dots \tag{3.32}$$

$$\beta_0 < \beta_{-1} < \beta_{-2} < \dots \tag{3.33}$$

give convex orders of the sets $\Delta^+ \times \mathbb{Z}_{<0}$ and $\Delta^+ \times \mathbb{Z}_{\geq 0}$, respectively.

Remark 3.11. The above exposition follows that of [6] as we consider $\mu \in P^\vee$. To reduce it to the setup of [2,35,36], where only elements of $Q^\vee$ are treated, we note that if $r \in \mathbb{N}$ is the order of τ, then $r\mu \in Q^\vee$, $s_{i_{1-rl}} s_{i_{2-rl}} \dots s_{i_{-1}} s_{i_0}$ is a reduced decomposition of $\widehat{r\mu}$, and the sequence $\{i_k\}_{k\in\mathbb{Z}}$ is periodic with period $l(\widehat{r\mu}) = rl$.

Remark 3.12. For any $k \in \mathbb{Z}$, if $\beta_k = (\alpha, d)$ and $\beta_{k+l} = (\alpha', d')$, then:

$$\beta_{k+l} = \widehat{\mu}(\beta_k) \qquad \Rightarrow \qquad \alpha = \alpha' \text{ and } d = d' + (\alpha, \mu) \tag{3.34}$$

due to (3.20). This reveals a periodicity of the entire set $\Delta^+ \times \mathbb{Z}$, not just of its two halves $\Delta^+ \times \mathbb{Z}_{<0}$ and $\Delta^+ \times \mathbb{Z}_{\geq 0}$ (it is also the reason for the minus sign in (3.31)).

3.13. Recall the element $\rho^\vee \in P^\vee \cap \frac{1}{2} Q^\vee$ defined by:

$$\rho^\vee = \sum_{i \in I} \omega_i^\vee = \frac{1}{2} \sum_{\alpha \in \Delta^+} \alpha^\vee$$

The following is the main result of this Section.

Theorem 3.14. *There exists a reduced decomposition of $\widehat{\rho^\vee} \in \widehat{W}^{\text{ext}}$ such that:*

- *the order (3.32) of the roots $\{(\alpha, d) | \alpha \in \Delta^+, d < 0\}$ matches the lexicographic order of the standard Lyndon loop words $\ell(\alpha, -d)$ via (1.16),*
- *the order (3.33) of the roots $\{(\alpha, d) | \alpha \in \Delta^+, d \geq 0\}$ matches the lexicographic order of the standard Lyndon loop words $\ell(\alpha, -d)$ via (1.16).*

The second bullet implies that i_0 equals the smallest letter in I. On the other hand, combining $s_{i_1} \rho^\vee = s_{\tau(i_{1-l})} \tau s_{i_{1-l}} s_{i_{2-l}} \dots s_{i_0} = \tau s_{i_{2-l}} \dots s_{i_0}$ with the fact that $l(s_j \rho^\vee) > l(\rho^\vee)$ $\forall j \in I$ (a consequence of (3.26)), implies that $i_1 = 0$.

Proof of Theorem 3.14. Consider the finite subset:

$$L = \left\{ (\alpha, d) \middle| \alpha \in \Delta^+, 0 \leq d < |\alpha| \right\}$$

of $\widehat{\Delta}^+$, ordered via:

$$(\alpha, d) < (\beta, e) \quad \Leftrightarrow \quad \ell(\alpha, -d) < \ell(\beta, -e) \tag{3.35}$$

If $(\alpha, d), (\beta, e) \in L$, $(\alpha, d) < (\beta, e)$ and $(\alpha+\beta, d+e) \in \widehat{\Delta}$, then clearly $(\alpha+\beta, d+e) \in L$, as well as $(\alpha, d) < (\alpha+\beta, d+e) < (\beta, e)$, due to Proposition 2.34.

Furthermore, we claim that if $\widetilde{\lambda}, \widetilde{\mu} \in \widehat{\Delta}^+$ with $\widetilde{\lambda}+\widetilde{\mu} \in L$, then at least one of $\widetilde{\lambda}$ or $\widetilde{\mu}$ belongs to L and is $< \widetilde{\lambda}+\widetilde{\mu}$. This is obvious when $\widetilde{\lambda} = (\alpha, d)$, $\widetilde{\mu} = (\beta, e)$ with $\alpha, \beta \in \Delta^+$ and $d, e \geq 0$. In the remaining case, we may assume $\widetilde{\lambda} = (\alpha+\beta, d), \widetilde{\mu} = (-\beta, e)$, so that $\alpha, \beta, \alpha+\beta \in \Delta^+$ and $d \geq 0, e > 0$. Then $d < d+e < |\alpha| < |\alpha+\beta|$, so that $\widetilde{\lambda} \in L$. It remains to verify $\widetilde{\lambda} < \widetilde{\lambda}+\widetilde{\mu}$, that is, $\ell(\alpha+\beta, -d) < \ell(\alpha, -d-e)$. Since $(\alpha+\beta, -d) = (\beta, e) + (\alpha, -d-e)$, it suffices to prove $\ell(\beta, e) < \ell(\alpha, -d-e)$, due to Proposition 2.34. But applying Proposition 2.26, we see that the exponent of the first letter in $\ell(\beta, e)$ is > 0, while the exponent of the first letter in $\ell(\alpha, -d-e)$ is ≤ 0, hence, indeed $\ell(\beta, e) < \ell(\alpha, -d-e)$.

Invoking [34] (which also applies to finite subsets in affine root systems), we get:

(I) there is a unique element $w \in \widehat{W}$ such that $L = E_w$
(II) the order of L arises via a certain reduced decomposition of w, cf. (3.27).

However, as noticed in our proof of Proposition 3.9, we have

$$L = E_{\widehat{\rho^\vee}} = \Big\{\beta_0, \beta_{-1}, \dots, \beta_{1-l}\Big\}$$

There is a unique $\tau \in \mathcal{T}$ such that $\tau^{-1}\widehat{\rho^\vee} \in \widehat{W}$ (note that $\tau^2 = 1$ since $2\rho^\vee \in Q^\vee$). Then:

$$L = E_{\widehat{\rho^\vee}} = E_{\tau^{-1}\widehat{\rho^\vee}}$$

Therefore, in view of the uniqueness statement of (I), the result of (II) implies that there exists a reduced decomposition (3.29) of $\widehat{\rho^\vee}$ such that the ordered finite sequence $\beta_0 < \beta_{-1} < \cdots < \beta_{1-l}$ exactly coincides with L ordered via (3.35).

The proof of Theorem 3.14 now follows by a simple combination of (3.34) and Propositions 2.26, 2.30. Indeed, let us split $\Delta^+ \times \mathbb{Z}$ into the blocks:

$$L_N = \Big\{(\alpha, d)\Big|\alpha \in \Delta^+, N|\alpha| \leq d < (N+1)|\alpha|\Big\}$$

so that:

$$\bigsqcup_{N \geq 0} L_N = \Delta^+ \times \mathbb{Z}_{\geq 0} = \{\beta_k\}_{k \leq 0}$$

$$\bigsqcup_{N < 0} L_N = \Delta^+ \times \mathbb{Z}_{<0} = \{\beta_k\}_{k > 0}$$

According to (3.34) and $L_0 = L = \{\beta_0, \dots, \beta_{1-l}\}$, we have:

$$L_N = \left\{\beta_{-Nl}, \beta_{-Nl-1}, \dots, \beta_{1-(N+1)l}\right\}, \qquad \forall\, N \in \mathbb{Z}$$

For any $(\alpha, d) \in L_N$, the exponent of the first letter in $\ell(\alpha, -d)$ is $-N$, due to Proposition 2.26 (and its proof). Therefore, for any $(\alpha, d) \in L_M, (\beta, e) \in L_N$ with $M > N$, we have $\ell(\alpha, -d) > \ell(\beta, -e)$. As for the affine roots from the same block, consider $\beta_{r-Nl}, \beta_{s-Nl} \in L_N$ with $1 - l \leq s < r \leq 0$. If $\beta_r = (\alpha, d)$ and $\beta_s = (\beta, e)$, then $\beta_{r-Nl} = (\alpha, d + N|\alpha|)$ and $\beta_{s-Nl} = (\beta, e + N|\beta|)$, due to (3.34). On the other hand, the words $\ell(\alpha, -d - N|\alpha|)$ and $\ell(\beta, -e - N|\beta|)$ are obtained from $\ell(\alpha, -d)$ and $\ell(\beta, -e)$, respectively, by decreasing each exponent by N, due to Proposition 2.30. Since the latter operation obviously preserves the lexicographic order, and $\ell(\alpha, -d) < \ell(\beta, -e)$ as a consequence of $r > s$, we obtain the required inequality $\ell(\alpha, -d - N|\alpha|) < \ell(\beta, -e - N|\beta|)$. □

We actually have the stronger result that the order of $\Delta^+ \times \mathbb{Z}$ given by:

$$\cdots < \beta_3 < \beta_2 < \beta_1 < \beta_0 < \beta_{-1} < \beta_{-2} < \cdots \tag{3.36}$$

matches the lexicographic order of the standard Lyndon loop words $\ell(\alpha, -d)$ (since $\ell(\alpha, -d) < \ell(\beta, -e)$ if $d < 0 \leq e$, itself a consequence of Proposition 2.26).

Remark 3.15. We expect that a similar treatment can be done for any $\mu \in P^\vee$ such that $(\alpha_i, \mu) > 0$ for all $i \in I$. On the side of Lyndon loop words, this would require an analogue of Proposition 2.30 stating that $\ell(\alpha, d + (\alpha, \mu))$ is obtained from $\ell(\alpha, d)$ by adding (α_i, μ) to all the exponents of letters $i \in I$. For this operation to preserve the property of words being Lyndon, one can replace the order (1.12) on loop letters $\{i^{(d)}\}_{i \in I}^{d \in \mathbb{Z}}$ by:

$$i^{(d)} < j^{(e)} \quad \text{if} \quad \begin{cases} \frac{d}{(\alpha_i, \mu)} > \frac{e}{(\alpha_j, \mu)} \\ \text{or} \\ \frac{d}{(\alpha_i, \mu)} = \frac{e}{(\alpha_j, \mu)} \text{ and } i < j \end{cases}$$

We expect the contents of Sections 2 and 3 to carry through in this more general setup, but we make no claims in this regard.

4. Quantum groups and shuffle algebras

We will review the connection between Drinfeld-Jimbo quantum groups and shuffle algebras, following [15,38,40]. We will also recall the point of view of [27] (see also [39]), which connects shuffle algebras with the notion of standard Lyndon words. Then we develop a loop version of this treatment, and prove Theorem 1.5.

We start with the exposition of the relevant results for finite quantum groups in Subsections 4.1–4.14, following the aforementioned references [15,38,40] and [27].

4.1. Let us recall the notation of Subsection 2.1 which, as we have seen, corresponds to a finite-dimensional simple Lie algebra $\mathfrak{g}$. Consider the q-numbers, q-factorials and q-binomial coefficients:

$$[k]_i = \frac{q_i^k - q_i^{-k}}{q_i - q_i^{-1}}, \qquad [k]!_i = [1]_i \dots [k]_i, \qquad \binom{n}{k}_i = \frac{[n]!_i}{[k]!_i [n-k]!_i}$$

for any $i \in I$, where $q_i = q^{\frac{d_{ii}}{2}}$.

Definition 4.2. The Drinfeld-Jimbo quantum group associated to $\mathfrak{g}$ is:

$$U_q(\mathfrak{g}) = \mathbb{Q}(q)\Big\langle e_i, f_i, \varphi_i^{\pm 1} \Big\rangle_{i \in I} \Big/ \text{relations (4.1)–(4.3)}$$

where we impose the following relations for all $i, j \in I$:

$$\sum_{k=0}^{1-a_{ij}} (-1)^k \binom{1-a_{ij}}{k}_i e_i^k e_j e_i^{1-a_{ij}-k} = 0, \qquad \text{if } i \neq j \tag{4.1}$$

$$\varphi_j e_i = q^{d_{ji}} e_i \varphi_j, \qquad \varphi_i \varphi_j = \varphi_j \varphi_i \tag{4.2}$$

as well as the opposite relations with e's replaced by f's, and finally the relation:

$$[e_i, f_j] = \delta_i^j \cdot \frac{\varphi_i - \varphi_i^{-1}}{q_i - q_i^{-1}} \tag{4.3}$$

If we let $\varphi_i = q_i^{h_i}$ and take the limit $q \to 1$, then $U_q(\mathfrak{g})$ degenerates to $U(\mathfrak{g})$.

4.3. Recall that $U_q(\mathfrak{g})$ is a bialgebra with respect to the coproduct ([21, §4.11]):

$$\begin{aligned} \Delta(\varphi_i) &= \varphi_i \otimes \varphi_i \\ \Delta(e_i) &= \varphi_i \otimes e_i + e_i \otimes 1 \\ \Delta(f_i) &= 1 \otimes f_i + f_i \otimes \varphi_i^{-1} \end{aligned}$$

This bialgebra structure preserves the Q-grading induced by setting ([21, §4.13]):

$$\deg e_i = \alpha_i, \quad \deg \varphi_i = 0, \quad \deg f_i = -\alpha_i$$

Recall the triangular decomposition ([21, §4.21]):

$$U_q(\mathfrak{g}) = U_q(\mathfrak{n}^+) \otimes U_q(\mathfrak{h}) \otimes U_q(\mathfrak{n}^-) \tag{4.4}$$

where $U_q(\mathfrak{n}^+), U_q(\mathfrak{h}), U_q(\mathfrak{n}^-)$ are the subalgebras of $U_q(\mathfrak{g})$ generated by the e_i's, $\varphi_i^{\pm 1}$'s, f_i's, respectively. We will also consider the following sub-bialgebras of $U_q(\mathfrak{g})$:

$$U_q(\mathfrak{b}^+) = U_q(\mathfrak{n}^+) \otimes U_q(\mathfrak{h})$$
$$U_q(\mathfrak{b}^-) = U_q(\mathfrak{h}) \otimes U_q(\mathfrak{n}^-)$$

Remark 4.4. As an associative algebra, $U_q(\mathfrak{n}^+)$ (resp. $U_q(\mathfrak{b}^+)$) is generated by e_i's (resp. $e_i, \varphi_i^{\pm 1}$'s) with the defining relations (4.1) (resp. (4.1), (4.2)), see e.g. [21, §4.21].

4.5. It is well-known ([21, §6.12]) that there is a non-degenerate bialgebra pairing[3]:

$$\langle \cdot, \cdot \rangle \colon U_q(\mathfrak{b}^+) \otimes U_q(\mathfrak{b}^-) \longrightarrow \mathbb{Q}(q) \tag{4.5}$$

where the word "bialgebra" means that it satisfies the following properties:

$$\langle a, bc \rangle = \langle \Delta(a), b \otimes c \rangle \tag{4.6}$$
$$\langle ab, c \rangle = \langle b \otimes a, \Delta(c) \rangle \tag{4.7}$$

for all applicable a, b, c. Then (4.5) is determined by the assignments:

$$\langle e_i, f_j \rangle = \frac{\delta_i^j}{q_i^{-1} - q_i}, \qquad \langle \varphi_i, \varphi_j \rangle = q^{-d_{ij}}$$

and the fact that

$$\langle a, b \rangle = 0 \quad \text{unless} \quad \deg a + \deg b = 0$$

The quantum group $U_q(\mathfrak{g})$ is the Drinfeld double of $(U_q(\mathfrak{b}^+), U_q(\mathfrak{b}^-), \langle \cdot, \cdot \rangle)$, which means that the multiplication map induces an isomorphism:

$$U_q(\mathfrak{b}^+) \otimes U_q(\mathfrak{b}^-) \Big/ (\varphi_i \otimes \varphi_i^{-1} - 1 \otimes 1) \xrightarrow{\sim} U_q(\mathfrak{g})$$

and that the commutation rule of the two factors is governed by the relation[4]:

$$a_1 b_1 \langle a_2, b_2 \rangle = \langle a_1, b_1 \rangle b_2 a_2 \tag{4.8}$$

for all $a \in U_q(\mathfrak{b}^+)$ and $b \in U_q(\mathfrak{b}^-)$. Here we use Sweedler notation $\Delta(a) = a_1 \otimes a_2$ for the coproduct of Subsection 4.3 (a summation sign is implied in front of $a_1 \otimes a_2$).

---

[3] Henceforth, given two algebras A, B over a ring K, a K-valued bilinear pairing $A \times B \to K$ shall be rather denoted $A \otimes B \to K$ (with $\otimes$ standing for $\otimes_K$) to indicate its K-bilinear nature.

[4] According to [33, Remark 2.4], formula (4.8) is equivalent to a more standard commutation rule appearing in the literature. We prefer our formula as it does not require us to define the antipode, which exists but will not be necessary in the present paper.

