STRUCTURE THEOREMS OF MIXABLE SHUFFLE ALGEBRAS AND FREE COMMUTATIVE ROTA-BAXTER ALGEBRAS

LI GUO AND BINGYONG XIE

ABSTRACT. We study the ring theoretical structures of mixable shuffle algebras and their associated free commutative Rota-Baxter algebras. For this study we utilize the connection of the mixable shuffle algebras with the overlapping shuffle algebra of Hazewinkel, quasi-shuffle algebras of Hoffman and quasi-symmetric functions. This connection allows us to apply methods and results on shuffle products and Lyndon words on ordered sets. As a result, we obtain structure theorems for a large class of mixable shuffle algebras and free commutative Rota-Baxter algebras with various coefficient rings.

1. Introduction

In this paper, all rings and algebras are assumed to be unitary unless otherwise specified. Let $\mathbf{k}$ denote a commutative ring. By an algebra we mean a $\mathbf{k}$-algebra and by a tensor product we mean the tensor product over $\mathbf{k}$.

1.1. **Rota-Baxter algebras and mixable shuffle algebras.** Given a commutative ring $\mathbf{k}$ and a $\lambda \in \mathbf{k}$, a **Rota-Baxter algebra of weight** λ is an associative $\mathbf{k}$-algebra R together with a $\mathbf{k}$-linear operator P on R such that

$$P(x)P(y) = P(xP(y)) + P(P(x)y) + \lambda P(xy), \forall x, y \in R. \tag{1}$$

Such an operator is called a **Rota-Baxter operator** (of weight λ). This operator is an abstraction of the integration operator $P(f)(x) := \int_0^x f(t)\,dt$ where the above identity is simply the integration by parts formula. This operator also include as special cases numerous other operators in mathematics and physics, such as the summation operator of functions, partial sum operator for sequences and projection operator on Laurent series, as well as the operator on distributions in the paper [4] where G. Baxter first defined this operator. Such broad connections lead to many applications of Rota-Baxter algebras [1, 2, 3, 6, 8, 11, 12, 18, 19, 25, 39] which further motivate the theoretical study of Rota-Baxter algebras. See the introductory and survey articles [10, 16, 17, 39] for further details.

As a first step in their theoretical study, free commutative Rota-Baxter algebras were constructed by Cartier and Rota [5, 38] with certain restrictions. A general construction was obtained by one of the authors and Keigher [20, 21] in terms of mixable shuffle products. For a commutative $\mathbf{k}$-algebra A, let $\text{Ш}_{\mathbf{k},\lambda}(A)$ be the free commutative Rota-Baxter algebra of weight λ generated by A. It is shown in [20] that

$$\text{Ш}_{\mathbf{k},\lambda}(A) = A \otimes \mathrm{MS}_{\mathbf{k},\lambda}(A) \tag{2}$$

where $\mathrm{MS}_{\mathbf{k},\lambda}(A)$ (denoted by $\text{Ш}^+_{\mathbf{k},\lambda}(A)$ in [20, 21]) is **the mixable shuffle algebra of weight** λ generated by A. The precise definitions will be recalled in Section 2.1. Thus the study of free commutative Rota-Baxter algebras is reduced to the study of mixable shuffle algebras.

1.2. **Overlapping shuffle algebra and quasi-symmetric functions.** During the same period of time when mixable shuffle product was constructed, Hazewinkel [27, 28] defined the overlapping shuffle algebra and showed that it gives another description of the algebra of quasi-symmetric functions. He then used the language and methods on Lyndon words of shuffles algebras to extend the well-known theorem of Radford [36] that the shuffle algebra with rational coefficients is a polynomial algebra generated by the set of Lyndon words to the algebra of quasi-symmetric functions with rational coefficients. More generally, Hoffman [31] showed that his quasi-shuffle algebras, also introduced during the same period of time, are polynomial algebras on Lyndon words when rational coefficients are considered.

The theory of these algebras with integer coefficients developed more slowly. As commented in [28, 29], Ditters announced in his 1972 paper [7] that the algebra of quasi-symmetric functions with integer coefficients is a polynomial algebra. But there was a gap in his proof, as well as in the quite a few subsequent efforts to prove the statement. Eventually, Hazewinkel was able to provide a correct proof (Theorem 2.2.(c)). So we will call this statement the **Ditters Conjecture** or the **Ditters-Hazewinkel Theorem**.

1.3. **Mixable shuffles and overlapping shuffles.** As we will see later in Section 2.2, the overlapping shuffle algebra, generalized overlapping shuffle algebras and quasi-shuffle algebras are all special cases of mixable shuffle algebras. In this paper we extend the results and methods for these special cases, especially from [28], to study more general mixable shuffle algebras with various coefficient rings. We then study the ring theoretical structure of free commutative Rota-Baxter algebras through the tensor decomposition in Eq. (2). This paper can be regarded as a continuation of our earlier studies [9, 15, 20, 21] on this subject.

In analogy to the cases of the overlapping shuffle algebra and quasi-symmetric functions, the structure of a mixable shuffle algebra depends on its base ring $\mathbf{k}$, as well as its weight λ, especially for those mixable shuffle algebras that appear in the construction of free commutative Rota-Baxter algebras. So we will consider mixable shuffle algebras and Rota-Baxter algebras in these separate cases. For notational simplicity, we will take the base ring $\mathbf{k}$ to be $\mathbb{Q}$, $\mathbb{F}_p$, $\mathbb{Z}_p$ or $\mathbb{Z}$. See Table 1 for a summary of previous and new results.

When $\mathbf{k} = \mathbb{Q}$, Radford's theorem and its generalizations by Hazewinkel [28] and Hoffman [31] can be quite easily generalized further to mixable shuffle algebras (Theorem 2.3) and then to free commutative Rota-Baxter algebras (Theorem 2.4). This is presented in Section 2 after preliminary notations and results.

The situation is already quite different in the case of $\mathbf{k} = \mathbb{F}_p$ which is considered in Section 3. By a careful study of the Lyndon words, we obtain the structure theorem (Theorem 3.17) for a quite large class of mixable shuffle algebras. This leads to the structure theorem of a quite large class of free commutative Rota-Baxter algebras (Theorem 3.20), including those generated by a finite set.

In Section 4, we lift the results in Section 3 from $\mathbb{F}_p$ to $\mathbb{Z}_p$ by studying the reduction map $\mathbb{Z}_p \to \mathbb{F}_p$. As is often the case in this lifting process, we can only recover part of the information and obtain a less precise structure theorem on the mixable shuffle algebras with $\mathbb{Z}_p$-coefficients (Theorem 4.5), which translates to a less precise structure theorem on the free commutative Rota-Baxter algebras with $\mathbb{Z}_p$-coefficients (Theorem 4.6). Nevertheless, in the case that we are most interested in and includes the overlapping shuffle algebra, we

show that the mixable shuffle algebra is a polynomial algebra generated by an explicitly defined set.

In the final Section 5, we give a local-global principle extracted from Hazewinkel's elegant proof of the Ditters-Hazewinkel Theorem [28] mentioned above. This principle allows us to "glue" together our local results over $\mathbb{Q}$ and $\mathbb{Z}_p$, for all p, to obtain results over $\mathbb{Z}$. As a result, we generalize the Ditters-Hazewinkel Theorem from the mixable shuffle algebra on free abelian semigroup with one generator to those with countably many generators (Theorem 5.4). We obtain a similar polynomial algebra in free commutative Rota-Baxter algebra generated by a set (Theorem 5.6).

The theoretical study in this paper should have some interesting applications. For example, the nested sum definition of multiple zeta values leads to their encoding in the quasi-shuffle (stuffle) algebra which is a mixable shuffle algebra of weight 1. In the same way, the restricted multiple zeta values [30] (also called star multiple zeta values [34]) can be encoded by a mixable shuffle algebra of weight -1 considered here. As another example, the study of multiple zeta values has benefited from the polynomial algebra structure on shuffle algebras with rational coefficients [33, 35]. Likewise, our study of the polynomial algebra structure on mixable shuffle algebras with coefficients in $\mathbb{F}_p$, $\mathbb{Z}_p$ and $\mathbb{Z}$ might be applied to study the congruence, p-adic and integral properties of the relations among multiple zeta values. This direction is being pursued in [24].

Acknowledgements: Both authors thank the Max Planck Institute for Mathematics at Bonn where this research was carried out. The first author acknowledges support from NSF grant DMS-0505643.

2. Structure theorems on $\mathbb{Q}$

In this section we first review the construction of free commutative Rota-Baxter algebras in terms of mixable shuffle algebras obtained in [20, 21]. We then relate mixable shuffle algebras to the overlapping shuffle algebra and generalized overlapping shuffle algebras of Hazewinkel [28, 29], and quasi-shuffle algebras of Hoffman [31]. This connection allows us to extend the study of overlapping shuffle algebra and quasi-shuffle algebras to the study the structure of mixable shuffle algebras and free commutative Rota-Baxter algebras with base ring $\mathbb{Q}$. This connection will also be used in later sections for other base rings.

2.1. **Mixable shuffle algebras and free commutative Rota-Baxter algebras.** We briefly recall the construction of mixable shuffle algebras and free commutative Rota-Baxter algebras [20, 21].

Let A be a commutative $\mathbf{k}$-algebra *that is not necessarily unitary.* For a given $\lambda \in \mathbf{k}$, the **mixable shuffle algebra of weight λ generated by** A (with coefficients in $\mathbf{k}$) is the $\mathbf{k}$-module

$$\mathrm{MS}(A) := \mathrm{MS}_{\mathbf{k},\lambda}(A) = \bigoplus_{k\geq 0} A^{\otimes k} = \mathbf{k} \oplus A \oplus A^{\otimes 2} \oplus \cdots \tag{3}$$

equipped with the **mixable shuffle product $\diamond_\lambda$ of weight λ** defined as follows.

For pure tensors $\mathfrak{a} = a_1 \otimes \ldots \otimes a_m \in A^{\otimes m}$ and $\mathfrak{b} = b_1 \otimes \ldots \otimes b_n \in A^{\otimes n}$, a **shuffle** of $\mathfrak{a}$ and $\mathfrak{b}$ is a tensor list of a_i and b_j without change the natural orders of the a_is and the b_js.

More generally, for the fixed $\lambda \in \mathbf{k}$, a **mixable shuffle** (of weight λ) of $\mathfrak{a}$ and $\mathfrak{b}$ is a shuffle of $\mathfrak{a}$ and $\mathfrak{b}$ in which some (or *none*) of the pairs $a_i \otimes b_j$ are merged into $\lambda\, a_i b_j$. Then define

$$\mathfrak{a} \diamond \mathfrak{b} = \mathfrak{a} \diamond_\lambda \mathfrak{b} = \sum \text{ mixable shuffles of } \mathfrak{a} \text{ and } \mathfrak{b} \tag{4}$$

where the subscript λ is often suppressed when there is no danger of confusion. For example,

$$\begin{aligned} a_1 \diamond (b_1 \otimes b_2) : &= a_1 \diamond_\lambda (b_1 \otimes b_2) \\ &= \underbrace{a_1 \otimes b_1 \otimes b_2 + b_1 \otimes a_1 \otimes b_2 + b_1 \otimes b_2 \otimes a_1}_{\text{shuffles}} + \underbrace{\lambda(a_1 b_1) \otimes b_2 + \lambda b_1 \otimes (a_1 b_2)}_{\text{merged shuffles}}. \end{aligned}$$

With $\mathbf{1} \in \mathbf{k}$ as the unit, this product makes $\mathrm{MS}_{\mathbf{k},\lambda}(A)$ into a commutative $\mathbf{k}$-algebra. See [20] for further details of the mixable shuffle product. When $\lambda = 0$, we simply have the shuffle product which is also defined when A is only a $\mathbf{k}$-module, treated as an algebra with zero multiplication.

The product $\diamond_\lambda$ can also be defined by the following recursion [9, 26] which gives the connection with quasi-shuffle algebras of Hoffman [31]. First define the multiplication by $A^{\otimes 0} = \mathbf{k}$ to be the scalar product. In particular, $\mathbf{1}$ is the identity. For any $m, n \geqslant 1$ and $\mathfrak{a} := a_1 \otimes \cdots \otimes a_m \in A^{\otimes m}$, $\mathfrak{b} := b_1 \otimes \cdots \otimes b_n \in A^{\otimes n}$, define $a \diamond_\lambda b$ by induction on the sum $m + n$. Then $m + n \geqslant 2$. When $m + n = 2$, we have $a = a_1$ and $b = b_1$. Define

$$a \diamond_\lambda b = a_1 \otimes b_1 + b_1 \otimes a_1 + \lambda a_1 b_1. \tag{5}$$

Assume that $\mathfrak{a} \diamond_\lambda \mathfrak{b}$ has been defined for $m + n \geqslant k \geqslant 2$ and consider $\mathfrak{a}$ and $\mathfrak{b}$ with $m + n = k + 1$. Then $m + n \geqslant 3$ and so at least one of m and n is greater than 1. Then we define

$$\mathfrak{a} \diamond_\lambda \mathfrak{b} = \begin{cases} a_1 \otimes b_1 \otimes \cdots \otimes b_n + b_1 \otimes \big(a_1 \diamond_\lambda (b_2 \otimes \cdots \otimes b_n)\big) \\ \qquad + \lambda(a_1 b_1) \otimes b_2 \otimes \cdots \otimes b_n, \text{ when } m = 1, n \geqslant 2, \\ a_1 \otimes \big((a_2 \otimes \cdots \otimes a_m) \diamond_\lambda b_1\big) + b_1 \otimes a_1 \otimes \cdots \otimes a_m \\ \qquad + \lambda(a_1 b_1) \otimes a_2 \otimes \cdots \otimes a_m, \text{ when } m \geqslant 2, n = 1, \\ a_1 \otimes \big((a_2 \otimes \cdots \otimes a_m) \diamond_\lambda (b_1 \otimes \cdots \otimes b_n)\big) + b_1 \otimes \big((a_1 \otimes \cdots \otimes a_m) \diamond_\lambda (b_2 \otimes \cdots \otimes b_n)\big) \\ \qquad + \lambda(a_1 b_1)\big((a_2 \otimes \cdots \otimes a_m) \diamond_\lambda (b_2 \otimes \cdots \otimes b_n)\big), \text{ when } m, n \geqslant 2. \end{cases}$$

Here the products by $\diamond_\lambda$ on the right hand side of the equation are well-defined by the induction hypothesis.