4.6. Since the quantum group of Definition 4.2 is a q-deformation of the universal enveloping of the Lie algebra of Definition 2.2, it is natural that many features of the latter admit q-deformations as well. For example, let us recall the notion of standard Lyndon words from Subsections 2.3–2.11, and consider the following q-version of the construction of Definition 2.9.

Definition 4.7. ([27]) For any word w, define $e_w \in U_q(\mathfrak{n}^+)$ by:

$$e_{[i]} = e_i$$

for all $i \in I$, and then recursively by:

$$e_\ell = [e_{\ell_1}, e_{\ell_2}]_q = e_{\ell_1} e_{\ell_2} - q^{(\deg \ell_1, \deg \ell_2)} e_{\ell_2} e_{\ell_1} \tag{4.9}$$

if ℓ is a Lyndon word with factorization (2.6), and:

$$e_w = e_{\ell_1} \dots e_{\ell_k} \tag{4.10}$$

if w is an arbitrary word with the canonical factorization $\ell_1 \dots \ell_k$, as in (2.7).

We also define $f_w \in U_q(\mathfrak{n}^-)$ by replacing e's by f's in the Definition above. Then we have the following q-deformation of the PBW statement (2.15).

Theorem 4.8. *We have:*

$$U_q(\mathfrak{n}^+) \ = \bigoplus_{\ell_1 \geq \dots \geq \ell_k \textit{ standard Lyndon words}}^{k \in \mathbb{N}} \mathbb{Q}(q) \cdot e_{\ell_1} \dots e_{\ell_k} \ = \bigoplus_{w \textit{ standard words}} \mathbb{Q}(q) \cdot e_w \tag{4.11}$$

The analogous result also holds with $+ \leftrightarrow -$ and $e \leftrightarrow f$.

This result is a consequence of the usual PBW theorem for $U_q(\mathfrak{n}^\pm)$, since e_ℓ's are simply renormalizations of the standard root vectors constructed in [30], according to [27, Theorem 28] (alternatively, the interested reader may find a detailed proof of this result in Subsections 5.1–5.5 of the arχiv-version of the present paper).

Remark 4.9. It's instructive to recall the argument of [27, Theorem 28]. Given any convex order $\leq$ of the set of positive roots Δ^+, as in Definition 2.19, Lusztig [30] established:

$$U_q(\mathfrak{n}^\pm) \ = \bigoplus_{\gamma_1 \leq \dots \leq \gamma_k \in \Delta^+}^{k \in \mathbb{N}} \mathbb{Q}(q) \cdot E_{\pm\gamma_1} \dots E_{\pm\gamma_k} \tag{4.12}$$

with the "root vectors" $E_{\pm\beta} \in U_q(\mathfrak{n}^{\pm})$, $\beta \in \Delta^+$, constructed using the braid group action. Following [28], these root vectors also satisfy the "convexity property":

$$E_{\pm\beta}E_{\pm\alpha} - q^{(\alpha,\beta)}E_{\pm\alpha}E_{\pm\beta} \in \bigoplus_{\substack{\alpha<\gamma_1\leq\cdots\leq\gamma_k<\beta \\ \gamma_1+\cdots+\gamma_k=\alpha+\beta}}^{k\in\mathbb{N}} \mathbb{Q}(q)\cdot E_{\pm\gamma_1}\dots E_{\pm\gamma_k} \tag{4.13}$$

for any positive roots $\alpha < \beta$. In particular, this implies that

$$[E_{\pm\beta}, E_{\pm\alpha}]_q := E_{\pm\beta}E_{\pm\alpha} - q^{(\alpha,\beta)}E_{\pm\alpha}E_{\pm\beta} \in \mathbb{Q}(q)^* \cdot E_{\pm(\alpha+\beta)} \tag{4.14}$$

whenever $\alpha+\beta$ is also a positive root such that its decomposition as the sum of α and β is minimal in the following sense:

$$\nexists\ \alpha', \beta' \in \Delta^+ \quad \text{s.t.} \quad \alpha < \alpha' < \beta' < \beta \quad \text{and} \quad \alpha+\beta = \alpha'+\beta' \tag{4.15}$$

The property (4.14) together with (the finite counterpart of) Proposition 2.38 allows to prove (by induction on the height of $\alpha \in \Delta^+$) that $e_{\ell(\alpha)} \in \mathbb{Q}(q)^* \cdot \varpi(E_{-\alpha})$, where ℓ is the bijection (2.13) and ϖ is the anti-isomorphism of $U_q(\mathfrak{g})$, determined by $e_i \mapsto f_i$, $f_i \mapsto e_i$, $\varphi_i \mapsto \varphi_i$. Hence, (4.11) is indeed a direct consequence of (4.12).

4.10. One of the main tools of [27] is the q-shuffle algebra interpretation of the quantum group $U_q(\mathfrak{n}^+)$, due to [15,38,40], which we recall now.

Definition 4.11. Consider the $\mathbb{Q}(q)$-vector space $\mathcal{F}$ with a basis given by words:

$$[i_1 \dots i_k] \tag{4.16}$$

for arbitrary $k \in \mathbb{N}$, $i_1, \dots, i_k \in I$, and endow it with the following shuffle product[5]:

$$[i_1 \dots i_k] * [j_1 \dots j_l] = \sum_{\substack{\{1,\dots,k+l\}=A\sqcup B \\ |A|=k, |B|=l}} q^{\lambda_{A,B}} \cdot [s_1 \dots s_{k+l}] \tag{4.17}$$

where in the right-hand side, if $A = \{a_1 < \dots < a_k\}$ and $B = \{b_1 < \dots < b_l\}$, we write:

$$s_c = \begin{cases} i_\bullet & \text{if } c = a_\bullet \\ j_\bullet & \text{if } c = b_\bullet \end{cases} \tag{4.18}$$

and:

[5] We note that formula (4.17) is worded differently from [27, formula (9)], but it is an immediate consequence of [27, formula (8)].

$$\lambda_{A,B} = \sum_{A \ni a > b \in B} d_{s_a s_b} \tag{4.19}$$

It is straightforward to see that $(\mathcal{F}, *)$ is an associative algebra. If we set $q = 1$, then $\mathcal{F}$ coincides with the classical shuffle algebra on the alphabet I. The classical shuffle algebra is actually a bialgebra, with coproduct defined by splitting words:

$$\Delta\left([i_1 \dots i_k]\right) = \sum_{a=0}^{k} [i_1 \dots i_a] \otimes [i_{a+1} \dots i_k]$$

But for generic q, the coproduct above is no longer multiplicative with respect to the shuffle product (4.17). To remedy this, we consider the extended shuffle algebra:

$$\mathcal{F}^{\text{ext}} = \mathcal{F} \otimes \mathbb{Q}(q) \left[\varphi_i^{\pm 1}\right]_{i \in I}$$

with pairwise commuting φ_i's, where the multiplication is governed by the rule:

$$\varphi_j \cdot [i_1 \dots i_k] = q^{\sum_{a=1}^{k} d_{j i_a}} [i_1 \dots i_k] \cdot \varphi_j \tag{4.20}$$

It is straightforward to check that the assignment $\Delta(\varphi_i) = \varphi_i \otimes \varphi_i$ and:

$$\Delta\left([i_1 \dots i_k]\right) = \sum_{a=0}^{k} [i_1 \dots i_a] \varphi_{i_{a+1}} \dots \varphi_{i_k} \otimes [i_{a+1} \dots i_k] \tag{4.21}$$

is both coassociative and gives rise to a bialgebra structure on $\mathcal{F}^{\text{ext}}$.

Remark 4.12. Our construction differs slightly from [15,38], where $\mathcal{F}$ itself is endowed with a bialgebra structure by modifying the product on $\mathcal{F} \otimes \mathcal{F}$ in the spirit of [30, p. 3]. However, the two approaches are easily seen to be equivalent.

4.13. It is straightforward to check that there is a unique algebra homomorphism:

$$U_q(\mathfrak{n}^+) \xrightarrow{\Phi} \mathcal{F} \tag{4.22}$$

sending e_i to $[i]$ (as one just needs to check that relations (4.1) hold in $\mathcal{F}$, due to Remark 4.4). Moreover, it is easy to prove by induction on $|\deg x|$ (using the bialgebra pairing properties (4.6)–(4.7)) that the map Φ is explicitly given by:

$$\Phi(x) = \sum_{i_1, \dots, i_k \in I}^{k \in \mathbb{N}} \left[\prod_{a=1}^{k} (q_{i_a}^{-1} - q_{i_a})\right] \left\langle x, f_{i_1} \dots f_{i_k} \right\rangle \cdot [i_1 \dots i_k] \tag{4.23}$$

Because the bialgebra pairing (4.5) is non-degenerate and $\langle x, y\varphi^- \rangle = \langle x, y \rangle$ for any $x \in U_q(\mathfrak{n}^+), y \in U_q(\mathfrak{n}^-)$ and φ^- a product of φ_i^-'s (which is a simple consequence of the bialgebra pairing properties (4.6)–(4.7)), (4.23) implies the injectivity of Φ. The image of the map Φ is described in [27, Theorem 5], which states that:

$$\operatorname{Im}\Phi = \left\{ \sum_{i_1,\dots,i_r \in I}^{r\in\mathbb{N}} \gamma(i_1 \dots i_r) \cdot [i_1 \dots i_r] \right\} \tag{4.24}$$

where the constants $\gamma(i_1 \dots i_r) \in \mathbb{Q}(q)$ vanish for all but finitely many values of r and satisfy the following property:

$$\sum_{k=0}^{1-a_{ij}} (-1)^k \binom{1-a_{ij}}{k}_i \gamma \left(w \quad \underbrace{i \dots i}_{k \text{ symbols}} \quad j \quad \underbrace{i \dots i}_{1-a_{ij}-k \text{ symbols}} \quad w' \right) = 0 \tag{4.25}$$

for any distinct $i, j \in I$ and any words w, w'.

Comparing (4.2) with (4.20), it is easy to see that the algebra homomorphism (4.22) extends to a bialgebra homomorphism:

$$U_q(\mathfrak{b}^+) \xrightarrow{\Phi} \mathcal{F}^{\text{ext}}$$

by sending $\varphi_i \mapsto \varphi_i$.

4.14. As in Subsection 2.3, we fix a total order on the set I, and consider the induced lexicographic order on the set of all words (2.5).

Definition 4.15. ([27]) A word w is called <u>good</u> if there exists an element:

$$w + \sum_{v<w} c_v \cdot v \tag{4.26}$$

in *Im* Φ, for certain constants $c_v \in \mathbb{Q}(q)$.

If a word is good, then so are all its prefixes and suffixes and hence all its subwords ([27, Lemma 13], see also Proposition 4.36 for a version of this statement in the loop case).

Proposition 4.16. *([27, Lemma 21]) A word is good if and only if it is standard.*

Above, we invoke the notion of standard words from Definition 2.12(a). Likewise, the standard Lyndon words from Definition 2.12(b) as well as the bijection (2.13) can also be characterized in terms of the map Φ, as follows.

Lemma 4.17. *([27, Corollary 27, Theorem 36]) For any $\alpha \in \Delta^+$, the leading word of $\Phi(e_{\ell(\alpha)})$ is $\ell(\alpha)$. Moreover, the word $\ell(\alpha)$ is the smallest good word of degree α.*

In the rest of this Section, we develop the loop version of the above results with the aim of proving Theorem 1.5. To this end, we construct a PBW basis of $U_q(L\mathfrak{n}^+)$ parametrized by standard loop words in Theorem 4.25, introduce the loop version $\mathcal{F}^L$ of the shuffle algebra $\mathcal{F}$ and relate it to $U_q(L\mathfrak{n}^+)$ in Subsections 4.27–4.32, establish a loop version of Proposition 4.16 in Proposition 4.41, and conjecture a loop version of Lemma 4.17 in Conjecture 4.44. Finally, with the aim of proving Theorem 1.7 in Section 5, we filter $U_q(L\mathfrak{n}^+)$ by the subspaces $U_q(L\mathfrak{n}^+)_{\leq w}$ of (4.67) for any loop word w, whose graded dimension (4.74) is expressed in terms of good words $\leq w$, and discuss their pairing with $U_q(L\mathfrak{n}^-)^{\leq w}$ of (4.66) in Proposition 4.39.

4.18. We will now develop a loop version of the above notions, with the goal of proving Theorem 1.5. In what follows, we will use the generating series:

$$e_i(z) = \sum_{k \in \mathbb{Z}} \frac{e_{i,k}}{z^k}, \qquad f_i(z) = \sum_{k \in \mathbb{Z}} \frac{f_{i,k}}{z^k}, \qquad \varphi_i^{\pm}(z) = \sum_{l=0}^{\infty} \frac{\varphi_{i,l}^{\pm}}{z^{\pm l}}$$

and consider the formal delta function $\delta(z) = \sum_{k \in \mathbb{Z}} z^k$. For any $i, j \in I$, set:

$$\zeta_{ij}\left(\frac{z}{w}\right) = \frac{z - wq^{-d_{ij}}}{z - w} \tag{4.27}$$

We now recall the definition of the quantum loop group (new Drinfeld realization).

Definition 4.19. The quantum loop group associated to $\mathfrak{g}$ is:

$$U_q(L\mathfrak{g}) = \mathbb{Q}(q)\Big\langle e_{i,k}, f_{i,k}, \varphi_{i,l}^{\pm}\Big\rangle_{i \in I, k \in \mathbb{Z}, l \in \mathbb{N}} \Big/ \text{relations (4.28)–(4.32)}$$

where we impose the following relations for all $i, j \in I$:

$$e_i(z)e_j(w)\zeta_{ji}\left(\frac{w}{z}\right) = e_j(w)e_i(z)\zeta_{ij}\left(\frac{z}{w}\right) \tag{4.28}$$

$$\sum_{\sigma \in S(1-a_{ij})} \sum_{k=0}^{1-a_{ij}} (-1)^k \binom{1-a_{ij}}{k}_i \cdot$$

$$e_i(z_{\sigma(1)}) \dots e_i(z_{\sigma(k)}) e_j(w) e_i(z_{\sigma(k+1)}) \dots e_i(z_{\sigma(1-a_{ij})}) = 0, \quad \text{if } i \neq j \tag{4.29}$$

$$\varphi_j^{\pm}(w)e_i(z)\zeta_{ij}\left(\frac{z}{w}\right) = e_i(z)\varphi_j^{\pm}(w)\zeta_{ji}\left(\frac{w}{z}\right) \tag{4.30}$$

$$\varphi_i^{\pm}(z)\varphi_j^{\pm'}(w) = \varphi_j^{\pm'}(w)\varphi_i^{\pm}(z), \qquad \varphi_{i,0}^{+}\varphi_{i,0}^{-} = 1 \tag{4.31}$$

as well as the opposite relations with e's replaced by f's, and finally the relation:

$$[e_i(z), f_j(w)] = \frac{\delta_i^j \delta\left(\frac{z}{w}\right)}{q_i - q_i^{-1}} \cdot \Big(\varphi_i^+(z) - \varphi_i^-(w)\Big) \tag{4.32}$$

Note that there is a unique algebra homomorphism:

$$U_q(\mathfrak{g}) \hookrightarrow U_q(L\mathfrak{g})$$

sending $e_i \mapsto e_{i,0}$, $f_i \mapsto f_{i,0}$, $\varphi_i^{\pm 1} \mapsto \varphi_{i,0}^{\pm}$.

4.20. Recall that $U_q(L\mathfrak{g})$ is a topological bialgebra with respect to the following coproduct ([8, formulas (5)–(7)]):

$$\Delta\left(\varphi_i^{\pm}(z)\right) = \varphi_i^{\pm}(z) \otimes \varphi_i^{\pm}(z) \tag{4.33}$$

$$\Delta\left(e_i(z)\right) = \varphi_i^{+}(z) \otimes e_i(z) + e_i(z) \otimes 1 \tag{4.34}$$

$$\Delta\left(f_i(z)\right) = 1 \otimes f_i(z) + f_i(z) \otimes \varphi_i^{-}(z) \tag{4.35}$$

This bialgebra structure preserves the $Q \times \mathbb{Z}$-grading induced by setting:

$$\deg e_{i,k} = (\alpha_i, k), \quad \deg \varphi_{i,l}^{\pm} = (0, \pm l), \quad \deg f_{i,k} = (-\alpha_i, k)$$

for all applicable indices. Recall the triangular decomposition ([18, §3.3]):

$$U_q(L\mathfrak{g}) = U_q(L\mathfrak{n}^+) \otimes U_q(L\mathfrak{h}) \otimes U_q(L\mathfrak{n}^-) \tag{4.36}$$

where $U_q(L\mathfrak{n}^+), U_q(L\mathfrak{h}), U_q(L\mathfrak{n}^-)$ are the subalgebras of $U_q(L\mathfrak{g})$ generated by the $e_{i,k}$'s, $\varphi_{i,l}^{\pm}$'s, $f_{i,k}$'s, respectively. We note that the following subalgebras of $U_q(L\mathfrak{g})$:

$$U_q(L\mathfrak{b}^+) = U_q(L\mathfrak{n}^+) \otimes \mathbb{Q}(q)\left[\varphi_{i,0}^{\pm}, \varphi_{i,1}^{+}, \varphi_{i,2}^{+}, \dots\right]_{i \in I}$$

$$U_q(L\mathfrak{b}^-) = \mathbb{Q}(q)\left[\varphi_{i,0}^{\mp}, \varphi_{i,1}^{-}, \varphi_{i,2}^{-}, \dots\right]_{i \in I} \otimes U_q(L\mathfrak{n}^-)$$

are preserved by the coproduct Δ, and hence are sub-bialgebras of $U_q(L\mathfrak{g})$.