Now let A be a (unitary) $\mathbf{k}$-algebra. We define the tensor product algebra

$$Ш(A) := Ш_{\mathbf{k},\lambda}(A) = A \otimes \mathrm{MS}_{\mathbf{k},\lambda}(A) = A \oplus A^{\otimes 2} \oplus \cdots. \tag{6}$$

Define a $\mathbf{k}$-linear operator P_A on $Ш(A)$ by assigning

$$P_A(x_0 \otimes x_1 \otimes \cdots \otimes x_n) = \mathbf{1}_A \otimes x_0 \otimes x_1 \otimes \cdots \otimes x_n,$$

for all $x_0 \otimes x_1 \otimes \cdots \otimes x_n \in A^{\otimes (n+1)}$ and extending by additivity. Let $j_A : A \to Ш(A)$ be the canonical inclusion map.

Theorem 2.1. [20]

(a) *The pair $(Ш(A), P_A)$, together with the natural embedding $j_A : A \to Ш(A)$, is a free commutative Rota-Baxter $\mathbf{k}$-algebra of weight λ on A. In other words, for any Rota-Baxter $\mathbf{k}$-algebra (R, P) and any $\mathbf{k}$-algebra homomorphism $\varphi : A \to R$, there exists a unique Rota-Baxter $\mathbf{k}$-algebra homomorphism $\tilde{\varphi} : (Ш(A), P_A) \to (R, P)$ such that $\varphi = \tilde{\varphi} \circ j_A$ as $\mathbf{k}$-algebra homomorphisms.*

(b) *When X is a set. The pair $(Ш(\mathbf{k}[X]), P_{\mathbf{k}[X]})$, together with the natural embedding $j_X : X \to \mathbf{k}[X] \to Ш(\mathbf{k}[X])$, is a free commutative Rota-Baxter $\mathbf{k}$-algebra on the set X of weight λ.*

2.2. **Mixable shuffles, overlapping shuffles and quasi-shuffles.** Let S be a semigroup and let $\mathbf{k}\,S = \sum_{s\in S} \mathbf{k}\,s$ be the semigroup nonunitary $\mathbf{k}$-algebra. Then a canonical $\mathbf{k}$-basis of $(\mathbf{k}\,S)^{\otimes k}, k \geqslant 0$, is the set $S^{\otimes k} := \{s_1 \otimes \cdots \otimes s_k \mid s_i \in S, 1 \leqslant i \leqslant k\}$. Thus a canonical $\mathbf{k}$-basis of $\mathrm{MS}_{\mathbf{k},\lambda}(A)$ is

$$M^{\otimes}(S) := \{1\} \cup \{u_1 \otimes \cdots \otimes u_r \mid u_i \in S, 1 \leqslant i \leqslant r, r \geqslant 1\}. \tag{7}$$

With the tensor concatenation, $M^{\otimes}(S)$ is simply the free monoid generated by S. We use the tensor concatenation instead of the usual concatenation for the product since we need to use the concatenation to denote the product in S when S is a semigroup. Elements in $M^{\otimes}(S)$ are still called **words** from the set S. Then we have

$$\mathrm{MS}_{\mathbf{k},\lambda}(S) := \mathrm{MS}_{\mathbf{k},\lambda}(\mathbf{k}S) = \mathbf{k}\,M^{\otimes}(S).$$

We denote $\mathrm{MS}_{\mathbf{k},\lambda}(S)$ for $\mathrm{MS}_{\mathbf{k},\lambda}(\mathbf{k}\,S)$ to make clear the connection with S and to simplify the notation.

Let S be a monoid and let $\mathbf{k}\,S$ be the (unitary) $\mathbf{k}$-algebra. As in Eq. (2) we have the free commutative Rota-Baxter algebra

$$Ш_{\mathbf{k},\lambda}(\mathbf{k}S) = (\mathbf{k}S) \otimes \mathrm{MS}_{\mathbf{k},\lambda}(S). \tag{8}$$

It is in fact the free commutative Rota-Baxter algebra generated by the monoid S in the sense that it comes from the left adjoint functor of the forgetful functor from the category of commutative Rota-Baxter algebras to the category of commutative multiplicative monoids.

Now let S be the multiplicative semigroup $\{x^i\}_{i\geqslant 1}$. Then

$$M^{\otimes}(S) = \{x^{a_1} \otimes \cdots \otimes x^{a_k} \mid a_j \geqslant 1, 1 \leqslant j \leqslant k, k \geqslant 0\}.$$

It is in bijection with the set of vectors

$$\{[a_1, \cdots, a_k] \mid a_j \geqslant 1, 1 \leqslant j \leqslant k, k \geqslant 0\}$$

and with the set of polynomials

$$\left\{ \sum_{1\leqslant i_1<\cdots<i_n} X_{i_1}^{a_1} \cdots X_{i_k}^{a_k} \mid a_j \geqslant 1, 1 \leqslant j \leqslant k, k \geqslant 0 \right\} \subseteq \mathbf{k}[X_i, i \geqslant 1].$$

Through the first bijection, we obtain the isomorphism of $\mathrm{MS}_{\mathbf{k},1}(S)$ with the **overlapping shuffle algebra**

$$\mathbf{k}\{[a_1, \cdots, a_k] \mid a_j \geqslant 1, 1 \leqslant j \leqslant k, k \geqslant 0\}$$

defined by Hazewinkel [27]. See [27] for more details and a more precise definition of the product in terms of order preserving injective maps (see also [5] and [13]). Through the second bijection, we obtain the isomorphism of $\mathrm{MS}_{\mathbf{k},1}(S)$ with the algebra $QSym_{\mathbf{k}}(S)$ of quasi-symmetric functions [14].

Let S be a graded semigroup $S = \coprod_{i\geqslant 0} S_i$, $S_iS_j \subseteq S_{i+j}$ such that $|S_i| < \infty$, $i \geqslant 0$. Then with $\lambda = 1$, the mixable shuffle algebra $\mathrm{MS}_{\lambda}(S)$ is isomorphic to the **quasi-shuffle algebra** defined by Hoffman [31, 9, 26].

For a general semigroup S, the mixable shuffle algebra $\mathrm{MS}_{\mathbf{k},1}(S)$ of weight 1 coincides with the **generalized overlapping shuffle algebra** on S [29].