4.21. It is well-known ([16, Lemma 9.1], see also [9, §4], [17, §1.3–1.4] for more details) that there exists a bialgebra pairing:

$$\langle \cdot, \cdot \rangle \colon\ U_q(L\mathfrak{b}^+) \otimes U_q(L\mathfrak{b}^-) \longrightarrow \mathbb{Q}(q) \tag{4.37}$$

that satisfies (4.6)–(4.7) and is determined by the properties:

$$\Big\langle e_i(z), f_j(w) \Big\rangle = \frac{\delta_i^j \delta\left(\frac{z}{w}\right)}{q_i^{-1} - q_i} \tag{4.38}$$

$$\Big\langle \varphi_i^{+}(z), \varphi_j^{-}(w) \Big\rangle = \frac{\zeta_{ij}\left(\frac{z}{w}\right)}{\zeta_{ji}\left(\frac{w}{z}\right)} \tag{4.39}$$

(the right-hand side of (4.39) is expanded in $|z| \gg |w|$) and the fact that:

$$\langle a, b\rangle = 0 \quad \text{unless} \quad \deg a + \deg b = (0,0) \in Q \times \mathbb{Z}$$

This pairing is known to be non-degenerate (cf. [16, Section 9.3], [17, Proposition 9], [10, Theorem 1.4]), although we will provide an alternative argument below.

Proposition 4.22. *The pairing $\langle\cdot,\cdot\rangle$ of (4.37) is non-degenerate in each argument.*

We will give a proof of this result in Subsection 5.16.

4.23. Let us now provide a loop version of the constructions of Subsection 4.6.

Definition 4.24. For any loop word w, define $e_w \in U_q(L\mathfrak{n}^+)$, $f_w \in U_q(L\mathfrak{n}^-)$ by:

$$e_{[i^{(d)}]} = e_{i,d} \quad \text{and} \quad f_{[i^{(d)}]} = f_{i,-d}$$

for all $i \in I$, $d \in \mathbb{Z}$, and then recursively by:

$$e_\ell = [e_{\ell_1}, e_{\ell_2}]_q = e_{\ell_1}e_{\ell_2} - q^{(\operatorname{hdeg}\ell_1, \operatorname{hdeg}\ell_2)} e_{\ell_2}e_{\ell_1} \tag{4.40}$$

$$f_\ell = [f_{\ell_1}, f_{\ell_2}]_q = f_{\ell_1}f_{\ell_2} - q^{(\operatorname{hdeg}\ell_1, \operatorname{hdeg}\ell_2)} f_{\ell_2}f_{\ell_1} \tag{4.41}$$

if ℓ is a Lyndon loop word with factorization (2.6), and:

$$e_w = e_{\ell_1}\dots e_{\ell_k} \quad \text{and} \quad f_w = f_{\ell_1}\dots f_{\ell_k} \tag{4.42}$$

if w is an arbitrary loop word with the canonical factorization $\ell_1 \dots \ell_k$, as in (2.7).

Note that $\deg e_w = -\deg f_w = \deg w$ for all loop words w. We have the following result, which is simultaneously an analogue of both (2.37)–(2.38) and Theorem 4.8.

Theorem 4.25. *We have:*

$$U_q(L\mathfrak{n}^+) = \bigoplus_{\ell_1 \geq \dots \geq \ell_k \text{ standard Lyndon loop words}}^{k\in\mathbb{N}} \mathbb{Q}(q)\cdot e_{\ell_1}\dots e_{\ell_k} = \bigoplus_{w \text{ standard loop words}} \mathbb{Q}(q)\cdot e_w \tag{4.43}$$

The analogous result also holds with $+ \leftrightarrow -$ and $e \leftrightarrow f$.

Remark 4.26. (a) Similar to Theorem 4.8 and Remark 4.9 in finite case, the above result is a consequence of the PBW theorem for $U_q(L\mathfrak{n}^\pm)$ established in [11, §3][6]:

[6] Alternatively, the interested reader may find a detailed proof of this result in Subsections 5.6–5.28 of the arχiv-version of the present paper.

$$U_q(L\mathfrak{n}^{\pm}) = \bigoplus_{r_1 \geq \dots \geq r_k \in \mathbb{Z}}^{k \in \mathbb{N}} \mathbb{Q}(q) \cdot E_{\pm\beta_{r_1}} \dots E_{\pm\beta_{r_k}} \tag{4.44}$$

where the set $\{\beta_r\}_{r \in \mathbb{Z}}$ coincides with $\Delta^+ \times \mathbb{Z}$ ordered via:

$$\beta_a < \beta_b \iff a > b.$$

This PBW result essentially follows from the Beck's PBW basis [2] of the Drinfeld-Jimbo affine quantum group $U_q(\widehat{\mathfrak{g}})$ through the "affine to loop" isomorphism:

$$U_q(L\mathfrak{g}) \xrightarrow{\sim} U_q(\widehat{\mathfrak{g}})/(C-1) \tag{4.45}$$

of [2,3,6]. Moreover, the root vectors $E_{\pm\beta_r}$ also satisfy the "convexity property":

$$E_{\pm\beta} E_{\pm\beta'} - q^{(\beta',\beta)} E_{\pm\beta'} E_{\pm\beta} \in \bigoplus_{\substack{\beta' < \gamma_1 \leq \dots \leq \gamma_k < \beta \\ \gamma_1 + \dots + \gamma_k = \beta' + \beta}}^{k \in \mathbb{N}} \mathbb{Q}(q) \cdot E_{\pm\gamma_1} \dots E_{\pm\gamma_k} \tag{4.46}$$

for any pair $\beta' < \beta$ of elements of $\Delta^+ \times \mathbb{Z}$. In particular, this implies that

$$[E_{\pm\beta}, E_{\pm\beta'}]_q := E_{\pm\beta} E_{\pm\beta'} - q^{(\beta,\beta')} E_{\pm\beta'} E_{\pm\beta} \in \mathbb{Q}(q)^* \cdot E_{\pm(\beta'+\beta)} \tag{4.47}$$

whenever $\beta' + \beta \in \Delta^+ \times \mathbb{Z}$ and β', β are minimal in the following sense:

$$\nexists\, \gamma', \gamma \in \Delta^+ \times \mathbb{Z} \quad \text{s.t.} \quad \beta' < \gamma' < \gamma < \beta \quad \text{and} \quad \beta' + \beta = \gamma' + \gamma \tag{4.48}$$

(b) The property (4.47) combined with Proposition 2.38 allow to prove that

$$e_{\ell(\alpha,d)} \in \mathbb{Q}(q)^* \cdot \varpi(E_{(-\alpha,d)})$$

(by induction on the height of $\alpha \in \Delta^+$), where ℓ is the bijection (2.35) and ϖ is the anti-isomorphism of $U_q(L\mathfrak{g})$, determined by $e_{i,k} \mapsto f_{i,k}, f_{i,k} \mapsto e_{i,k}, \varphi^{\pm}_{i,\ell} \mapsto \varphi^{\pm}_{i,\ell}$. Thus, (4.43) follows from (4.44).

4.27. We will now define a "loop" version of the shuffle algebra, which is to $U_q(L\mathfrak{g})$ as the shuffle algebra of Definition 4.11 is to $U_q(\mathfrak{g})$. The careful reader will observe a slight error in Definition 4.28 as the right-hand side in the shuffle product (4.50) contains infinitely many summands. This will be remedied in Subsection 4.32 by introducing an appropriate completion, but we prefer this slightly imprecise approach in order to keep the exposition clear.

Definition 4.28. Take the $\mathbb{Q}(q)$-vector space $\mathcal{F}^L$ with a basis given by loop words:

$$\left[i_1^{(d_1)} \dots i_k^{(d_k)}\right] \tag{4.49}$$

for arbitrary $k \in \mathbb{N}$, $i_1, \dots, i_k \in I$, $d_1, \dots, d_k \in \mathbb{Z}$, and endow it with the following shuffle product:

$$\left[i_1^{(d_1)} \dots i_k^{(d_k)}\right] * \left[j_1^{(e_1)} \dots j_l^{(e_l)}\right] = \sum_{\substack{\{1,\dots,k+l\}=A\sqcup B \\ |A|=k,|B|=l}} \left(\sum_{\substack{\pi_1+\dots+\pi_{k+l}=0 \\ \pi_1,\dots,\pi_{k+l}\in\mathbb{Z}}} \gamma_{A,B,\pi_1,\dots,\pi_{k+l}} \cdot \left[s_1^{(t_1+\pi_1)} \dots s_{k+l}^{(t_{k+l}+\pi_{k+l})}\right] \right) \tag{4.50}$$

where in the right-hand side, if $A = \{a_1 < \dots < a_k\}$ and $B = \{b_1 < \dots < b_l\}$, we write:

$$s_c = \begin{cases} i_\bullet & \text{if } c = a_\bullet \\ j_\bullet & \text{if } c = b_\bullet \end{cases}, \qquad t_c = \begin{cases} d_\bullet & \text{if } c = a_\bullet \\ e_\bullet & \text{if } c = b_\bullet \end{cases} \tag{4.51}$$

and $\gamma_{A,B,\pi_1,\dots,\pi_{k+l}}$ are defined as the coefficients of the Taylor expansion:

$$\prod_{A\ni a>b\in B} \frac{\zeta_{s_a s_b}\left(\frac{z_a}{z_b}\right)}{\zeta_{s_b s_a}\left(\frac{z_b}{z_a}\right)} = \sum_{\substack{\pi_1+\dots+\pi_{k+l}=0 \\ \pi_1,\dots,\pi_{k+l}\in\mathbb{Z}}} \gamma_{A,B,\pi_1,\dots,\pi_{k+l}} \cdot z_1^{\pi_1} \dots z_{k+l}^{\pi_{k+l}} \tag{4.52}$$

in the limit when $|z_a| \gg |z_b|$ for all $a \in A,\ b \in B$.

Remark 4.29. (a) We note that in the inner sum of (4.50) the only terms which appear with non-zero coefficient are those with $\pi_c \leq 0$ if $c \in A$ and $\pi_c \geq 0$ if $c \in B$.

(b) We also have $\gamma_{A,B,0,\dots,0} = q^{\lambda_{A,B}}$ with $\lambda_{A,B}$ defined in (4.19).

It is straightforward to see that $(\mathcal{F}^L, *)$ is an associative algebra, $Q^+ \times \mathbb{Z}$-graded by (2.19), and we leave this check as an exercise to the interested reader.

Proposition 4.30. *There is a unique algebra homomorphism:*

$$U_q(L\mathfrak{n}^+) \xrightarrow{\Phi^L} \mathcal{F}^L \tag{4.53}$$

sending $e_{i,d} \mapsto \left[i^{(d)}\right]$. *The homomorphism* Φ^L *is injective and is explicitly given by*

$$\Phi^L(x) = \sum_{\substack{k\in\mathbb{N} \\ i_1,\dots,i_k\in I \\ d_1,\dots,d_k\in\mathbb{Z}}} \left[\prod_{a=1}^{k} (q_{i_a}^{-1} - q_{i_a})\right] \left\langle x, f_{i_1,-d_1} \dots f_{i_k,-d_k} \right\rangle \cdot \left[i_1^{(d_1)} \dots i_k^{(d_k)}\right] \tag{4.54}$$

for all $x \in U_q(L\mathfrak{n}^+)$, *where the pairing is that of* (4.37).

The Proposition above is straightforward, so we leave it as an exercise to the interested reader (alternatively, it follows from Proposition 5.21 below). The injectivity follows immediately from the non-degeneracy of (4.37), due to Proposition 4.22.

Remark 4.31. We note that our definition of $\mathcal{F}^L$ is actually equivalent to the main construction of [17, §2] (in fact our presentation is to [17, §2] as Green's presentation [15] is to Rosso's presentation [38] of shuffle algebras in the finite type case). Moreover, a version of the above construction of $\mathcal{F}^L$ and the homomorphism (4.53) (which correspond in our notation to $|I| = 1$, but a more complicated ζ-factor) featured in [41, §1.9].

4.32. We note a certain imprecision in Definition 4.28, which we will remedy now: the right-hand side of (4.50) is an infinite sum. However, because of the power series nature of this infinite sum, the imprecision can be easily fixed as follows. Amend Definition 4.28 by considering instead:

$$\mathcal{F}^L = \bigoplus_{\mathbf{k}\in Q^+, d\in\mathbb{Z}} \mathcal{F}^L_{\mathbf{k},d} \tag{4.55}$$

where we consider the following completions:

$$\mathcal{F}^L_{\mathbf{k},d} = \left\{ \sum_{\substack{d_1+\dots+d_a \text{ bounded from} \\ \text{below, for all } a\in\{1,\dots,k\}}} c_{i_1,\dots,i_k;d_1,\dots,d_k} \cdot \underbrace{\left[i_1^{(d_1)} \dots i_k^{(d_k)} \right]}_{\text{has degree } (\mathbf{k},d)} \right\} \tag{4.56}$$

with arbitrary coefficients $c_{i_1,\dots,i_k;d_1,\dots,d_k} \in \mathbb{Q}(q)$.

Proposition 4.33. *The shuffle product* (4.50) *is well-defined on $\mathcal{F}^L$ of (4.55)–(4.56).*

Proof. We begin by showing that the operation $w * w'$ of (4.50) extends to a well-defined operation on infinite linear combinations of the form:

$$\left(\sum_{\deg w = (\mathbf{k},d)} c_w \cdot w \right) * \left(\sum_{\deg w' = (\mathbf{k}',d')} c'_{w'} \cdot w' \right) \tag{4.57}$$

where we have $c_w \neq 0$ (resp. $c'_{w'} \neq 0$) only if every prefix of w (resp. w') has vertical degree bounded from below by some fixed $m \in \mathbb{Z}$. Take an arbitrary word v and consider the set:

$$S = \Big\{ (w, w') \text{ such that } c_w \neq 0, c'_{w'} \neq 0 \text{ and } v \text{ appears as a summand in } w * w' \Big\}$$

We need to show that S is finite, which would imply that the coefficient of v in the shuffle product (4.57) is well-defined. Let us assume for the purpose of contradiction that S is infinite. Since the vertical degrees of arbitrary prefixes of w and w' are bounded from below, this implies that one of these prefixes has arbitrarily large vertical degree. Without loss of generality, let us assume that we are talking about the length a prefix of w. Thus, for any $N \in \mathbb{N}$, there exists $(w, w') \in S$ such that the vertical degree of $w_{a|}$ is at least N. However, since all the prefixes of w' have vertical degree at least equal to the fixed constant m, then all terms in the shuffle product $w * w'$ will have some prefix with vertical degree at least $N + m$. If N is large enough, this contradicts the fact that v appears as a summand in $w * w'$.

We now need to prove that the expression (4.57) is of the form (4.55)–(4.56). The loop words v that appear in the expression (4.57) also do appear in the shuffle products $w * w'$, where w and w' are loop words of fixed degrees, such that every prefix of w and w' has vertical degree bounded from below by some fixed $m \in \mathbb{Z}$. Thus, any loop word appearing in the shuffle product $w * w'$ has degree $\deg w + \deg w'$, while any of its prefixes has vertical degree bounded from below by $2m$ (an immediate consequence of (4.50) and (4.52)), which is precisely what we needed to prove. $\square$

4.34. Just like in Subsection 4.10, there is no bialgebra structure on $\mathcal{F}^L$. However, there is a bialgebra structure on the extended shuffle algebra:

$$\mathcal{F}^{L,\text{ext}} = \mathcal{F}^L \otimes \mathbb{Q}(q) \left[(\varphi^+_{i,0})^{\pm 1}, \varphi^+_{i,1}, \varphi^+_{i,2}, \dots \right]_{i \in I}$$

with pairwise commuting φ's, where the multiplication is governed by the rule:

$$\varphi^+_{j,e} * \left[i_1^{(d_1)} \dots i_k^{(d_k)} \right] = \sum_{\pi_1, \dots, \pi_k \geq 0} \mu_{\pi_1, \dots, \pi_k} \cdot \left[i_1^{(d_1 + \pi_1)} \dots i_k^{(d_k + \pi_k)} \right] * \varphi^+_{j, e - \pi_1 - \dots - \pi_k} \tag{4.58}$$

where $\varphi^+_{j,<0} = 0$ and $\mu_{\pi_1, \dots, \pi_k}$ are defined as the coefficients of the Taylor expansion:

$$\prod_{r=1}^{k} \frac{\zeta_{j i_r}(w/z_i)}{\zeta_{i_r j}(z_i/w)} = \sum_{\pi_1, \dots, \pi_k \geq 0} \mu_{\pi_1, \dots, \pi_k} \cdot \frac{z_1^{\pi_1} \dots z_k^{\pi_k}}{w^{\pi_1 + \dots + \pi_k}}$$

It is straightforward to check that the right-hand side of (4.58) indeed lies in $\mathcal{F}^L$ of (4.55)–(4.56) tensored with $\mathbb{Q}(q) \left[(\varphi^+_{i,0})^{\pm 1}, \varphi^+_{i,1}, \varphi^+_{i,2}, \dots \right]_{i \in I}$, and that (4.58) extends to the entire $\mathcal{F}^L$. It is also easy to check that the assignment

$$\Delta(\varphi^+_i(z)) = \varphi^+_i(z) \otimes \varphi^+_i(z)$$

and

$$\Delta\left(\left[i_1^{(d_1)} \dots i_k^{(d_k)} \right] \right) = \tag{4.59}$$

$$\sum_{a=0}^{k} \sum_{\pi_{a+1}, \dots, \pi_k \geq 0} \left[i_1^{(d_1)} \dots i_a^{(d_a)} \right] \varphi^+_{i_{a+1}, \pi_{a+1}} \dots \varphi^+_{i_k, \pi_k} \otimes \left[i_{a+1}^{(d_{a+1} - \pi_{a+1})} \dots i_k^{(d_k - \pi_k)} \right]$$

is both coassociative and gives rise to a bialgebra structure on $\mathcal{F}^{L,\mathrm{ext}}$. We note that the coproduct (4.59) is topological, in the same sense as the coproduct (4.34).

Finally, comparing (4.30) with (4.58) as well as (4.34) with (4.59), we see that the algebra homomorphism (4.53) extends to a bialgebra homomorphism:

$$U_q(L\mathfrak{b}^+) \xrightarrow{\Phi^L} \mathcal{F}^{L,\mathrm{ext}}$$

by sending $\varphi^+_{i,r} \mapsto \varphi^+_{i,r}$.

4.35. Define good loop words just like in Definition 4.15 (by replacing Φ with Φ^L).

Proposition 4.36. *Any subword of a good loop word is good.*

Proof. It is enough to prove that any prefix and suffix of a good loop word is good. To this end, assume that w is a good loop word of length k, which implies that there exists $x \in U_q(L\mathfrak{n}^+)$ such that:

$$\Phi^L(x) = w + \sum_{v<w} c_v \cdot v$$

for various $c_v \in \mathbb{Q}(q)$. We may assume that x is homogeneous of degree $\deg w = (\mathbf{k}, d)$, which implies that $c_v \neq 0$ only if $\deg v = (\mathbf{k}, d)$. Formula (4.59) implies:

$$\Delta(\Phi^L(x)) = \sum_{b=0}^{k} w_{b|} \cdot \varphi \otimes w_{|k-b} + \dots \tag{4.60}$$

where the ellipsis denotes tensors $\alpha\varphi' \otimes \beta$ with φ' being products of $\varphi^+_{i,r}$'s and α, β being loop words, such that if the loop word α has length b, then either ($\alpha < w_{b|}$) or ($\alpha = w_{b|}$ and $\beta < w_{|k-b}$) or ($\alpha = w_{b|}$ and $\mathrm{vdeg}\ \beta < \mathrm{vdeg}\ w_{|k-b}$) [7]; the latter option accounts for the situation when φ' is a product of Cartan elements $\varphi^+_{i,r}$ with at least one such element having $r > 0$. Fix $a \in \{0, \dots, k\}$. We will write:

$$\Delta(x) = \sum_{c} y_c \cdot \varphi \otimes z_c + \underline{\hspace{2em}}$$

for some $y_c, z_c \in U_q(L\mathfrak{n}^+)$ of degrees $(\mathbf{k}_a, d_a)$, $(\mathbf{k} - \mathbf{k}_a, d - d_a)$, respectively, where (above and henceforth) $(\mathbf{k}_a, d_a) = \deg w_{a|}$, φ is a product of $\varphi^+_{i,0}$'s and their inverses that depends only on $(\mathbf{k} - \mathbf{k}_a, d - d_a)$, and the blank denotes tensors of degrees other than $(\mathbf{k}_a, d_a) \otimes (\mathbf{k} - \mathbf{k}_a, d - d_a)$. Therefore, we have:

$$\left(\Phi^L \otimes \Phi^L\right)(\Delta(x)) = \sum_{c} \Phi^L(y_c) \cdot \varphi \otimes \Phi^L(z_c) + \underline{\hspace{2em}} \tag{4.61}$$

[7] Here the vertical degree vdeg of a word (4.49) is naturally defined to be $d_1 + \dots + d_k$, cf. (2.21).

Using the fact that Φ^L intertwines the coproducts, we conclude that the left-hand sides of (4.60) and (4.61) are equal, hence so are their right-hand sides. If we just look at the tensors of degrees $(\mathbf{k}_a, d_a) \otimes (\mathbf{k} - \mathbf{k}_a, d - d_a)$, then we obtain the following identity:

$$\sum_c \Phi^L(y_c) \otimes \Phi^L(z_c) = w_{a|} \otimes w_{|k-a} + \dots \tag{4.62}$$

where the ellipsis denotes tensors $\alpha\varphi' \otimes \beta$ with φ' being products of $\varphi^+_{i,r}$'s and α, β being loop words, such that if the loop word α has length a, then either $(\alpha < w_{a|})$ or $(\alpha = w_{a|}$ and $\beta < w_{|k-a})$. Among all the tensors $y_c \otimes z_c$ that appear in (4.62), let us consider the one for which:

$$\Phi^L(y_c)$$

has the maximal leading order term. If there are several such tensors with the same maximal leading order term, then by taking appropriate linear combinations, we can ensure that there is a single one. Formula (4.62) then requires:

$$\Phi^L(y_c) = s \cdot w_{a|} + \sum_{v < w_{a|}} r_{v,a} \cdot v \tag{4.63}$$

for $s \in \mathbb{Q}(q)^*$ and various $r_{v,a} \in \mathbb{Q}(q)$. Since only the tensor $y_c \otimes z_c$ can produce terms of the form $w_{a|} \otimes$ ____ in (4.62), then:

$$\Phi^L(z_c) = t \cdot w_{|k-a} + \sum_{v < w_{|k-a}} r'_{v,a} \cdot v \tag{4.64}$$

for $t \in \mathbb{Q}(q)^*$ and various $r'_{v,a} \in \mathbb{Q}(q)$. Formulas (4.63)–(4.64) imply that both $w_{a|}$ and $w_{|k-a}$ are good loop words, as we needed to show. □

Proposition 4.37. *A loop word is good if and only if it can be written as:*

$$\ell_1 \dots \ell_k$$

where $\ell_1 \geq \dots \geq \ell_k$ are good Lyndon loop words.

Proof. The "only if" statement is an immediate consequence of Proposition 2.7 and Proposition 4.36. As for the "if" statement, suppose that we have good Lyndon loop words $\ell_1 \geq \dots \geq \ell_k$. By definition, there exist elements:

$$\Phi^L(x_r) = \ell_r + \sum_{v < \ell_r} \text{coefficient} \cdot v \tag{4.65}$$

for various $x_r \in U_q(L\mathfrak{n}^+)$. We may assume that each x_r is homogeneous, and that so are the v's in (4.65), hence all of them have the same number of letters as ℓ_r. But then the leading order term of $\Phi^L(x_1 \dots x_k)$ is the leading word in the shuffle product $\ell_1 * \dots * \ell_k$. By the obvious analogue of [27, Lemma 15], this shuffle product has the leading order term equal to the concatenation $\ell_1 \dots \ell_k$. This exactly means that the latter concatenation is a good loop word, as we needed to show. □

4.38. Invoking Definition 4.24, for any loop word w consider:

$$U_q(L\mathfrak{n}^-)^{\leq w} = \bigoplus_{v \leq w \text{ standard loop word}} \mathbb{Q}(q) \cdot f_v \tag{4.66}$$

which is finite-dimensional in any degree $\in Q^- \times \mathbb{Z}$ according to Corollary 2.32. For any loop word w, we also define:

$$U_q(L\mathfrak{n}^+)_{\leq w} \subset U_q(L\mathfrak{n}^+) \tag{4.67}$$

to consist of those elements x such that the leading order term of $\Phi^L(x)$ is $\leq w$. Invoking (4.54), we note that $U_q(L\mathfrak{n}^+)_{\leq w}$ consists of those $x \in U_q(L\mathfrak{n}^+)$ such that:

$$\langle x, {}_u f \rangle = 0, \quad \forall\, u > w \tag{4.68}$$

where for any loop word $u = \left[i_1^{(d_1)} \dots i_k^{(d_k)} \right]$ we set:

$${}_u f := f_{i_1,-d_1} \dots f_{i_k,-d_k} \tag{4.69}$$

Proposition 4.39. *The restriction of the pairing (4.37) to the subspaces:*

$$U_q(L\mathfrak{n}^+)_{\leq w} \otimes U_q(L\mathfrak{n}^-)^{\leq w} \longrightarrow \mathbb{Q}(q)$$

is still non-degenerate in the first factor, i.e. $\langle x, - \rangle = 0$ *implies* $x = 0$.

Proof. Assume $x \in U_q(L\mathfrak{n}^+)_{\leq w}$ has the property that:

$$\langle x, f_v \rangle = 0 \tag{4.70}$$

for any standard loop word $v \leq w$, and our goal is to show that $x = 0$. To this end, note that for any loop word v we have (by analogy with [27, Proposition 20]):

$$f_v \in \sum_{u \geq v} \mathbb{Q}(q) \cdot {}_u f \tag{4.71}$$

Since $\langle x, {}_u f \rangle = 0$ for all $u > w$ by (4.68), we conclude:

$$\langle x, f_v \rangle = 0 \tag{4.72}$$

for any loop word $v > w$. By Theorem 4.25, the set $\{f_v | v \text{ standard loop word}\}$ is a basis of $U_q(L\mathfrak{n}^-)$, so relations (4.70) and (4.72) imply that:

$$\left\langle x, U_q(L\mathfrak{n}^-)\right\rangle = 0$$

Thus $x = 0$ due to the non-degeneracy statement of Proposition 4.22. $\square$

4.40. As a consequence of Proposition 4.39, we conclude that:

$$\dim U_q(L\mathfrak{n}^+)_{\leq w} \leq \#\Big\{\text{standard loop words } \leq w\Big\} \tag{4.73}$$

Note a slight imprecision in the inequality above: what we actually mean is that the dimension of the left-hand side in any fixed degree $(\alpha, d) \in Q^+ \times \mathbb{Z}$ is less than or equal to the number of standard loop words $\leq w$ of degree (α, d) (the latter number is finite by Corollary 2.32). On the other hand, by the very definition of a good loop word, we have:

$$\dim U_q(L\mathfrak{n}^+)_{\leq w} = \#\Big\{\text{good loop words } \leq w\Big\} \tag{4.74}$$

The following Proposition establishes the fact that we have equality in (4.73).

Proposition 4.41. *A loop word is standard if and only if it is good.*

Proof. Assume for the purpose of contradiction that there exists a good loop word w which is not standard, and choose it such that its degree $(\alpha, d) \in Q^+ \times \mathbb{Z}$ has minimal $|\alpha|$. This minimality, combined with Propositions 2.16 (see Remark 2.17) and 4.37, implies that w must be Lyndon. Therefore, we may write it as (2.6):

$$w = \ell_1 \ell_2$$

where $\ell_1 < w < \ell_2$ are Lyndon loop words. By Proposition 4.36, ℓ_1 and ℓ_2 are good Lyndon loop words, hence by the minimality of $|\alpha|$, standard Lyndon loop words. However, because of (4.73) and (4.74), there must exist a standard loop word $v < w$ with $\deg v = \deg w$. Then let us consider the canonical factorization (2.7) $v = \ell'_1 \dots \ell'_k$ where $\ell'_1 \geq \dots \geq \ell'_k$ are standard Lyndon loop words. Because:

$$\deg \ell_1 + \deg \ell_2 = \deg w = \deg v = \deg \ell'_1 + \dots + \deg \ell'_k$$

Corollary 2.37 implies that $\ell'_1 \geq \ell_1$. However, the only way this is compatible with:

$$\ell_1 \ell_2 = w > v = \ell'_1 \dots \ell'_k$$

is if $\ell'_1 = \ell_1 u$ for some loop word u that satisfies:

$$\ell_2 > u\ell_2' \dots \ell_k' \qquad \text{and} \qquad \deg \ell_2 = \deg u + \deg \ell_2' + \dots + \deg \ell_k' \tag{4.75}$$

Because ℓ_1' is standard, Proposition 2.15 (see Remark 2.17) implies that so is u. Therefore we may write $u = \ell_1'' \dots \ell_m''$ for various standard Lyndon loop words $\ell_1'' \geq \dots \geq \ell_m''$. Formula (4.75) implies that $\ell_2 > u$, so $\ell_2 > \ell_1'' \geq \dots \geq \ell_m''$. However, we also have $\ell_2 > w > v > \ell_2' \geq \dots \geq \ell_k'$, and so (4.75) contradicts Corollary 2.37. Thus, any good loop word is standard.

For the converse, let us prove by induction on $|\alpha|$ that for any standard loop word w of degree (α, d), there exists a linear combination:

$$\sum_{v \geq w} \text{coefficient} \cdot \Phi^L(e_v) \in \mathbb{Q}(q)^* \cdot w + \text{smaller words} \tag{4.76}$$

for various coefficients in $\mathbb{Q}(q)$ with v being standard loop words, where we may further assume that all summands have the same $Q^+ \times \mathbb{Z}$-degree (α, d).

Claim 4.42. *If (4.76) holds for two loop words $w = \ell_1$ and $w' = \ell_2 \dots \ell_k$, where $\ell_1 \geq \ell_2 \geq \dots \geq \ell_k$ are all standard Lyndon loop words, then (4.76) also holds for the concatenation ww'.*

Let us first show how the Claim allows us to complete the proof of the Proposition. Since any standard loop word can be written as $w = \ell_1 \dots \ell_k$ where $\ell_1 \geq \dots \geq \ell_k$ are standard Lyndon loop words, then the Claim says that it suffices to prove (4.76) when $w = \ell$ is a standard Lyndon loop word. To this end, let us write:

$$\Phi^L(e_\ell) = c \cdot u + \sum_{v < u} \text{coefficient} \cdot v$$

for some $c \in \mathbb{Q}(q)^*$ and a loop word u. Since u is the leading word, it must be good, hence standard. Corollary 2.37 implies that $u \geq \ell$. If $u = \ell$, then we have proved (4.76). If $u > \ell$, then u is a concatenation of standard Lyndon loop words of length less than that of ℓ, to which we may apply the induction hypothesis. According to the Claim, we may thus use (4.76) for u to write:

$$\Phi^L(e_\ell) - \text{coefficient} \cdot \Phi^L(e_u) = \sum_{v < u} \text{coefficient} \cdot v$$

By repeating this argument (finitely many times, due to Corollary 2.32) we either establish (4.76) for $w = \ell$ as wanted, or arrive at the following equality:

$$\Phi^L(e_\ell) - \sum_{v > \ell} \text{coefficient} \cdot \Phi^L(e_v) = \sum_{v < \ell} \text{coefficient} \cdot v \tag{4.77}$$

Since Φ^L is injective and $\{e_v | v \text{ standard loop word}\}$ is a basis of $U_q(L\mathfrak{n}^+)$ due to Theorem 4.25, the left-hand side of (4.77) is non-zero, hence so is the right-hand side. This implies that there are good, hence standard, loop words of degree $\deg \ell$ which are $< \ell$. The latter contradicts Corollary 2.37, and so (4.77) is impossible.