TABLE 1. Structure of $\mathrm{MS}_{\mathbf{k},\lambda}(S)$

	base ring $\mathbf{k}$	weight λ	ordered set or semigroup S	reference
Radford [36]	$\mathbb{Q}$	0	ordered set	Theorem 2.2.(a)
Hoffman [31]	$\mathbb{Q}$	1	ordered abelian semigroups	Theorem 2.2.(b)
Hazewinkel [28]	$\mathbb{Q}, \mathbb{Z}_p, \mathbb{Z}$	1	$\mathbb{Z}_{>0}$	Theorem 2.2.(b) & (c)
This paper	$\mathbb{Q}$	$\neq 0$	ordered abelian semigroups	Theorem 2.3
	$\mathbb{F}_p$	0	ordered set	Theorem 3.7
	$\mathbb{F}_p$	$\neq 0$	$S \in \mathcal{P}, \mathcal{J}$	Theorem 3.17
	$\mathbb{Z}_p$	p-unit	$S \in \mathcal{F}, \mathcal{J}$	Theorem 4.5
	$\mathbb{Z}$	± 1	$S \cong \mathbb{Z}_{>0}^n$ or $\mathbb{Z}_{>0}^{(\infty)}$	Theorem 5.3 & 5.4

Let $(S, <)$ be an ordered set. Extend the order on S to the **lexicographic order** $<_{\mathrm{lex}}$ on $M^{\otimes}(S)$. Thus, for $u, v \in M^{\otimes}(S)$, $u <_{\mathrm{lex}} v$ if and only if either $v = u \otimes x$ for some non-empty word x, or $u = x \otimes a \otimes u', v = x \otimes b \otimes v'$ for some words x, u', v' and some letter a, b with $a < b$. Recall that a **Lyndon word** in $M^{\otimes}(S)$ is a non-empty word w such that if $w = u \otimes v$ with $u, v \neq 1$, then $w <_{\mathrm{lex}} v$. Let $\mathrm{Lyn} = \mathrm{Lyn}(S)$ be the set of Lyndon words in $M^{\otimes}(S)$.

The following theorem summarizes what is known about when a mixable shuffle algebra is a polynomial algebra.

Theorem 2.2. (a) **(**[36][37, Theorem 6.1]**)** *Let S be an ordered set. Then $\mathrm{MS}_{\mathbb{Q},0}(S)$, namely the shuffle algebra $Sh(S)$ on S with coefficients in $\mathbb{Q}$, is isomorphic to $\mathbb{Q}[\mathrm{Lyn}(S)]$.*

(b) **(Hazewinkel-Hoffman Theorem** [28]**,**[31, Theorem 2.6.]**)** *Let S be an ordered abelian semigroup. Then $\mathrm{MS}_{\mathbb{Q},1}(S)$, namely the quasi-shuffle algebra on S with coefficients in $\mathbb{Q}$, is isomorphic to $\mathbb{Q}[\mathrm{Lyn}(S)]$.*

(c) **(Ditters-Hazewinkel Theorem** [7, 28]**)** *Let S be the free abelian semigroup with one generator. Then $\mathrm{MS}_{\mathbb{Z},1}(S)$, namely the $\mathbb{Z}$-algebra of overlapping shuffles, and the algebra quasi-symmetric functions with integer coefficients, is a polynomial algebra.*

Thus quite much is known about the mixable shuffle algebras with coefficients in $\mathbb{Q}$ and with weight 0 or 1, but little is known in the other cases. One of our main goals in this paper is to extend this theorem to the cases for other coefficient rings and other weights, as summarized in Table 1.

We first consider the easy case when $\mathbf{k} = \mathbb{Q}$ and $\lambda \in \mathbb{Q}$ is arbitrary.

Theorem 2.3. *Let S be an ordered abelian semigroup and let λ be in $\mathbb{Q}$. Then $\mathrm{MS}_{\mathbb{Q},\lambda}(S)$ is isomorphic to $\mathbb{Q}[\mathrm{Lyn}(S)]$.*

Proof. Fix a $\lambda \in \mathbb{Q}$. If $\lambda = 0$, then by definition, $\mathrm{MS}_{\mathbb{Q},\lambda}(S)$ is the shuffle algebra $Sh(S)$ on the $\mathbb{Q}$-vector space $\mathbb{Q}S$. By Theorem 2.2.(a), we have $\mathrm{MS}_{\mathbb{Q},0}(S) = \mathbb{Q}[\mathrm{Lyn}]$. If $\lambda = 1$, then as was shown in [9] and [26], $\mathrm{MS}_{\mathbb{Q},1}(S)$ is the quasi-shuffle $\mathbb{Q}$-algebra on the semigroup S and thus is $\mathbb{Q}[\mathrm{Lyn}(S)]$ by Theorem 2.2.(b).

If $\lambda \neq 0, 1$, the algebra isomorphism

$$\begin{aligned} f :& \text{ш}_{\mathbb{Q},\lambda}(\mathbb{Q}S) \to \text{ш}_{\mathbb{Q},1}(\mathbb{Q}S), \\ & a_0 \otimes \cdots \otimes a_n \mapsto \lambda^n (a_0 \otimes \cdots \otimes a_n), \forall a_0 \otimes \cdots \otimes a_n \in \mathbb{Q}S^{\otimes(n+1)} \end{aligned}$$

from [9] (Lemma 2.8 and the comments afterward) restricts to an algebra isomorphism

$$\begin{aligned} f :& \mathrm{MS}_{\mathbb{Q},\lambda}(\mathbb{Q}S) \to \mathrm{MS}_{\mathbb{Q},1}(\mathbb{Q}S), \\ & a_1 \otimes \cdots \otimes a_n \mapsto \lambda^n (a_1 \otimes \cdots \otimes a_n), \forall a_1 \otimes \cdots \otimes a_n \in \mathbb{Q}S^{\otimes n}. \end{aligned}$$

Thus a Lyndon word $\omega \in \mathrm{MS}_{\mathbb{Q},1}(S)$ is sent to $\lambda^{\ell(\omega)}\omega \in \mathrm{MS}_{\mathbb{Q},\lambda}(S)$ where $\ell(\omega)$ is the length of the word ω. Since $\lambda \in \mathbb{Q}$ is invertible, $\mathrm{MS}_{\mathbb{Q},\lambda}(S)$ is still generated by $\mathrm{Lyn}(S)$. Thus the theorem holds for all $\lambda \in \mathbb{Q}$. □

2.3. **Free commutative Rota-Baxter algebras over a $\mathbb{Q}$-algebra.** We now apply Theorem 2.3 to free commutative Rota-Baxter algebras.

Theorem 2.4. *Let S be an ordered abelian monoid and let $\mathbb{Q}S$ be the monoid algebra. Then*

$$\text{ш}_{\mathbb{Q},\lambda}(\mathbb{Q}S) = \mathbb{Q}S \otimes \mathbb{Q}[\mathrm{Lyn}(S)], \tag{9}$$

where $\mathrm{Lyn}(S)$ is the set of Lyndon words on S. In particular, let X be an ordered set. Let $M^{\mathrm{c}}(X)$ be the free abelian monoid generated by X. Then

$$\text{ш}_{\mathbb{Q},\lambda}(\mathbb{Q}[X]) = \mathbb{Q}[\overline{\mathrm{Lyn}}(M^{\mathrm{c}}(X))], \tag{10}$$

where

$$\overline{\mathrm{Lyn}}(M^{\mathrm{c}}(X)) := X \cup \{1 \otimes w \mid w \in \mathrm{Lyn}(M^{\mathrm{c}}(X))\}.$$

Proof. By Theorem 2.3 and Eq. (8), we have $\text{ш}_{\mathbb{Q},\lambda}(\mathbb{Q}S) = \mathbb{Q}S \otimes \mathbb{Q}[\mathrm{Lyn}]$ by Eq. (2).

For the second statement, let X be an ordered set. Then $\mathbb{Q}[X] = \mathbb{Q}M^{\mathrm{c}}(X)$ and

$$\text{ш}_{\mathbb{Q},\lambda}(\mathbb{Q}[X]) = \mathbb{Q}[X] \otimes \mathrm{MS}_{\mathbb{Q},\lambda}(M^{\mathrm{c}}(X)) = \mathbb{Q}[X] \otimes \mathbb{Q}[\mathrm{Lyn}(M^{\mathrm{c}}(X))] = \mathbb{Q}[\overline{\mathrm{Lyn}}(M^{\mathrm{c}}(X))].$$

□

3. Structure theorems on $\mathbb{F}_p$

Given a prime number p, we now consider the algebra structure of the mixable shuffle algebras $\mathrm{MS}_{\mathbb{F}_p,\lambda}(S)$ where S is an ordered semigroup with base ring $\mathbb{F}_p$. Here the situation is quite different from the case when the base ring is $\mathbb{Q}$. As an easy illustration, let $x \in S$, then the shuffle product $x^{\text{ш}p} = x^{\diamond_{\mathrm{o}}p} = p!x^{\otimes p} = 0$ in $\mathrm{MS}_{\mathbb{F}_p,0}(X)$. We will show that this phenomenon prevails when the weight λ is zero and, as a result, $\mathrm{MS}_{\mathbb{F}_p,0}(S)$ has no polynomial subalgebras. When $\lambda \neq 0$, the structure of $\mathrm{MS}_{\mathbb{F}_p,\lambda}(S)$ is more diversified. For a large class

of abelian semigroups S, including free semigroups, free monoids, p-nilpotent groups and p-idempotent groups, we determine the factorization of $\mathrm{MS}_{\mathbb{F}_p,\lambda}(S)$ into a polynomial part and a non-polynomial part. We then apply these structure theorems to the free commutative Rota-Baxter algebras $\text{Ш}_{\mathbb{F}_p,\lambda}(\mathbb{F}_pS)$ with coefficients in $\mathbb{F}_p$.

3.1. **Notations and preparatories.** Let $(S,<)$ be an ordered set and let the free monoid $M^{\otimes}(S)$ be as defined in Eq. (7). Recall that we use $<_{\mathrm{lex}}$ to denote the lexicographic order on $M^{\otimes}(S)$ induced from the order on S. We will use another order $<_{\mathrm{leng}}$ on $M^{\otimes}(S)$.

Definition 3.1. *Let $(S,<)$ be an ordered semigroup. For $u = u_1 \otimes \cdots \otimes u_r \in S^{\otimes r}$ and $v = v_1 \otimes \cdots \otimes v_s \in S^{\otimes s}$, define*

$$u <_{\mathrm{leng}} v \Leftrightarrow \begin{cases} r < s \text{ or} \\ r = s \text{ and } \exists\ 1 \leqslant i \leqslant r, \text{ such that } u_1 = v_1, \cdots, u_{i-1} = v_{i-1}, u_i < v_i. \end{cases} \tag{11}$$

$<_{\mathrm{leng}}$ will be called the **pro-length order** *(or* **L-order** *for short).*

We note that, when u and v have the same length, $u <_{\mathrm{lex}} v$ if and only if $u <_{\mathrm{leng}} v$. Recall that a well-ordered set is a totally ordered set whose every non-empty subset has a smallest element.

Lemma 3.2. *Let $(S,<)$ be a well-ordered set. Then the* L-order $<_{\mathrm{leng}}$ *defines a well order on the set $M^{\otimes}(S)$.*

Proof. $<_{\mathrm{leng}}$ is clearly a total order on $M^{\otimes}(S)$. Let T be a non-empty subset of $M^{\otimes}(S)$. Define T_0 to be the subset of T consisting of words of the smallest length r, T_1 to be the subset of T_0 consisting of tensors $u_1 \otimes \cdots \otimes u_r$ such that u_1 is the smallest, T_2 to be the the subset of T_1 consisting of tensors $u_1 \otimes \cdots \otimes u_r$ such that u_2 is the smallest, $\cdots$, T_r to be the subset of T_{r-1} consisting of tensors $u_1 \otimes \cdots \otimes u_r$ such that u_r is the smallest. Then the smallest element of T is the unique element of T_r. □

We list the following results for later references.

Theorem 3.3. (a) **(Chen-Fox-Lyndon factorization)** [37] *Any word $w \in M^{\otimes}(S)$ can be written uniquely as a tensor product of Lyndon words*

$$w = w_1^{\otimes i_1} \otimes \cdots \otimes w_k^{\otimes i_k}, \quad w_1 > \cdots > w_k,\ i_1, \cdots, i_k \geqslant 1.$$

(b) **(Tensor form of freshman's dream)** [19, Theorem 4.1] *For any $w = w_1 \otimes \cdots \otimes w_n \in M^{\otimes}(S)$ and $\lambda \in \mathbf{k}$,*

$$w^{\diamond_\lambda p} \equiv \lambda^{(p-1)(n-1)} w_1^p \otimes \cdots \otimes w_n^p \mod p. \tag{12}$$

Notation: For $u \in \mathrm{MS}_{\mathbf{k},\lambda}(S)$ and $w \in M^{\otimes}(S)$, we write

$$u = w + \text{ lower L-order terms}$$

if $u - w$ is a linear combination of words in $M^{\otimes}(S)$ with L-order less than w.

Lemma 3.4. *The following statements hold in* $\mathrm{MS}_{\mathbb{Z},\lambda}(S)$.