Claim 4.42 follows immediately from the two facts below (assume $w, w', \ell_1, \dots, \ell_k$ are as in the statement of the Claim):

(1) the largest word which appears in the shuffle product $w * w'$ is ww'
(2) $e_v e_{v'}$ is a linear combination of e_t's with $t \geq ww'$, for all $v \geq w$ and $v' \geq w'$ satisfying $\deg v = \deg w$ and $\deg v' = \deg w'$

The first fact is proved as in [27, Lemma 15] (cf. our proof of Proposition 4.37). To prove the second fact, note (using the convexity property (4.46) and the identification of $e_{\ell(\alpha,d)}$ with scalar multiples of $\varpi(E_{-(\alpha,d)})$ from Remark 4.26) that for all standard Lyndon loop words $\ell < \ell'$, we can write:

$$e_\ell e_{\ell'} = \text{a linear combination of } e_{\ell'\ell} \text{ and various } e_{m''_1 \dots m''_{t''}} \tag{4.78}$$

with $\ell' > m''_1 \geq \dots \geq m''_{t''} > \ell$ standard Lyndon loop words. Consider the canonical factorizations (2.7):

$$v = m_1 \dots m_t \quad \text{and} \quad v' = m'_1 \dots m'_{t'}$$

where $m_1 \geq \dots \geq m_t$ and $m'_1 \geq \dots \geq m'_{t'}$ are standard Lyndon loop words. It is elementary to prove that $v \geq w$, $\deg v = \deg w$, and w being Lyndon imply that either $m_1 > w$, or that $v = w$. In the former case ($m_1 > w$), (4.78) implies that:

$$e_v e_{v'} = e_{m_1} \dots e_{m_t} e_{m'_1} \dots e_{m'_{t'}} = \text{a linear combination of } e_t\text{'s}$$

for standard t with the canonical factorization $m''_1 \dots m''_{t''}$ satisfying $m''_1 \geq m_1 > w$. A result of Melançon ([31]), which states that two words with the canonical factorization (2.7) are in the relative order $>$ if the largest Lyndon words in their canonical factorizations are in the relative order $>$, implies that $t > ww'$, as we needed to show. In the latter case ($v = w = \ell_1$), we have two more possible situations:

- if $\ell_1 \geq m'_1$, then $e_v e_{v'} = e_{vv'}$ and we are done since $vv' \geq ww'$ (as $v \geq w, v' \geq w'$ and the loop words v, w are of the same length)
- if $m'_i > \ell_1 \geq m'_{i+1}$ for some $i \in \{1, \dots, t'\}$ (where $\ell_1 \geq m'_{t'+1}$ is vacuous), then (4.78) implies that:

$$e_v e_{v'} = e_{\ell_1} e_{m'_1} \dots e_{m'_{t'}} = \text{a linear combination of } e_t\text{'s}$$

where $t = m''_1 \dots m''_{i''} m'_{i+1} \dots m'_{t'}$ satisfies $m''_1 \geq \dots \geq m''_{i''} \geq m'_{i+1} \geq \dots \geq m'_{t'}$ and $m''_1 > \ell_1$. Thus, the aforementioned result of Melançon implies that $t > ww'$. $\square$

4.43. The results of the present Section amount to the proof of Theorem 1.5.

Proof of Theorem 1.5. The statement about the homomorphism Φ^L is proved in Subsection 4.27. The classification of standard Lyndon loop words is accomplished in (2.35). The construction of the root vectors (1.14) is done in Definition 4.24. Finally, the PBW statement (1.15) is precisely the subject of Theorem 4.25. $\square$

Computer experiments (in all types, but for a particular order of the simple roots) suggest that the generalization of Lemma 4.17 to the loop case holds.

Conjecture 4.44. *For any $(\alpha, d) \in \Delta^+ \times \mathbb{Z}$, the leading word of $\Phi^L(e_{\ell(\alpha,d)})$ is $\ell(\alpha, d)$. Moreover, the word $\ell(\alpha, d)$ is the smallest good loop word of degree (α, d).*

5. Shuffle algebras of Feigin-Odesskii and Enriquez

In the present Section, we will connect the loop shuffle algebra $\mathcal{F}^L$ with the trigonometric degeneration of the Feigin-Odesskii shuffle algebra associated with $\mathfrak{g}$, with the goal of establishing Theorem 1.7.

5.1. We now recall the trigonometric degeneration ([9]) of the Feigin-Odesskii shuffle algebra ([13]) of type $\mathfrak{g}$. Consider the vector space of color-symmetric rational functions:

$$\mathcal{V} = \bigoplus_{\mathbf{k}=\sum_{i \in I} k_i \alpha_i \in Q^+} \mathbb{Q}(q)(\dots, z_{i1}, \dots, z_{ik_i}, \dots)^{\text{Sym}}_{i \in I} \tag{5.1}$$

The index $i \in I$ will be called the <u>color</u> of the variables $z_{i1}, \dots, z_{ik_i}$. The term <u>color-symmetric</u> (as well as the superscript "Sym" in the formula above) refers to rational functions which are symmetric in the variables of each color separately. We make the vector space $\mathcal{V}$ into a $\mathbb{Q}(q)$-algebra via the following <u>shuffle product</u>:

$$F(\dots, z_{i1}, \dots, z_{ik_i}, \dots) * G(\dots, z_{i1}, \dots, z_{il_i}, \dots) = \frac{1}{\mathbf{k}! \cdot \mathbf{l}!} \cdot \tag{5.2}$$

$$\text{Sym}\left[F(\dots, z_{i1}, \dots, z_{ik_i}, \dots) G(\dots, z_{i,k_i+1}, \dots, z_{i,k_i+l_i}, \dots) \prod_{i,j \in I} \prod_{a \leq k_i, b > k_j} \zeta_{ij}\left(\frac{z_{ia}}{z_{jb}}\right)\right]$$

In (5.2), Sym denotes symmetrization with respect to the:

$$(\mathbf{k} + \mathbf{l})! := \prod_{i \in I} (k_i + l_i)! \tag{5.3}$$

permutations that permute the variables $z_{i1}, \dots, z_{i,k_i+l_i}$ for each i independently.

Definition 5.2. ([9], inspired by [13]) The positive shuffle algebra $\mathcal{A}^+$ is the subspace of $\mathcal{V}$ consisting of rational functions of the form:

$$R(\dots, z_{i1}, \dots, z_{ik_i}, \dots) = \frac{r(\dots, z_{i1}, \dots, z_{ik_i}, \dots)}{\prod_{\{i \neq i'\} \subset I}^{\text{unordered}} \prod_{1 \leq a \leq k_i}^{1 \leq a' \leq k_{i'}} (z_{ia} - z_{i'a'})} \tag{5.4}$$

where r is a symmetric Laurent polynomial that satisfies the wheel conditions:

$$r(\dots, z_{ia}, \dots)\Big|_{(z_{i1}, z_{i2}, z_{i3}, \dots, z_{i,1-a_{ij}}) \mapsto (w, wq_i^2, wq_i^4, \dots, wq_i^{-2a_{ij}}),\ z_{j1} \mapsto wq_i^{-a_{ij}}} = 0 \tag{5.5}$$

for any distinct $i, j \in I$.

Remark 5.3. Because of (5.5), any r as in (5.4) is actually divisible by:

$$\prod_{\{i \neq i'\} \subset I : a_{ii'} = 0}^{\text{unordered}} \prod_{1 \leq b \leq k_i}^{1 \leq b' \leq k_{i'}} (z_{ib} - z_{i'b'})$$

Therefore, rational functions R satisfying (5.4), (5.5) can only have simple poles on the diagonals $z_{ib} = z_{i'b'}$ with adjacent $i, i' \in I$, that is, such that $a_{ii'} < 0$.

The following is elementary, and we leave it to the interested reader.

Proposition 5.4. *$\mathcal{A}^+$ is closed under the product (5.2), and is thus an algebra.*

5.5. The algebra $\mathcal{A}^+$ is graded by $\mathbf{k} = \sum_{i \in I} k_i \alpha_i \in Q^+$ that encodes the number of variables of each color, and by the total homogeneous degree $d \in \mathbb{Z}$. We write:

$$\deg R = (\mathbf{k}, d)$$

and say that $\mathcal{A}^+$ is $Q^+ \times \mathbb{Z}$-graded. We will denote the graded pieces by:

$$\mathcal{A}^+ = \bigoplus_{\mathbf{k} \in Q^+} \mathcal{A}_{\mathbf{k}} \qquad \text{and} \qquad \mathcal{A}_{\mathbf{k}} = \bigoplus_{d \in \mathbb{Z}} \mathcal{A}_{\mathbf{k},d}$$

We define the negative shuffle algebra as $\mathcal{A}^- = (\mathcal{A}^+)^{\text{op}}$. It is graded by $Q^- \times \mathbb{Z}$, where a rational function in $\mathbf{k}$ variables of homogeneous degree d is assigned degree $(-\mathbf{k}, d)$, when viewed as an element of $\mathcal{A}^-$. We will denote the graded pieces by:

$$\mathcal{A}^- = \bigoplus_{-\mathbf{k} \in Q^-} \mathcal{A}_{-\mathbf{k}} \quad \text{and} \quad \mathcal{A}_{-\mathbf{k}} = \bigoplus_{d \in \mathbb{Z}} \mathcal{A}_{-\mathbf{k},d}$$

Proposition 5.6. *([9]) There exist unique algebra homomorphisms:*

$$U_q(L\mathfrak{n}^+) \xrightarrow{\Upsilon} \mathcal{A}^+ \quad \textit{and} \quad U_q(L\mathfrak{n}^-) \xrightarrow{\Upsilon} \mathcal{A}^- \tag{5.6}$$

determined by $\Upsilon(e_{i,d}) = z_{i1}^d \in \mathcal{A}_{\alpha_i,d}$ *and* $\Upsilon(f_{i,d}) = z_{i1}^d \in \mathcal{A}_{-\alpha_i,d}$*, respectively.*

Proposition 5.7. *The maps* Υ *of* (5.6) *are injective.*

Proof. We will prove the required statement for $U_q(L\mathfrak{n}^+)$, as taking the opposite of both algebras yields the statement for $U_q(L\mathfrak{n}^-)$. Let us consider the ring $\mathbb{A} = \mathbb{Q}[[\hbar]]$, its fraction field $\mathbb{F} = \mathbb{Q}((\hbar))$, and define:

$$U_{\mathbb{A}}(L\mathfrak{n}^+) \quad \text{and} \quad U_{\mathbb{F}}(L\mathfrak{n}^+)$$

by replacing $\mathbb{Q}(q)$ in Definition 4.19 with $\mathbb{A}$ and $\mathbb{F}$, respectively. Similarly, let us define $\mathcal{A}^+_{\mathbb{A}}$ and $\mathcal{A}^+_{\mathbb{F}}$ by replacing $\mathbb{Q}(q)$ with $\mathbb{A}$ and $\mathbb{F}$ in the definition of $\mathcal{A}^+$, respectively (more precisely, by requiring r of (5.4) to have coefficients in $\mathbb{A}$ or $\mathbb{F}$, respectively). Then we have a commutative diagram:

$$\begin{tikzcd} U_{\mathbb{A}}(L\mathfrak{n}^+) \arrow[r, "\Upsilon_{\mathbb{A}}"] \arrow[d, "\jmath"] & \mathcal{A}^+_{\mathbb{A}} \arrow[d] \\ U_{\mathbb{F}}(L\mathfrak{n}^+) \arrow[r, "\Upsilon_{\mathbb{F}}"] & \mathcal{A}^+_{\mathbb{F}} \end{tikzcd}$$

where the horizontal maps are defined by analogy with Υ (just over different coefficient rings). Note that the right-most map is injective, but the left-most map is not necessarily so, due to the fact that $U_{\mathbb{A}}(L\mathfrak{n}^+)$ might have $\mathbb{A}$-torsion.

Claim 5.8. *The map* $\Upsilon_{\mathbb{F}}$ *is injective.*

Let us first show how Claim 5.8 allows us to complete the proof of the Proposition. The assignment $q = e^\hbar$ gives us vertical maps which make the following diagram commute:

$$\begin{tikzcd} U_q(L\mathfrak{n}^+) \arrow[r, "\Upsilon"] \arrow[d] & \mathcal{A}^+ \arrow[d] \\ U_{\mathbb{F}}(L\mathfrak{n}^+) \arrow[r, "\Upsilon_{\mathbb{F}}"] & \mathcal{A}^+_{\mathbb{F}} \end{tikzcd}$$

We need to show that the top map is injective. Since the claim tells us that the bottom map is injective, then it suffices to show that the left-most map is injective. The latter claim follows from the fact that $U_q(L\mathfrak{n}^+)$ (respectively $U_{\mathbb{F}}(L\mathfrak{n}^+)$) is a free $\mathbb{Q}(q)$ (respectively $\mathbb{F}$) module with a basis given by ordered products of the root vectors $\{E_{(\alpha,d)}\}^{d\in\mathbb{Z}}_{\alpha\in\Delta^+}$ from Remark 4.26. In the case of $U_q(L\mathfrak{n}^+)$, this is precisely (4.44), while in the case of $U_{\mathbb{F}}(L\mathfrak{n}^+)$ one simply does the same proof, replacing the field $\mathbb{Q}(q)$ by $\mathbb{F}$ everywhere.

Let us now prove Claim 5.8. Consider any $x \in U_{\mathbb{F}}(L\mathfrak{n}^+)$ such that $\Upsilon_{\mathbb{F}}(x) = 0$, and our goal is to prove that $x = 0$. We may write:

$$x = \frac{\jmath(y)}{\hbar^k}$$

for some $k \in \mathbb{N}$ and $y \in U_{\mathbb{A}}(L\mathfrak{n}^+)$, and assume for the purpose of contradiction that $\jmath(y) \neq 0$. The fact that $\Upsilon_{\mathbb{F}}(x) = 0$ and the injectivity of the map $\mathcal{A}^+_{\mathbb{A}} \to \mathcal{A}^+_{\mathbb{F}}$ implies that $\Upsilon_{\mathbb{A}}(y) = 0$. By [10, Corollary 1.4], this implies that:

$$y \in \bigcap_{n=0}^{\infty} \hbar^n \cdot U_{\mathbb{A}}(L\mathfrak{n}^+)$$

Thus, for all $n \geq 0$, there exists $y_n \in U_{\mathbb{A}}(L\mathfrak{n}^+)$ such that $y = \hbar^n y_n$. Passing this equality through the map $\jmath$, we have for all $n \geq 0$:

$$\jmath(y) = \hbar^n \cdot \jmath(y_n) \tag{5.7}$$

However, because y and y_n's lie in $U_{\mathbb{A}}(L\mathfrak{n}^+)$, their images under $\jmath$ will lie in the free $\mathbb{A}$-submodule of $U_{\mathbb{F}}(L\mathfrak{n}^+)$ spanned by ordered products of the root vectors $E_{(\alpha,d)}$ (this statement uses the fact that the generators $e_{i,d}$ of $U_{\mathbb{A}}(L\mathfrak{n}^+)$ are among the $E_{(\alpha,d)}$'s together with the fact that the structure constants of arbitrary products of $E_{(\alpha,d)}$'s lie in $\mathbb{Z}[q,q^{-1}] \subset \mathbb{A}$, as follows from [14]). Therefore, there exist uniquely determined constants $c^{d_1,\dots,d_k}_{\alpha_1,\dots,\alpha_k} \in \mathbb{A}$ such that:

$$\jmath(y) \ = \sum_{(\alpha_1,d_1)\leq\dots\leq(\alpha_k,d_k)}^{k\in\mathbb{N}} c^{d_1,\dots,d_k}_{\alpha_1,\dots,\alpha_k} \cdot E_{(\alpha_1,d_1)} \dots E_{(\alpha_k,d_k)}$$

But if in (5.7) we take n larger than the leading power of $\hbar$ in all the $c^{d_1,\dots,d_k}_{\alpha_1,\dots,\alpha_k}$ which appear as coefficients of $\jmath(y)$, we obtain a contradiction. $\square$

Remark 5.9. In type A_{n-1} (and its affine version corresponding to quantum toroidal algebras of $\mathfrak{sl}_n$), a proof of Proposition 5.7 was provided in [33, Theorem 1.1]. In simply laced finite types (as well as simply laced affine types), a proof of injectivity follows from [43, Theorem 2.3.2(b) combined with formula (2.50)], using the framework of K-theoretic Hall algebras of quivers, see [41]. In contrast, our proof of Proposition 5.7 for all finite types is based on [10] and the PBW bases of Section 4.

5.10. Define the extended shuffle algebras as:

$$\mathcal{A}^{\geq} = \mathcal{A}^+ \otimes \mathbb{Q}(q) \left[(\varphi^+_{i,0})^{\pm 1}, \varphi^+_{i,1}, \varphi^+_{i,2}, \dots\right]_{i\in I} \tag{5.8}$$

$$\mathcal{A}^{\leq} = \mathcal{A}^- \otimes \mathbb{Q}(q) \left[(\varphi^-_{i,0})^{\pm 1}, \varphi^-_{i,1}, \varphi^-_{i,2}, \dots\right]_{i\in I} \tag{5.9}$$

with pairwise commuting φ's, where the multiplication is governed by the rule:

$$\varphi_j^{\pm}(w) * R^{\pm}(\dots, z_{ia}, \dots) = R^{\pm}(\dots, z_{ia}, \dots) * \varphi_j^{\pm}(w) \cdot \prod_{i \in I} \prod_{a=1}^{k_i} \frac{\zeta_{ji}\left(w/z_{ia}\right)^{\pm 1}}{\zeta_{ij}\left(z_{ia}/w\right)^{\pm 1}} \tag{5.10}$$

for any $R^{\pm} \in \mathcal{A}_{\pm\mathbf{k}}$, where the ζ-factors are expanded as power series in non-negative powers of $w^{\mp 1}$. Above, as before, we encode all φ's into the generating series:

$$\varphi_i^{\pm}(w) = \sum_{d=0}^{\infty} \frac{\varphi_{i,d}^{\pm}}{w^{\pm d}} \tag{5.11}$$

Our reason for defining the extended shuffle algebras is that they admit coproducts.

Proposition 5.11. *([10], see also [32,33]) There exist bialgebra structures on $\mathcal{A}^{\geq}$ and $\mathcal{A}^{\leq}$, with coproduct determined by:*

$$\Delta(\varphi_i^{\pm}(z)) = \varphi_i^{\pm}(z) \otimes \varphi_i^{\pm}(z) \tag{5.12}$$

and the following assignments for all $R^{\pm} \in \mathcal{A}_{\pm\mathbf{k}}$:

$$\Delta(R^+) \;=\; \sum_{\mathbf{l}=\sum_{i \in I} l_i \alpha_i \in Q^+,\ l_i \leq k_i} \frac{\left[\prod_{i \in I}^{a > l_i} \varphi_i^+(z_{ia})\right] * R^+(z_{i,a \leq l_i} \otimes z_{i,a > l_i})}{\prod_{i,i' \in I} \prod_{a \leq l_i}^{a' > l_{i'}} \zeta_{i'i}(z_{i'a'}/z_{ia})} \tag{5.13}$$

$$\Delta(R^-) \;=\; \sum_{\mathbf{l}=\sum_{i \in I} l_i \alpha_i \in Q^+,\ l_i \leq k_i} \frac{R^-(z_{i,a \leq l_i} \otimes z_{i,a > l_i}) * \left[\prod_{i \in I}^{a \leq l_i} \varphi_i^-(z_{ia})\right]}{\prod_{i,i' \in I} \prod_{a \leq l_i}^{a' > l_{i'}} \zeta_{ii'}(z_{ia}/z_{i'a'})} \tag{5.14}$$

Remark 5.12. To think of (5.13) as a well-defined tensor, we expand the right-hand side in non-negative powers of $z_{ia}/z_{i'a'}$ for $a \leq l_i$ and $a' > l_{i'}$, thus obtaining an infinite sum of monomials. In each of these monomials, we put the symbols $\varphi_{i,d}^+$ to the very left of the expression, then all powers of z_{ia} with $a \leq l_i$, then the $\otimes$ sign, and finally all powers of z_{ia} with $a > l_i$. The resulting expression will be a power series, and therefore lies in a completion of $\mathcal{A}^{\geq} \otimes \mathcal{A}^+$. The same argument applies to (5.14), still using non-negative powers of $z_{ia}/z_{i'a'}$ for $a \leq l_i$ and $a' > l_{i'}$, and keeping all the $\varphi_{i,d}^-$ to the very right.

The following is straightforward.

Proposition 5.13. *The maps (5.6) extend to bialgebra homomorphisms:*

$$U_q(L\mathfrak{b}^+) \xrightarrow{\Upsilon} \mathcal{A}^{\geq} \quad \text{and} \quad U_q(L\mathfrak{b}^-) \xrightarrow{\Upsilon} \mathcal{A}^{\leq} \tag{5.15}$$

by sending $\varphi_{i,d}^{\pm} \in U_q(L\mathfrak{b}^+), U_q(L\mathfrak{b}^-)$ to the same-named $\varphi_{i,d}^{\pm} \in \mathcal{A}^{\geq}, \mathcal{A}^{\leq}$.

5.14. There exists a bialgebra pairing between $\mathcal{A}^{\geq}$ and $\mathcal{A}^{\leq}$. As a first step toward defining it, we start with the following result. Let $Dz = \frac{dz}{2\pi i z}$.

Proposition 5.15. *There exists a unique bialgebra pairing:*

$$\langle \cdot, \cdot \rangle : \ \mathcal{A}^{\geq} \otimes U_q(L\mathfrak{b}^-) \longrightarrow \mathbb{Q}(q) \tag{5.16}$$

satisfying (4.39) *as well as:*

$$\Big\langle R, f_{i_1,-d_1} \dots f_{i_k,-d_k} \Big\rangle = \prod_{a=1}^{k} (q_{i_a}^{-1} - q_{i_a})^{-1} \int_{|z_1| \ll \dots \ll |z_k|} \frac{R(z_1, \dots, z_k) z_1^{-d_1} \dots z_k^{-d_k}}{\prod_{1 \leq a < b \leq k} \zeta_{i_a i_b}(z_a/z_b)} \prod_{a=1}^{k} Dz_a \tag{5.17}$$

for any $k \in \mathbb{N}$, $i_1, \dots, i_k \in I$, $d_1, \dots, d_k \in \mathbb{Z}$, $R \in \mathcal{A}_{\alpha_{i_1}+\dots+\alpha_{i_k}, d_1+\dots+d_k}$ (all pairings between elements of non-opposite degrees are set to be 0). In the right-hand side of (5.17)*, we plug each variable z_a into an argument of color i_a of the function R; since the latter is color-symmetric, the result is independent of any choices made.*

Proof. This Proposition is a slight variant of the analogous result from [10, §3.2] (in that the wheel conditions (5.5) play a crucial role in our formulation, while in [10] only $\operatorname{Im} \Upsilon \subset \mathcal{A}^+$ is considered; by Theorem 1.7, the two settings are a posteriori equivalent), so we will only sketch the proof.

First of all, we need to show that the formula (5.17) gives rise to a well-defined pairing $\mathcal{A}^+ \otimes U_q(L\mathfrak{n}^-) \to \mathbb{Q}(q)$. To do this, we need to acknowledge the fact that relations (4.28) and (4.29) (or more precisely, the opposite of these relations, since we are using f's instead of e's) imply linear relations between the various $f_{i_1,-d_1} \dots f_{i_k,-d_k}$, and we need to check that these relations also hold in the right-hand side of (5.17). Explicitly, the equalities in question read:

$$f_{i,-r+1} f_{j,-s} q^{d_{ij}} - f_{i,-r} f_{j,-s+1} = f_{j,-s} f_{i,-r+1} - f_{j,-s+1} f_{i,-r} q^{d_{ij}} \tag{5.18}$$

for all $i, j \in I$ and all $r, s \in \mathbb{Z}$, and:

$$\sum_{\sigma \in S(1-a_{ij})} \sum_{k=0}^{1-a_{ij}} (-1)^k \binom{1-a_{ij}}{k}_i \cdot f_{i,-r_{\sigma(1)}} \dots f_{i,-r_{\sigma(k)}} f_{j,-s} f_{i,-r_{\sigma(k+1)}} \dots f_{i,-r_{\sigma(1-a_{ij})}} = 0 \tag{5.19}$$

for all distinct $i, j \in I$ and all $r_1, \dots, r_{1-a_{ij}}, s \in \mathbb{Z}$. If we multiply the above formulas both on the left and the right with arbitrary products of f's, then we obtain various linear relations between products $f_{i_1,-d_1} \dots f_{i_k,-d_k}$. The issue as to why these linear relations hold in the right-hand side of (5.17) is an interesting, but straightforward, exercise that we leave to the interested reader: in the case of (5.18) it is because any rational function $R \in \mathcal{A}^+$ can be written as in (5.4) with r a Laurent polynomial, while in the case of (5.19) it is because this r satisfies the wheel conditions (5.5). Details can be found in [9, §2–3] and [7], cf. our proof of Proposition 5.23.

Showing that one can upgrade the pairing of vector spaces (5.17) to a bialgebra pairing as in (5.16) involves a straightforward check of properties (4.6) and (4.7). The interested reader can find the details in the final arχiv version of the present paper. □

5.16. We note the following immediate consequence of formula (5.17).

Proposition 5.17. *The pairing (5.16) is non-degenerate in the first argument:*

$$\Big\langle R, - \Big\rangle = 0 \quad \Rightarrow \quad R = 0$$

for any $R \in \mathcal{A}^{\geq}$.

Proof. Because of (5.8), elements of $\mathcal{A}^{\geq}$ are linear combinations of $R \cdot \varphi^+$, where:

$$R \in \mathcal{A}^+ \qquad \text{and} \qquad \varphi^+ \in \mathbb{Q}(q) \left[(\varphi^+_{i,0})^{\pm 1}, \varphi^+_{i,1}, \varphi^+_{i,2}, \dots \right]_{i \in I}$$

As a consequence of the bialgebra pairing properties (4.6)–(4.7), it is easy to see that:

$$\Big\langle R\varphi^+, x\varphi^- \Big\rangle = \Big\langle R, x \Big\rangle \cdot \Big\langle \varphi^+, \varphi^- \Big\rangle$$

for any $x \in U_q(L\mathfrak{n}^-)$ and φ^- a product of $\varphi^-_{i,d}$'s. Thus the non-degeneracy of the pairing (5.16) is a consequence of the non-degeneracy of its restriction:

$$\langle \cdot, \cdot \rangle \colon \ \mathcal{A}^+ \otimes U_q(L\mathfrak{n}^-) \longrightarrow \mathbb{Q}(q) \tag{5.20}$$

(indeed, the pairing between φ's is easily seen to be non-degenerate, due to the explicit formula (4.39)). However, the non-degeneracy of (5.20) in the first argument is an immediate consequence of formula (5.17): if R is a non-zero rational function, then we simply choose an arbitrary order of its variables $|z_1| \ll \dots \ll |z_k|$, and consider the leading order term of R when expanded as a power series in this particular order. On one hand, the coefficient of this leading order term must be non-zero, but on the other hand, it is of the form in the right-hand side of (5.17). □

We note that the pairings (4.37) and (5.16) are compatible, in the sense that:

$$\Big\langle x, y \Big\rangle = \Big\langle \Upsilon(x), y \Big\rangle \tag{5.21}$$

for all $x \in U_q(L\mathfrak{b}^+)$ and $y \in U_q(L\mathfrak{b}^-)$. Indeed, both sides of (5.21) define bialgebra pairings:

$$U_q(L\mathfrak{b}^+) \otimes U_q(L\mathfrak{b}^-) \longrightarrow \mathbb{Q}(q)$$

which coincide on the generators, thus must be equal as a consequence of (4.6)–(4.7).

Combining (5.21) with Propositions 5.7, 5.17, we thus obtain the non-degeneracy statement of Proposition 4.22 (strictly speaking, we obtain the aforementioned non-degeneracy statement only in the first argument, but the case of the second argument is treated by simply switching the roles of $+$ and $-$ everywhere).

5.18. Once Theorem 1.7 will be proved, Proposition 5.15 can be construed as the existence of a bialgebra pairing (which is non-degenerate by Proposition 4.22):

$$\langle \cdot, \cdot \rangle \colon \mathcal{A}^{\geq} \otimes \mathcal{A}^{\leq} \longrightarrow \mathbb{Q}(q)$$

Hence, we may construct the Drinfeld double:

$$\mathcal{A} \ := \ \mathcal{A}^{\geq} \otimes \mathcal{A}^{\leq} / (\varphi^+_{i,0} \otimes \varphi^-_{i,0} - 1 \otimes 1) \tag{5.22}$$

Since all the structures (product, coproduct, and pairing) are preserved by Υ, we conclude that Proposition 5.13 and Theorem 1.7 imply the following result.

Theorem 5.19. *There exists a bialgebra isomorphism:*

$$U_q(L\mathfrak{g}) \xrightarrow{\Upsilon} \mathcal{A} \tag{5.23}$$

which maps

$$e_{i,d} \mapsto z_{i1}^d \in \mathcal{A}^+, \ f_{i,d} \mapsto z_{i1}^d \in \mathcal{A}^-, \ \varphi^{\pm}_{i,r} \mapsto \varphi^{\pm}_{i,r}$$

5.20. Let us consider the linear map:

$$\mathcal{A}^+ \xrightarrow{\iota} \mathcal{F}^L \tag{5.24}$$

given by the following formula:

$$\iota(R) \ = \sum_{\substack{i_1,\dots,i_k \in I \\ d_1,\dots,d_k \in \mathbb{Z}}} \left[\prod_{a=1}^k (q_{i_a}^{-1} - q_{i_a}) \right] \left\langle R, f_{i_1,-d_1} \dots f_{i_k,-d_k} \right\rangle \cdot \left[i_1^{(d_1)} \dots i_k^{(d_k)} \right] \tag{5.25}$$

for all $R \in \mathcal{A}_{\mathbf{k}}$, where $k = |\mathbf{k}|$. Because of (5.17), we have the explicit formula:

$$\iota(R) \ = \sum_{\substack{i_1,\dots,i_k \in I \\ d_1,\dots,d_k \in \mathbb{Z}}} \left[i_1^{(d_1)} \dots i_k^{(d_k)} \right] \cdot \int_{|z_1| \ll \dots \ll |z_k|} \frac{R(z_1, \dots, z_k) z_1^{-d_1} \dots z_k^{-d_k}}{\prod_{1 \leq a < b \leq k} \zeta_{i_a i_b}(z_a/z_b)} \prod_{a=1}^k Dz_a \tag{5.26}$$

where all sequences $i_1, \dots, i_k \in I$ that appear in the formula above satisfy:

$$\alpha_{i_1} + \dots + \alpha_{i_k} = \mathbf{k}$$

and each variable z_a is plugged into an argument of color i_a of the function R (since the latter is color-symmetric, the result is independent of any choices made). It is easy to see that $\iota(R)$ indeed lands in the completion (4.55)–(4.56).

As a consequence of the non-degeneracy of the pairing (5.20) in the first argument, we conclude that ι is injective. Comparing (5.10) with (4.58), we can further extend (5.24) to an algebra homomorphism:

$$\mathcal{A}^{\geq} \overset{\iota}{\hookrightarrow} \mathcal{F}^{L,\text{ext}} \tag{5.27}$$

sending $\varphi^+_{i,r} \mapsto \varphi^+_{i,r}$.

Proposition 5.21. *The map ι of (5.27) is a bialgebra homomorphism.*

Proof. The first thing we need to prove is that ι is an algebra homomorphism. Since the multiplicative relations involving the $\varphi^+_{i,r}$'s are the same for the domain and target of (5.27) (this is so by design), then it suffices to show that the map (5.24) is an algebra homomorphism. In other words, we must show that ι intertwines the product (5.2) on $\mathcal{A}^+$ with the product (4.50) on $\mathcal{F}^L$. To this end, consider any $F \in \mathcal{A}_{\mathbf{k}}$, $G \in \mathcal{A}_{\mathbf{l}}$ and let $k = |\mathbf{k}|$, $l = |\mathbf{l}|$. According to (5.26), $\iota(F * G)$ equals:

$$\sum_{\substack{s_1,\dots,s_{k+l} \in I \\ t_1,\dots,t_{k+l} \in \mathbb{Z}}} \left[s_1^{(t_1)} \dots s_{k+l}^{(t_{k+l})}\right] \int_{|z_1| \ll \dots \ll |z_{k+l}|} \frac{(F * G)(z_1, \dots, z_{k+l}) z_1^{-t_1} \dots z_{k+l}^{-t_{k+l}}}{\prod_{1 \leq a < b \leq k+l} \zeta_{s_a s_b}(z_a/z_b)} \prod_{a=1}^{k+l} Dz_a$$

where we implicitly assume that $s_1, \dots, s_{k+l} \in I$ are acceptable in the sense that:

$$\alpha_{s_1} + \dots + \alpha_{s_{k+l}} = \mathbf{k} + \mathbf{l}$$

According to the definition of the shuffle product in (5.2), we have:

$$(F * G)(z_1, \dots, z_{k+l}) \ = \sum_{A \sqcup B = \{1,\dots,k+l\}}^{\text{acceptable partitions}} F\left(\{z_a\}_{a \in A}\right) G\left(\{z_b\}_{b \in B}\right) \prod_{a \in A, b \in B} \zeta_{s_a s_b}\left(\frac{z_a}{z_b}\right)$$

where a partition $A \sqcup B = \{1, \dots, k + l\}$ is called acceptable if the number of variables of each color in the set A (resp. B) is equal to the number of variables of that color of the rational function F (resp. G). With this in mind, we conclude:

$$\iota(F * G) \ = \sum_{\substack{s_1,\dots,s_{k+l} \in I \\ t_1,\dots,t_{k+l} \in \mathbb{Z}}} \left[s_1^{(t_1)} \dots s_{k+l}^{(t_{k+l})}\right] \sum_{A \sqcup B = \{1,\dots,k+l\}}^{\text{acceptable partitions}} \int_{|z_1| \ll \dots \ll |z_{k+l}|}$$

$$\frac{F(\{z_a\}_{a\in A})\prod_{a\in A} z_a^{-t_a}}{\prod_{a<a'\in A}\zeta_{s_a s_{a'}}(z_a/z_{a'})}\cdot\frac{G(\{z_b\}_{b\in B})\prod_{b\in B} z_b^{-t_b}}{\prod_{b<b'\in B}\zeta_{s_b s_{b'}}(z_b/z_{b'})}\prod_{A\ni a>b\in B}\frac{\zeta_{s_a s_b}\left(\frac{z_a}{z_b}\right)}{\zeta_{s_b s_a}\left(\frac{z_b}{z_a}\right)}\prod_{a=1}^{k+l} Dz_a \tag{5.28}$$

For various $a \in A$ and $b \in B$, the expression above has poles involving z_a and z_b only if $a > b$. This implies that the value of the integral above is unchanged if we move the variables in such a way that all the z_a's with $a \in A$ are much greater than all the z_b's with $b \in B$. In other words we may replace:

$$\int_{|z_1|\ll\dots\ll|z_{k+l}|} \quad \text{by} \quad \int_{|x_1|\ll\dots\ll|x_l|\ll|y_1|\ll\dots\ll|y_k|}$$

where $x_1,\dots,x_l$ (resp. $y_1,\dots,y_k$) are simply relabellings of the variables $\{z_b\}_{b\in B}$ in the increasing order of b (resp. $\{z_a\}_{a\in A}$ in the increasing order of a). Moreover, let $i_1,\dots,i_k,d_1,\dots,d_k$ (resp. $j_1,\dots,j_l,e_1,\dots,e_l$) refer to those of the elements $s_c \in I$ and $t_c \in \mathbb{Z}$ for $c \in A$ (resp. $c \in B$), as in formula (4.51). It is straightforward to see that applying the shuffle product (4.50) to $\iota(F)$ and $\iota(G)$ gives us precisely (5.28). Therefore, $\iota(F * G) = \iota(F) * \iota(G)$, as claimed.