(a) *Let* $w = w_1^{\otimes i_1} \otimes \cdots \otimes w_k^{\otimes i_k}$ *be the Chen-Fox-Lyndon factorization. We have*

$$w_1^{\diamond_\lambda i_1} \diamond_\lambda \cdots \diamond_\lambda w_k^{\diamond_\lambda i_k} = (i_1! \cdots i_k!)w + \textit{lower} \text{ L-order } \textit{terms}.$$

(b) *Let* u *be a Lyndon word and let* v *be a word with* $u > v$*. Then*

$$u^{\otimes s} \diamond_\lambda v = u^{\otimes s} \otimes v + \textit{lower} \text{ L-order } \textit{terms}.$$

(c) *Let* u *be a Lyndon word and let* $n_1, \cdots n_k$ *be positive integers. Then*

$$u^{\otimes n_1} \diamond \cdots \diamond u^{\otimes n_k} = \frac{(n_1 + \cdots + n_k)!}{n_1! \cdots n_k!} u^{\otimes (n_1 + \cdots n_k)} + \textit{lower} \text{ L-order } \textit{terms}.$$

(d) *For any Lyndon word* u *and integer* $n = a_0 + a_1 p + a_2 p^2 + \cdots a_k p^k$ *with* $a_0, \cdots, a_k \in \{0, 1, \cdots, p-1\}$*, we have*

$$(u^{\otimes p^0})^{\diamond_\lambda a_0} \diamond_\lambda \cdots \diamond_\lambda (u^{\otimes p^k})^{\diamond_\lambda a_k} = N_n u^{\otimes n} + \textit{ lower} \text{ L-order } \textit{terms}, \tag{13}$$

where N_n *is a p-adic unit.*

Proof. (a). As is well-known [37], for the shuffle product $\text{ш} = \diamond_0$ (mixable shuffle product of weight 0), we have

$$w_1^{\diamond_0 i_1} \diamond_0 \cdots \diamond_0 w_k^{\diamond_0 i_k} = (i_1! \cdots i_k!)w + \sum_{\ell(u)=\ell(w), u<w} \alpha_u u$$

for some natural integer α_u. By the definition of the mixable shuffle product of weight λ,

$$w_1^{\diamond_\lambda i_1} \diamond_\lambda \cdots \diamond_\lambda w_k^{\diamond_\lambda i_k} = w_1^{\diamond_0 i_1} \diamond_0 \cdots \diamond_0 w_k^{\diamond_0 i_k} + \text{terms of length} < \ell(w).$$

Since either $\ell(u) = \ell(w)$ with $u <_{\text{lex}} w$ or $\ell(u) < \ell(w)$ implies $u <_{\text{leng}} w$, we are done.

(b). Let $v = v_1^{\otimes i_1} \otimes \cdots \otimes v_k^{\otimes i_k}$ be the Chen-Fox-Lyndon factorization. Since v_1 is a Lyndon word, we have $v > v_1$. Since it is assume that $v < u$, we have $u > v_1$. Thus $u^{\otimes s} \otimes v = u^{\otimes s} \otimes v_1^{\otimes i_1} \otimes \cdots \otimes v_k^{\otimes i_k}$ is the Chen-Fox-Lyndon factorization of $u^{\otimes s} \otimes v$. Then by Item (a),

$$u^{\diamond_\lambda s} \diamond_\lambda v_1^{\diamond_\lambda i_1} \diamond_\lambda \cdots \diamond_\lambda v_k^{\diamond_\lambda i_k} = (s!)(i_1!) \cdots (i_k!) u^{\otimes s} \otimes v + \text{lower L-order terms}.$$

On the other hand, applying Item (a) separately to $u^{\otimes s}$ and $v = v_1^{\otimes i_1} \otimes \cdots \otimes v_k^{\otimes i_k}$, we have $u^{\diamond_\lambda s} \diamond_\lambda v_1^{\diamond_\lambda i_1} \diamond_\lambda \cdots \diamond_\lambda v_k^{\diamond_\lambda i_k} = (s!) u^{\otimes s} \diamond_\lambda ((i_1!) \cdots (i_k!)) v + \text{terms with L-order lower than } u^{\otimes s} \otimes v$. This gives what we need.

(c). By Item (a) we have

$$\frac{1}{n_i!} u^{\diamond_\lambda n_i} = u^{\otimes n_i} + \text{lower L-order terms}.$$

So

$$\begin{aligned} u^{\otimes n_1} \diamond_\lambda \cdots \diamond_\lambda u^{\otimes n_k} &= \frac{1}{n_1! \cdots n_k!} u^{\diamond_\lambda (n_1 + \cdots + n_k)} + \text{terms with L-order lower than } u^{\otimes (n_1 + \cdots + n_k)} \\ &= \frac{(n_1 + \cdots + n_k)!}{n_1! \cdots n_k!} u^{\otimes (n_1 + \cdots + n_k)} + \text{lower L-order terms}, \end{aligned}$$

as desired.

(d) is a special case of (c) since $N_n = \frac{n!}{\prod_{j=0}^{k}(p^j!)^{a_j}}$ is a p-adic unit [28, Corollary 7.6]. □

Let A be a commutative $\mathbf{k}$-algebra. For a pure tensor a in $A^{\otimes n}$, denote $a^{\otimes k}$ to be the k fold tensor power of a. For a set Y of pure tensors and a prime number p, denote

$$Y^{\otimes k} = \{a^{\otimes k} \mid a \in Y\}, \quad \mathrm{T}(Y) = \coprod_{k \geqslant 0} Y^{\otimes p^k}. \tag{14}$$

Here T stands for tensor power. When $Y = \mathrm{Lyn}$ is the set of Lyndon words in $\mathrm{MS}_{\mathbf{k},\lambda}(S)$ where S is an ordered semigroup, we denote $\mathrm{TL} = \mathrm{T}(\mathrm{Lyn})$.

We will use the following proposition several times.

Proposition 3.5. *Let* $\mathbf{k}$ *be either* $\mathbb{F}_p$ *or* $\mathbb{Z}_p$. *Let* S *be a well-ordered semigroup and let* $\lambda \in \mathbf{k}$. *Denote* $\diamond = \diamond_\lambda$.

(a) *As a* $\mathbf{k}$*-algebra,* $\mathrm{MS}_{\mathbf{k},\lambda}(S)$ *is generated by* TL *for any* $\lambda \in \mathbf{k}$.

(b) *The subset*

$$U := \{1\} \cup \{w_1^{\diamond n_1} \diamond \cdots \diamond w_r^{\diamond n_r} \mid w_j \in \mathrm{TL}, w_1 > \cdots > w_r, 1 \leqslant n_j \leqslant p-1, 1 \leqslant j \leqslant r, r \geqslant 1\} \tag{15}$$

of $\mathrm{MS}_{\mathbf{k},\lambda}(S)$ *is linearly independent.*

Proof. (a). Let $\mathrm{MS}_{\mathbf{k},\lambda}(S)'$ be the $\mathbf{k}$-subalgebra of $\mathrm{MS}_{\mathbf{k},\lambda}(S)$ generated by TL. We just need to prove $M^{\otimes}(S) \subseteq \mathrm{MS}_{\mathbf{k},\lambda}(S)'$ by contradiction. First of all, the smallest element in $M^{\otimes}(S)$ is the 1-tensor s_0 where s_0 denotes the smallest element of the well-ordered semigroup S. Since s_0 is a Lyndon word, s_0 is in $\mathrm{MS}_{\mathbf{k},\lambda}(S)'$. Therefore $M^{\otimes}(S) \backslash \mathrm{MS}_{\mathbf{k},\lambda}(S)'$ is not $M^{\otimes}(S)$. Suppose $M^{\otimes}(S) \not\subseteq \mathrm{MS}_{\mathbf{k},\lambda}(S)'$, then $M^{\otimes}(S) \backslash \mathrm{MS}_{\mathbf{k},\lambda}(S)'$ is not empty. Since by Lemma 3.2, $M^{\otimes}(S)$ is a well-ordered set with respect to the L-order, there is a smallest element w in $M^{\otimes}(S) \backslash \mathrm{MS}_{\mathbf{k},\lambda}(S)'$. Let $w = w_1^{\otimes i_1} \otimes \cdots \otimes w_r^{i_r}, w_1 > \cdots > w_r$, be the Chen-Fox-Lyndon factorization of w.