The second thing we need to prove is that the map ι is a coalgebra homomorphism, i.e. that it intertwines the coproduct (5.13) on $\mathcal{A}^{\geq}$ with the coproduct (4.59) on $\mathcal{F}^{L,\mathrm{ext}}$. To this end, consider any $R \in \mathcal{A}_{\mathbf{k}}$ and note that (5.13) reads:

$$\Delta(R) = \sum_{\mathbf{l}=\sum_{i\in I} l_i\alpha_i\in Q^+}^{l_i\leq k_i}\sum_{\pi_{ia}\geq 0}\frac{\prod_{i\in I}^{a>l_i}\varphi^+_{i,\pi_{ia}} * R(z_{i,a\leq l_i}\otimes z_{i,a>l_i})\prod_{i\in I}^{a>l_i} z_{ia}^{-\pi_{ia}}}{\prod_{i,i'\in I}\prod_{a\leq l_i}^{a'>l_{i'}}\zeta_{i'i}(z_{i'a'}/z_{ia})}$$

where the second sum is over all collections of non-negative integers $\{\pi_{ia}\}_{i\in I}^{l_i<a\leq k_i}$. Applying the map $\iota\otimes\iota$ to the above expression, we obtain by (5.26):

$$(\iota\otimes\iota)(\Delta(R)) =$$
$$\sum_{\substack{i_1,\dots,i_k\in I\\ d_1,\dots,d_k\in\mathbb{Z}\\ \pi_{l+1},\dots,\pi_k\geq 0}}^{0\leq l\leq k}\varphi^+_{i_{l+1},\pi_{l+1}}\dots\varphi^+_{i_k,\pi_k}\left[i_1^{(d_1)}\dots i_l^{(d_l)}\right]\otimes\left[i_{l+1}^{(d_{l+1})}\dots i_k^{(d_k)}\right]\cdot$$
$$\int_{|z_1|\ll\dots\ll|z_k|}\frac{R(z_1,\dots,z_k)\prod_{a=l+1}^k z_a^{-\pi_a}\prod_{a=1}^k z_a^{-d_a}Dz_a}{\prod_{1\leq a<b\leq l}\zeta_{i_a i_b}(z_a/z_b)\prod_{l<a<b\leq k}\zeta_{i_a i_b}(z_a/z_b)\prod_{a\leq l<b}\zeta_{i_b i_a}(z_b/z_a)}$$

If we substitute $d_a \mapsto d_a - \pi_a$ for $a \in \{l+1,\dots,k\}$ in the above relation, and use (4.58) to commute the product of φ's to the right of the word $[i_1^{(d_1)}\dots i_l^{(d_l)}]$, then we obtain precisely formula (4.59) for $\Delta(\iota(R))$, as required. □

5.22. As:

$$\iota(\Upsilon(e_{i,d})) = \left[i^{(d)}\right] = \Phi^L(e_{i,d})$$

for any $i \in I$ and $d \in \mathbb{Z}$, the composition of the maps (5.6) and (5.24) recovers (4.53):

$$\Phi^L : \ U_q(L\mathfrak{n}^+) \xrightarrow{\Upsilon} \mathcal{A}^+ \xrightarrow{\iota} \mathcal{F}^L \tag{5.29}$$

The main result of this Section, Theorem 1.7, states that the map Υ is an isomorphism, so it would naturally imply that the image of Φ^L is equal to the image of ι. Therefore, let us characterize the latter, by analogy with (4.24)–(4.25).

Proposition 5.23. *We have:*

$$\mathrm{Im}\,\iota = \left\{ \sum_{\substack{i_1,\dots,i_k \in I \\ d_1,\dots,d_k \in \mathbb{Z}}}^{k \in \mathbb{N}} \gamma \begin{pmatrix} i_1 & \dots & i_k \\ d_1 & \dots & d_k \end{pmatrix} \cdot \left[i_1^{(d_1)} \dots i_k^{(d_k)} \right] \right\} \tag{5.30}$$

where the scalars $\gamma \begin{pmatrix} i_1 & \dots & i_k \\ d_1 & \dots & d_k \end{pmatrix} \in \mathbb{Q}(q)$ *vanish for all but finitely many values of* $(\mathbf{k}, d) = (\alpha_{i_1} + \dots + \alpha_{i_k}, d_1 + \dots + d_k) \in Q^+ \times \mathbb{Z}$ *and satisfy equations (5.31)–(5.34):*

$$\exists M \text{ s.t. } \gamma \begin{pmatrix} i_1 & \dots & i_k \\ d_1 & \dots & d_k \end{pmatrix} = 0 \text{ if } d_1 + \dots + d_a < M \text{ for some } 1 \le a < k \tag{5.31}$$

$$\gamma \begin{pmatrix} w & i & j & w' \\ \chi & r-1 & s & \chi' \end{pmatrix} - \gamma \begin{pmatrix} w & i & j & w' \\ \chi & r & s-1 & \chi' \end{pmatrix} q^{-d_{ij}} = \gamma \begin{pmatrix} w & j & i & w' \\ \chi & s & r-1 & \chi' \end{pmatrix} q^{-d_{ij}} - \gamma \begin{pmatrix} w & j & i & w' \\ \chi & s-1 & r & \chi' \end{pmatrix} \tag{5.32}$$

for all $i, j \in I$ *and* $r, s \in \mathbb{Z}$. *Moreover:*

$$\sum_{\sigma \in S(1-a_{ij})} \sum_{k=0}^{1-a_{ij}} (-1)^k \binom{1-a_{ij}}{k}_i \cdot \gamma \begin{pmatrix} w & i & \dots & i & j & i & \dots & i & w' \\ \chi & p_{\sigma(1)} & \dots & p_{\sigma(k)} & t & p_{\sigma(k+1)} & \dots & p_{\sigma(1-a_{ij})} & \chi' \end{pmatrix} = 0 \tag{5.33}$$

for all distinct $i, j \in I$ *and* $p_1, \dots, p_{1-a_{ij}}, t \in \mathbb{Z}$. *In the formulas above,* w, w' *denote arbitrary finite words and* χ, χ' *denote arbitrary collections of integers, so that* $(w, \chi), (w', \chi')$ *encode a pair of arbitrary loop words. Finally, we require:*

$$\sum_{\substack{\varepsilon_{ab}\in\{0,1\},\\ \forall\, 1\le a<b\le k}} \prod_{a<b}^{\varepsilon_{ab}=1} (-q^{-d_{i_a i_b}})\cdot$$

$$\gamma\begin{pmatrix} \dots & i_a & \dots \\ \dots & d_a - \#\{b>a|\varepsilon_{ab}=0\} - \#\{b<a|\varepsilon_{ba}=1\} & \dots \end{pmatrix} = 0 \quad (5.34)$$

for all but finitely many $(d_1,\dots,d_k)\in\mathbb{Z}^k$ *(note that there are only finitely many choices of* $i_1,\dots,i_k\in I$ *in formula (5.34), because* I *is a finite set).*

Proof. Consider any $R\in\mathcal{A}_{\mathbf{k},d}$ and set $k=|\mathbf{k}|$. Since ι is injective, $\iota(R)$ is completely determined by the collection of $\gamma(\dots)\in\mathbb{Q}(q)$ that appear in (5.30), which can be thought of as a function:

$$\gamma\colon \left\{\begin{pmatrix} i_1 & \dots & i_k \\ d_1 & \dots & d_k \end{pmatrix} \text{ s.t. } \sum_{a=1}^k \alpha_{i_a} = \mathbf{k},\ \sum_{a=1}^k d_a = d\right\} \longrightarrow \mathbb{Q}(q) \quad (5.35)$$

subject to the constraint (5.31).

For any $1\le a<b\le k$, consider the following operator on the set of such functions:

$$\tau_{ab}(\gamma)\begin{pmatrix} \dots & i_a & \dots & i_b & \dots \\ \dots & d_a & \dots & d_b & \dots \end{pmatrix} =$$
$$\gamma\begin{pmatrix} \dots & i_a & \dots & i_b & \dots \\ \dots & d_a-1 & \dots & d_b & \dots \end{pmatrix} - \gamma\begin{pmatrix} \dots & i_a & \dots & i_b & \dots \\ \dots & d_a & \dots & d_b-1 & \dots \end{pmatrix} q^{-d_{i_a i_b}} \quad (5.36)$$

It is easy to see that the various operators τ_{ab} commute with each other. This notion is motivated by the obvious observation that if a function γ encodes the coefficients of $\iota(R)$:

$$\gamma\begin{pmatrix} i_1 & \dots & i_k \\ d_1 & \dots & d_k \end{pmatrix} = \int_{|z_1|\ll\dots\ll|z_k|} \frac{R(z_1,\dots,z_k) z_1^{-d_1}\dots z_k^{-d_k}}{\prod_{1\le a<b\le k}\zeta_{i_a i_b}(z_a/z_b)} \prod_{a=1}^k Dz_a \quad (5.37)$$

then:

$$\tau_{c,c+1}(\gamma)\begin{pmatrix} \dots & i_c & i_{c+1} & \dots \\ \dots & d_c & d_{c+1} & \dots \end{pmatrix} =$$
$$\int_{\dots\ll|z_c|\ll|z_{c+1}|\ll\dots} \frac{R(z_1,\dots,z_k)(z_c-z_{c+1}) z_1^{-d_1}\dots z_k^{-d_k}}{\prod_{1\le a<b\le k,(a,b)\neq(c,c+1)}\zeta_{i_a i_b}(z_a/z_b)} \prod_{a=1}^k Dz_a \quad (5.38)$$

Similarly, (5.37) implies:

$$-\tau_{c,c+1}(\gamma)\begin{pmatrix} \dots & i_{c+1} & i_c & \dots \\ \dots & d_{c+1} & d_c & \dots \end{pmatrix} =$$

$$\int_{\dots \ll |z_{c+1}| \ll |z_c| \ll \dots} \frac{R(z_1, \dots, z_k)(z_c - z_{c+1}) z_1^{-d_1} \dots z_k^{-d_k}}{\prod_{1 \leq a < b \leq k, (a,b) \neq (c,c+1)} \zeta_{i_a i_b}(z_a/z_b)} \prod_{a=1}^{k} Dz_a \tag{5.39}$$

The right-hand sides of (5.38) and (5.39) have the same integrand. Moreover, because elements $R \in \mathcal{A}^+$ only have poles as prescribed in (5.4), the integrand in question has no poles involving z_c and z_{c+1}. Therefore, one may change the order of variables in the integral from $|z_c| \ll |z_{c+1}|$ to $|z_{c+1}| \ll |z_c|$ without changing the value of the integral, which implies that the right-hand sides of (5.38) and (5.39) are equal. Hence, we conclude that if a function γ as in (5.35) encodes the coefficients of $\iota(R)$ for some $R \in \mathcal{A}^+$, then:

$$\tau_{c,c+1}(\gamma) \begin{pmatrix} \dots & i_c & i_{c+1} & \dots \\ \dots & d_c & d_{c+1} & \dots \end{pmatrix} = -\tau_{c,c+1}(\gamma) \begin{pmatrix} \dots & i_{c+1} & i_c & \dots \\ \dots & d_{c+1} & d_c & \dots \end{pmatrix} \tag{5.40}$$

for all c, which is precisely the linear constraint (5.32).

Going further, one may iterate the process of going from (5.37) to (5.38) a number of $\frac{k(k-1)}{2}$ times, obtaining:

$$\left(\prod_{1 \leq a < b \leq k} \tau_{ab} \right) (\gamma) \begin{pmatrix} i_1 & \dots & i_k \\ d_1 & \dots & d_k \end{pmatrix} =$$
$$\int_{|z_1| \ll \dots \ll |z_k|} R(z_1, \dots, z_k) z_1^{-d_1} \dots z_k^{-d_k} \prod_{1 \leq a < b \leq k} (z_a - z_b) \prod_{a=1}^{k} Dz_a$$

The product $R(z_1, \dots, z_k) \prod_{1 \leq a < b \leq k} (z_a - z_b)$ is a Laurent polynomial, due to (5.4), hence the integral above vanishes for all but finitely many values of $(d_1, \dots, d_k)$:

$$\left(\prod_{1 \leq a < b \leq k} \tau_{ab} \right) (\gamma) \begin{pmatrix} i_1 & \dots & i_k \\ d_1 & \dots & d_k \end{pmatrix} = 0 \quad \text{for all but finitely many } (d_1, \dots, d_k) \in \mathbb{Z}^k \tag{5.41}$$

Unpacking the definition of τ in (5.36), we see that identity (5.41) is precisely equivalent to the linear constraint (5.34).

Finally, let us consider the linear combination in the left-hand side of (5.33) (to keep our notation simple, we will assume that the words w and w' are vacuous, as this will not interfere with our argument) and replace all the γ's therein by the right-hand sides of (5.37). We obtain the following equality:

$$\mathrm{Sym} \left[\sum_{k=0}^{1-a_{ij}} (-1)^k \binom{1-a_{ij}}{k}_i \cdot \int_{|z_1| \ll \dots \ll |z_k| \ll |w| \ll |z_{k+1}| \ll \dots \ll |z_{1-a_{ij}}|} \right.$$

$$\left.\frac{R(z_1,\dots,z_{1-a_{ij}},w)z_1^{-p_1}\dots z_{1-a_{ij}}^{-p_{1-a_{ij}}}w^{-t}Dz_1\dots Dz_{1-a_{ij}}Dw}{\prod_{b=1}^{k}\zeta_{ij}(z_b/w)\prod_{b=k+1}^{1-a_{ij}}\zeta_{ji}(w/z_b)\prod_{1\le b<c\le 1-a_{ij}}\zeta_{ii}(z_b/z_c)}\right]=0$$

where Sym[...] denotes symmetrization with respect to the z-variables. In the formula above, let us write the rational function R in terms of the Laurent polynomial r of (5.4):

$$\mathrm{Sym}\left[\sum_{k=0}^{1-a_{ij}}\binom{1-a_{ij}}{k}_i\cdot\int_{|z_1|\ll\dots\ll|z_k|\ll|w|\ll|z_{k+1}|\ll\dots\ll|z_{1-a_{ij}}|}\right.$$
$$\left.\frac{r(z_1,\dots,z_{1-a_{ij}},w)z_1^{-p_1}\dots z_{1-a_{ij}}^{-p_{1-a_{ij}}}w^{-t}Dz_1\dots Dz_{1-a_{ij}}Dw}{\prod_{b=1}^{k}(z_b-wq_i^{-a_{ij}})\prod_{b=k+1}^{1-a_{ij}}(w-z_bq_i^{-a_{ij}})\prod_{1\le b<c\le 1-a_{ij}}\zeta_{ii}(z_b/z_c)}\right]=0 \quad (5.42)$$

We claim that formula (5.42) is equivalent to (5.5), due to the combinatorial identity between power series expansions of rational functions and certain formal δ functions established in [9, Proposition 4] (proved in full generality in [7, Theorem 1.1]). Indeed, the validity of (5.42) for all $p_1,\dots,p_{1-a_{ij}},t\in\mathbb{Z}$ is equivalent to the equality:

$$0 \;=\; r(z_1,\dots,z_{1-a_{ij}},w)\cdot \quad (5.43)$$
$$\mathrm{Sym}\left[\sum_{k=0}^{1-a_{ij}}\binom{1-a_{ij}}{k}_i\cdot\prod_{b=1}^{k}\frac{1}{w-q_i^{a_{ij}}z_b}\prod_{b=k+1}^{1-a_{ij}}\frac{1}{z_b-q_i^{a_{ij}}w}\prod_{1\le b<c\le 1-a_{ij}}\frac{z_c-z_b}{z_c-q_i^2z_b}\right]$$

where all rational functions $\frac{1}{x-y}$ above are expanded as formal series $\sum_{r=0}^{\infty}\frac{y^r}{x^{r+1}}$. According to [7, Theorem 1.1], where we set $m=-a_{ij}$ and $q=q_i^{-1}$, we have:

$$\mathrm{Sym}\left[\sum_{k=0}^{1-a_{ij}}\binom{1-a_{ij}}{k}_i\cdot\prod_{b=1}^{k}\frac{1}{w-q_i^{a_{ij}}z_b}\prod_{b=k+1}^{1-a_{ij}}\frac{1}{z_b-q_i^{a_{ij}}w}\prod_{b<c}\frac{z_c-z_b}{z_c-q_i^2z_b}\right]=$$
$$q_i^{1+a_{ij}}\mathrm{Sym}\left[\delta(w,q_i^{-a_{ij}}z_1)\delta(z_1,q_i^{-2}z_2)\delta(z_2,q_i^{-2}z_3)\dots\delta(z_{-a_{ij}},q_i^{-2}z_{1-a_{ij}})\right]$$

where the formal δ-function $\delta(x,y)$ is defined via:

$$\delta(x,y)\;=\;\sum_{r\in\mathbb{Z}}\frac{y^r}{x^{r+1}}\;=\;\underbrace{\frac{1}{x-y}}_{\text{expanded in }|x|\gg|y|}+\underbrace{\frac{1}{y-x}}_{\text{expanded in }|y|\gg|x|}$$

Since r is a Laurent polynomial, the fundamental property of δ implies that:

$$r(z_1,\dots,z_{1-a_{ij}},w)\cdot\delta(w,q_i^{-a_{ij}}z_1)\delta(z_1,q_i^{-2}z_2)\dots\delta(z_{-a_{ij}},q_i^{-2}z_{1-a_{ij}})=$$
$$r(z_1,q_i^2z_1,\dots,q_i^{-2a_{ij}}z_1,q_i^{-a_{ij}}z_1)\cdot\delta(w,q_i^{-a_{ij}}z_1)\delta(z_1,q_i^{-2}z_2)\dots\delta(z_{-a_{ij}},q_i^{-2}z_{1-a_{ij}})$$

Thus (5.43), and hence (5.42), is indeed equivalent to (5.5).