Suppose $r = 1$. Then $w = w_1^{\otimes n}$ for some $n \geqslant 1$. Using the notation of Lemma 3.4.(d), we have

$$w_1^{\otimes n} = N_n^{-1}(w_1^{\otimes p^0})^{\diamond a_0} \diamond \cdots \diamond (w_1^{\otimes p^r})^{\diamond a_r} + \text{terms with L-order lower than } w_1^{\otimes n},$$

where N_n is a p-adic unit. Since $(w_1^{\otimes p^0})^{\diamond a_0} \diamond \cdots \diamond (w_1^{\otimes p^r})^{\diamond a_r}$ is a product of the elements $w_1^{\otimes p^i}, i \geqslant 0$, that are already in TL, this product is in $\mathrm{MS}_{\mathbf{k},\lambda}(S)'$. By the minimality of $w = w_1^{\otimes n}$, the other terms on the right hand side of the above equation are also in $\mathrm{MS}_{\mathbf{k},\lambda}(S)'$. Thus $w_1^{\otimes n}$ is in $\mathrm{MS}_{\mathbf{k},\lambda}(S)'$. This is a contradiction.

Suppose $r > 1$. Then by the Chen-Fox-Lyndon factorization, we have $w_2^{\otimes i_2} \otimes \cdots \otimes w_r^{i_r} < w_1$. Hence Lemma 3.4 (b) gives

$$w = w_1^{\otimes i_1} \otimes w_2^{\otimes i_2} \otimes \cdots \otimes w_r^{i_r} = w_1^{\otimes i_1} \diamond (w_2^{\otimes i_2} \otimes \cdots \otimes w_r^{i_r}) + \text{terms with L-order lower than } w.$$

By the minimality of w, we have $w_1^{\otimes s}, w_2^{\otimes i_2} \otimes \cdots \otimes w_r^{i_r} \in \mathrm{MS}(S)'$ since they have lengths shorter than w and hence L-orders lower than w. Therefore, w is also in $\mathrm{MS}(X)'$. This again is a contradiction and completes our proof that $M^{\otimes}(S) \subseteq \mathrm{MS}_{\mathbf{k},\lambda}(S)'$.

(b). Define

$$\Gamma = \{\gamma : \mathrm{TL} \to \{0, \cdots, p-1\} \mid \gamma \text{ has finite support}\}. \tag{16}$$

Then we have

$$U = \{w_\gamma := \mathop{\diamond}_{w\in \mathrm{TL}} w^{\diamond_\lambda \gamma(w)} \mid \gamma \in \Gamma\}. \tag{17}$$

For $\gamma \neq 0$, let the support of γ be $\{w_1, \cdots, w_r\} \subseteq \mathrm{TL}$ with $w_1 > \cdots > w_r$. Note that each w_i is a $u^{\otimes p^j}$ for some $u \in \mathrm{Lyn}$ and $j \geqslant 0$. Let $u_1 > \cdots > u_t$ be such u's in Lyn. Then

$$(w_1, \cdots, w_r) = (u_1^{\otimes p^{i_{1,1}}}, \cdots, u_1^{\otimes p^{i_{1,a_1}}}, u_2^{\otimes p^{i_{2,1}}}, \cdots, u_2^{\otimes p^{i_{2,a_2}}}, \cdots, u_t^{\otimes p^{i_{t,1}}}, \cdots, u_t^{\otimes p^{i_{t,a_t}}}),$$

where $i_{j,1} > \cdots > i_{j,a_j}$, $a_j \geqslant 1, 1 \leqslant j \leqslant t$. Thus

$$\begin{aligned} w_\gamma &= w_1^{\diamond_\lambda \gamma(w_1)} \diamond_\lambda \cdots \diamond_\lambda w_r^{\diamond_\lambda \gamma(w_r)} \\ &= \mathop{\diamond_\lambda}_{j=1}^{t} \Big(\mathop{\diamond_\lambda}_{k=1}^{a_j} (u_j^{\otimes p^{i_{j,k}}})^{\diamond_\lambda \gamma(u_j^{\otimes p^{i_{j,k}}})} \Big) \\ &= \mathop{\diamond_\lambda}_{j=1}^{t} \Big(\mathop{\diamond_\lambda}_{\ell=1}^{\infty} (u_j^{\otimes p^{\ell}})^{\diamond_\lambda \gamma(u_j^{\otimes p^{\ell}})} \Big) \end{aligned} \tag{18}$$

since $\gamma(u_j^{\otimes p^\ell}) = 0$ outside the support of γ. Similarly,

$$\begin{aligned} w_1^{\otimes \gamma(w_1)} \otimes \cdots \otimes w_r^{\otimes \gamma(w_r)} &= \mathop{\otimes}_{j=1}^{t} \Big(\mathop{\otimes}_{k=1}^{a_j} (u_j^{\otimes p^{i_{j,k}}})^{\otimes \gamma(u_j^{\otimes p^{i_{j,k}}})} \Big) \\ &= \mathop{\otimes}_{j=1}^{t} u_j^{\otimes (\sum_{k=1}^{a_j} p^{i_{j,k}} \gamma(u_j^{\otimes p^{i_{j,k}}}))} \\ &= \mathop{\otimes}_{j=1}^{t} u_j^{\otimes (\sum_{\ell=0}^{\infty} p^{\ell} \gamma(u_j^{\otimes p^{\ell}}))}. \end{aligned} \tag{19}$$

Then by Eq. (18),

$$\begin{aligned} w_\gamma &= \mathop{\diamond_\lambda}_{j=1}^{t} (N_{\gamma,u_j} u_j^{\otimes (\sum_{\ell=0}^{\infty} p^{\ell} \gamma(u_j^{\otimes p^{\ell}}))} + \text{ lower L-order terms}) \qquad \text{(by Lemma 3.4. (d))} \\ &= N_\gamma \mathop{\otimes}_{j=1}^{t} u_j^{\otimes (\sum_{\ell=0}^{\infty} p^{\ell} \gamma(u_j^{\otimes p^{\ell}}))} + \text{ lower L-order terms} \qquad \text{(by Lemma 3.4. (b))} \\ &= N_\gamma w_1^{\otimes \gamma(w_1)} \otimes \cdots \otimes w_r^{\otimes \gamma(w_r)} + \text{ lower L-order terms} \qquad \text{(by Eq. (19)).} \end{aligned} \tag{20}$$

Here N_{γ,u_j} is a p-adic unit that only depends on u_j and γ, and $N_\gamma = \prod_{j=1}^{t} N_{\gamma,u_j}$. Since all the leading terms are distinct and the leading coefficients are p-adic units, the displayed elements in U are all distinct.