Conversely, suppose we have a function (5.35) satisfying properties (5.31)–(5.34). Our goal is to construct a rational function $R \in \mathcal{A}_{\mathbf{k},d}$ such that (5.37) holds.

For any ordered collection $\mathbf{i} = (i_1, \dots, i_k) \in I^k$ with $\alpha_{i_1} + \dots + \alpha_{i_k} = \mathbf{k}$, define a formal bi-infinite power series $F_{\mathbf{i}}(z_1, \dots, z_k) \in \mathbb{Q}(q)[[z_1, z_1^{-1}, \dots, z_k, z_k^{-1}]]$ via:

$$F_{\mathbf{i}}(z_1, \dots, z_k) \;=\; \sum_{d_1,\dots,d_k \in \mathbb{Z}} \gamma \begin{pmatrix} i_1 & \dots & i_k \\ d_1 & \dots & d_k \end{pmatrix} z_1^{d_1} \dots z_k^{d_k} \tag{5.44}$$

Here, we shall think of the variable z_c being of color i_c for all $1 \le c \le k$. However, due to (5.31), we actually have

$$F_{\mathbf{i}}(z_1, \dots, z_k) \in \mathbb{Q}(q)((z_k)) \dots ((z_2))((z_1)) \tag{5.45}$$

Similarly to (5.41), property (5.34) can be recast as:

$$\int_{|z_1| \ll \dots \ll |z_k|} F_{\mathbf{i}}(z_1, \dots, z_k) \;\cdot \prod_{1 \le a < b \le k} (z_a - z_b q^{-d_{i_a i_b}}) z_1^{-d_1} \dots z_k^{-d_k} \prod_{a=1}^{k} Dz_a = 0$$

for all but finitely many $(d_1, \dots, d_k) \in \mathbb{Z}^k$, which is equivalent to:

$$r_{\mathbf{i}}(z_1, \dots, z_k) := F_{\mathbf{i}}(z_1, \dots, z_k) \;\cdot \prod_{1 \le a < b \le k} (z_a - z_b q^{-d_{i_a i_b}}) \tag{5.46}$$

being a Laurent polynomial. Invoking (5.45), we conclude that:

$$F_{\mathbf{i}}(z_1, \dots, z_k) = \frac{r_{\mathbf{i}}(z_1, \dots, z_k)}{\prod_{1 \le a < b \le k} (z_a - z_b q^{-d_{i_a i_b}})} \tag{5.47}$$

with the right-hand side expanded in $|z_1| \ll \dots \ll |z_k|$. If we let:

$$R_{\mathbf{i}}(z_1, \dots, z_k) := \frac{r_{\mathbf{i}}(z_1, \dots, z_k)}{\prod_{1 \le a < b \le k} (z_a - z_b)} \tag{5.48}$$

then we obtain:

$$\gamma \begin{pmatrix} i_1 & \dots & i_k \\ d_1 & \dots & d_k \end{pmatrix} = \int_{|z_1| \ll \dots \ll |z_k|} \frac{R_{\mathbf{i}}(z_1, \dots, z_k) z_1^{-d_1} \dots z_k^{-d_k}}{\prod_{1 \le a < b \le k} \zeta_{i_a i_b}(z_a / z_b)} \prod_{a=1}^{k} Dz_a \tag{5.49}$$

for all $d_1, \dots, d_k \in \mathbb{Z}$. Let us now prove that the rational functions $R_{\mathbf{i}}$ actually do not depend on $\mathbf{i}$. To do so, note that property (5.40) allows us to recast (5.32) as:

$$\int_{\dots \ll |z_c| \ll |z_{c+1}| \ll \dots} \frac{R_{\mathbf{i}}(z_1, \dots, z_k)(z_c - z_{c+1}) z_1^{-d_1} \dots z_k^{-d_k}}{\prod_{1 \le a < b \le k, (a,b) \neq (c,c+1)} \zeta_{i_a i_b}(z_a/z_b)} \prod_{a=1}^k Dz_a =$$

$$\int_{\dots \ll |z_{c+1}| \ll |z_c| \ll \dots} \frac{R_{\sigma_c(\mathbf{i})}(z_1, \dots, z_k)(z_c - z_{c+1}) z_1^{-d_1} \dots z_k^{-d_k}}{\prod_{1 \le a < b \le k, (a,b) \neq (c,c+1)} \zeta_{i_a i_b}(z_a/z_b)} \prod_{a=1}^k Dz_a$$

for all $d_1, \dots, d_k \in \mathbb{Z}$, where $\sigma_c(\mathbf{i}) = (i_1, \dots, i_{c-1}, i_{c+1}, i_c, i_{c+2}, \dots, i_k)$. As the integrands above have no poles involving z_c and z_{c+1}, we conclude that $R_{\mathbf{i}} = R_{\sigma_c(\mathbf{i})}$. Since this holds for all $c \in \{1, \dots, k-1\}$, we conclude that there exists a unique rational function $R = R_{\mathbf{i}}$, for all $\mathbf{i}$. Moreover, this rational function R must be symmetric in the variables of each color separately, since γ of (5.35) is unchanged if we permute a and b such that $i_a = i_b$ and $d_a = d_b$. Because a rational function which is symmetric in variables z and w cannot have a simple pole at $z = w$, we conclude that the rational function R thus constructed is of the form (5.4).

Finally, the fact that the numerator r of R satisfies the wheel conditions (5.5) is equivalent to (5.42), as we have already seen, which is in turn equivalent to (5.33).

Thus, we have constructed $R \in \mathcal{A}_{\mathbf{k},d}$ such that (5.37) holds, as needed. □

5.24. We conclude the present Section with a proof of Theorem 1.7.

Proof of Theorem 1.7. According to Proposition 5.7, the map $\Upsilon \colon U_q(L\mathfrak{n}^+) \to \mathcal{A}^+$ is injective, hence it remains to prove that it is also surjective. To this end, recall the filtration (4.67), and consider the following vector subspaces for any loop word w:

$$\mathcal{A}^+_{\le w} \subset \mathcal{A}^+$$

consisting of rational functions R such that the leading order term of $\iota(R)$ is $\le w$. It is clear, due to (5.29), that the map Υ restricts to an injection:

$$U_q(L\mathfrak{n}^+)_{\le w} \stackrel{\Upsilon}{\hookrightarrow} \mathcal{A}^+_{\le w} \tag{5.50}$$

Recall the vector subspace (4.66) and consider the restriction of the pairing (5.20):

$$\mathcal{A}^+_{\le w} \otimes U_q(L\mathfrak{n}^-)^{\le w} \longrightarrow \mathbb{Q}(q) \tag{5.51}$$

With Proposition 5.17 in mind, we claim that the pairing (5.51) is non-degenerate in the first argument, cf. Proposition 4.39. This claim holds because elements:

$$R \in \mathcal{A}^+_{\le w}$$

pair trivially with the basis elements $\{{}_v f\}_{v > w}$ of (4.69), due to (5.25), and hence also with $\{f_v\}_{v > w}$ of (4.42), due to (4.71). The non-degeneracy of (5.51) implies that:

$$\dim \mathcal{A}^+_{\leq w} \leq \dim U_q(L\mathfrak{n}^-)^{\leq w} = \#\Big\{\text{standard loop words } \leq w\Big\} \tag{5.52}$$

(although the dimensions above are technically speaking infinite, they become finite when we restrict to each $Q^+ \times \mathbb{Z}$-graded component, see Corollary 2.32). However, the domain of the map (5.50) has dimension equal to the number of standard loop words $\leq w$, see Subsection 4.40, which together with (5.52) implies that the map (5.50) is an isomorphism. As $\mathcal{A}^+ = \cup_w \mathcal{A}^+_{\leq w}$, the surjectivity of Υ follows. □

References

[1] I.E. Angiono, A presentation by generators and relations of Nichols algebras of diagonal type and convex orders on root systems, J. Eur. Math. Soc. 17 (10) (2015) 2643–2671.

[2] J. Beck, Convex bases of PBW type for quantum affine algebras, Commun. Math. Phys. 165 (1) (1994) 193–199.

[3] J. Beck, Braid group action and quantum affine algebras, Commun. Math. Phys. 165 (3) (1994) 555–568.

[4] S. Clark, D. Hill, W. Wang, Quantum shuffles and quantum supergroups of basic type, Quantum Topol. 7 (3) (2016) 553–638.

[5] I. Damiani, A basis of type Poincare-Birkhoff-Witt for the quantum algebra of $\widehat{\mathrm{sl}}(2)$, J. Algebra 161 (2) (1993) 291–310.

[6] I. Damiani, Drinfeld realization of affine quantum algebras: the relations, Publ. Res. Inst. Math. Sci. 48 (3) (2012) 661–733.

[7] J. Ding, N. Jing, On a combinatorial identity, Int. Math. Res. Not. (6) (2000) 325–332.

[8] V. Drinfeld, A new realization of Yangians and of quantum affine algebras, preprint, 1986, FTINT 30–86.

[9] B. Enriquez, On correlation functions of Drinfeld currents and shuffle algebras, Transform. Groups 5 (2) (2000) 111–120.

[10] B. Enriquez, PBW and duality theorems for quantum groups and quantum current algebras, J. Lie Theory 13 (1) (2003) 21–64.

[11] B. Enriquez, S. Khoroshkin, S. Pakuliak, Weight functions and Drinfeld currents, Commun. Math. Phys. 276 (3) (2007) 691–725.

[12] B. Feigin, Integrable systems, shuffle algebras, and Bethe equations, Trans. Mosc. Math. Soc. (2016) 203–246.

[13] B. Feigin, A. Odesskii, Quantized moduli spaces of the bundles on the elliptic curve and their applications, in: Integrable Structures of Exactly Solvable Two-Dimensional Models of Quantum Field Theory, Kiev, 2000, in: NATO Sci. Ser. II Math. Phys. Chem., vol. 35, Kluwer Acad. Publ., Dordrecht, 2001, pp. 123–137.

[14] F. Gavarini, A PBW basis for Lusztig's form of untwisted affine quantum groups, Commun. Algebra 27 (2) (1999) 903–918.

[15] J. Green, Quantum groups, Hall algebras and quantized shuffles, in: Finite Reductive Groups (Luminy 1994), in: Prog. Math., vol. 141, Birkhäuser, 1997, pp. 273–290.

[16] I. Grojnowski, Affinizing quantum algebras: from D-modules to K-theory, preprint, https://www.dpmms.cam.ac.uk/~groj/char.ps, 1994.

[17] P. Grosse, On quantum shuffle and quantum affine algebras, J. Algebra 318 (2) (2007) 495–519.

[18] D. Hernandez, Representations of quantum affinizations and fusion product, Transform. Groups 10 (2) (2005) 163–200.

[19] N. Hu, M. Rosso, H. Zhang, Two-parameter quantum affine algebra $U_{r,s}(\widehat{\mathfrak{sl}_n})$, Drinfel'd realization and quantum affine Lyndon basis, Commun. Math. Phys. 278 (2) (2008) 453–486.

[20] J. Humphreys, Introduction to Lie Algebras and Representation Theory, Graduate Texts in Mathematics, vol. 9, Springer-Verlag, New York, ISBN 978-0-387-90052-0, 1972.

[21] J. Jantzen, Lectures on Quantum Groups, Graduate Studies in Mathematics, American Mathematical Society, Providence, RI, 1996.

[22] V. Kac, Infinite-Dimensional Lie Algebras, 3d edition, Cambridge University Press, Cambridge, 1990.

[23] S. Khoroshkin, V. Tolstoy, The universal R-matrix for quantum untwisted affine Lie algebras, Funct. Anal. Appl. 26 (1) (1992) 69–71.
[24] A. Kirillov, N. Reshetikhin, q-Weyl group and a multiplicative formula for universal R-matrices, Commun. Math. Phys. 134 (2) (1990) 421–431.
[25] A. Kleshchev, A. Ram, Representations of Khovanov-Lauda-Rouquier algebras and combinatorics of Lyndon words, Math. Ann. 349 (4) (2011) 943–975.
[26] P. Lalonde, R.A. Standard, Lyndon bases of Lie algebras and enveloping algebras, Trans. Am. Math. Soc. 347 (5) (1995) 1821–1830.
[27] B. Leclerc, Dual canonical bases, quantum shuffles and q-characters, Math. Z. 246 (4) (2004) 691–732.
[28] S. Levendorsky, S. Ya, Some applications of the quantum Weyl groups, J. Geom. Phys. 7 (2) (1990) 241–254.
[29] S. Levendorsky, Ya. Soibelman, V. Stukopin, The quantum Weyl group and the universal quantum R-matrix for affine Lie algebra $A_1^{(1)}$, Lett. Math. Phys. 27 (4) (1993) 253–264.
[30] G. Lusztig, Introduction to Quantum Groups, Birkhäuser, Boston, 1993.
[31] G. Melançon, Combinatorics of Hall trees and Hall words, J. Comb. Theory, Ser. A 59 (2) (1992) 285–308.
[32] A. Neguț, The shuffle algebra revisited, Int. Math. Res. Not. (22) (2014) 6242–6275.
[33] A. Neguț, Quantum toroidal and shuffle algebras, Adv. Math. 372 (2020) 107288, 60 pp.
[34] P. Papi, A characterization of a special ordering in a root system, Proc. Am. Math. Soc. 120 (3) (1994) 661–665.
[35] P. Papi, Convex orderings in affine root systems, J. Algebra 172 (3) (1995) 613–623.
[36] P. Papi, Convex orderings in affine root systems, II, J. Algebra 186 (1) (1996) 72–91.
[37] M. Rosso, An analogue of P.B.W. theorem and the universal R-matrix for $U_h\mathfrak{sl}(N+1)$, Commun. Math. Phys. 124 (2) (1989) 307–318.
[38] M. Rosso, Quantum groups and quantum shuffles, Invent. Math. 133 (2) (1998) 399–416.
[39] M. Rosso, Lyndon bases and the multiplicative formula for R-matrices, unpublished.
[40] P. Schauenburg, A characterization of the Borel-like subalgebras of quantum enveloping algebras, Commun. Algebra 24 (9) (1996) 2811–2823.
[41] O. Schiffmann, E. Vasserot, Hall algebras of curves, commuting varieties and Langlands duality, Math. Ann. 353 (4) (2012) 1399–1451.
[42] A. Tsymbaliuk, Shuffle algebra realizations of type A super Yangians and quantum affine superalgebras for all Cartan data, Lett. Math. Phys. 110 (8) (2020) 2083–2111.
[43] M. Varagnolo, E. Vasserot, K-theoretic Hall algebras, quantum groups and super quantum groups, Selecta Math. (N.S.) 28 (2022) 7, 56 pp.