Now suppose the set U is linearly dependent. Then there is a linear combination

$$\sum_{u\in U} a_u u = 0$$

such that not all a_u are zero. Among all the u's with nonzero coefficients, let u_0 be the one such that the leading word w of u_0 in Eq. (20) is the largest. Then a_{u_0} is in fact the coefficient of w when $\sum_{u\in U} a_u u = 0$ is expanded by Eq. (20). Therefore $u_0 = 0$, a contradiction. $\square$

3.2. **Mixable shuffle algebras with coefficients in $\mathbb{F}_p$.** Let p be a prime and let $\mathbf{k} = \mathbb{F}_p$ in this section. We study the structure of $\mathrm{MS}_{\mathbf{k},\lambda}(S)$ for a semigroup S. When $\lambda = 0$, this structure is easy to give (Theorem 3.7). It is more subtle when $\lambda \neq 0$ and we have to distinguish several types of abelian semigroups, such as free semigroups, elementary p-groups and p-idempotent semigroups. To avoid case by case consideration and repeated arguments, we provide an axiomatic framework in Section 3.2.2 before stating and proving our main theorem in Section 3.2.3.

3.2.1. *Mixable shuffle algebras of weight* 0. We consider mixable shuffle algebras $\mathrm{MS}_{\mathbb{F}_p,\lambda}(S)$ of weight 0, that is, shuffle product algebras. It is defined as long as S is a set.

Definition 3.6. *Let A be a $\mathbf{k}$-algebra. Let Y be a subset of A. Define*

$$\widehat{Y} := \{\widehat{y} \mid y \in Y\}$$

to be the set of symbols that is in bijection with Y. Define

$$\phi : \mathbf{k}[\widehat{Y}] \to A, \quad \widehat{y} \mapsto y, \quad y \in Y,$$

to be the algebra homomorphism that "evaluates" $\widehat{y}$ to y.

Theorem 3.7. *Let S be a finite ordered set. Let $\mathrm{TL} = \mathrm{T}(\mathrm{Lyn}(S))$ be as defined in Eq. (14). Let $\widehat{\mathrm{TL}} = \{\widehat{w} \mid w \in \mathrm{TL}\}$ be as defined in Definition 3.6. Then*

$$\mathrm{MS}_{\mathbb{F}_p,0}(S) \cong \mathbb{F}_p[\widehat{\mathrm{TL}}]/\langle \widehat{w}^p \mid \widehat{w} \in \mathrm{TL}\rangle = \bigotimes_{\widehat{w}\in\mathrm{TL}} \Big(\mathbb{F}_p[\widehat{w}]/\langle \widehat{w}^p\rangle\Big). \tag{21}$$

Here $\langle Y\rangle$ denotes the ideal generated by Y.

Proof. By Proposition 3.5.(a), we have a surjective $\mathbb{F}_p$-algebra homomorphism

$$\phi : \mathbb{F}_p[\widehat{\mathrm{TL}}] \to \mathrm{MS}_{\mathbb{F}_p,0}(S), \widehat{w} \mapsto w, w \in \mathrm{TL}.$$

As remarked at the beginning of Section 3, $u^p = p!u^{\otimes p} = 0$ for any word u in $\mathrm{MS}_{\mathbb{F}_p,0}(S)$. Thus $\langle \widehat{w}^p \mid \widehat{w} \in \widehat{\mathrm{TL}}\rangle$ is in the kernel of ϕ. Note that the set

$$\{1\} \cup \{\widehat{w}_1^{n_1} \cdots \widehat{w}_r^{n_r} \mid \widehat{w}_j \in \widehat{\mathrm{TL}}, w_1 > \cdots > w_r, 1 \leqslant n_j \leqslant p-1, 1 \leqslant j \leqslant r, r \geqslant 1\}$$

is a $\mathbb{F}_p$-basis of $\mathbb{F}_p[\widehat{\mathrm{TL}}]/\langle \widehat{w}^p \mid \widehat{w} \in \mathrm{TL}\rangle$ which is mapped onto the subset

$$U = \{1\} \cup \{w_1^{\diamond n_1} \diamond \cdots \diamond w_r^{\diamond n_r} \mid w_j \in \mathrm{TL}, w_1 > \cdots > w_r, 1 \leqslant n_j \leqslant p-1, 1 \leqslant j \leqslant r, r \geqslant 1\}$$

of $\mathrm{MS}_{\mathbb{F}_p,0}(S)$ defined in Eq. (15). Thus to show that ϕ is injective and hence finish the proof of the theorem, we only need to show that U is linearly independent. This is just Proposition 3.5.(b). □

3.2.2. *Two classes of semigroups and their Lyndon words.* For an abelian semigroup S, define

$$S_1 = \{g \in S \mid g^p = g\}, \quad S_2 = \{g \in S \mid g^p \neq g\}. \tag{22}$$

Then $S = S_1 \coprod S_2$. We will study $\mathrm{MS}_{\mathbb{F}_p,\lambda}(S)$ for S in the following two classes of abelian semigroups.

Definition 3.8. (a) Let $\mathcal{P}$ denote the class of well-ordered abelian semigroups $(S, <)$ such that, for any $a, b \in S$,

$$a > b \Rightarrow a^p > b^p, \text{and} \tag{23}$$

$$a^p \geqslant a. \tag{24}$$

(b) Let $\mathcal{J}$ denote the class of well-ordered abelian semigroups $(S, <)$ such that every element $g \in S$ satisfies $g^{p^2} = g^p$ and $g_1 < g_2$ for $g_1 \in S_1$ and $g_2 \in S_2$.

We give some examples to illustrate the wide range of semigroups covered by these two classes. We start with some examples and properties of $\mathcal{P}$.

Proposition 3.9. (a) *$\mathcal{P}$ contains the class $\mathcal{I}$ of pairs $(S, <)$ consisting of a finite abelian semigroup S that is p-**idempotent**, that is, $g^p = g$ for any element g in the semigroup, and any well order $<$ on S.*

(b) *Let $\mathcal{F}$ be the class of free abelian semigroups $F = F(X)$ generated by ordered finite sets X. For $(x_1^{n_1}, \cdots, x_{|X|}^{n_{|X|}}) \in F, x_i \in X, n_i \geqslant 1, 1 \leqslant i \leqslant |X|$, define $\deg(x_1^{n_1}, \cdots, x_{|X|}^{n_{|X|}}) = \sum_{i=1}^{|X|} n_i$. For $y_1, y_2 \in F$, define $y_1 > y_2$ if $\deg(y_1) > \deg(y_2)$, or if $\deg(y_1) = \deg(y_2)$ and y_1 is larger than y_2 according to the lexicographic order on F induced by the order on X. Then $\mathcal{F}$ is a subclass of $\mathcal{P}$.*

(c) *The class $\mathcal{P}$ is closed under the semigroup unitarization that adds an identity ι_P to an ordered semigroup $P \in \mathcal{P}$. The order on P is extended to $P \cup \{\iota_P\}$ by defining ι_P to be the smallest element. In particular, $\mathcal{P}$ contains free abelian monoids $M^{\mathrm{c}}(X)$ generated by ordered finite sets X.*

(d) *The class $\mathcal{P}$ is closed under taking finite direct products and sub-objects, with the (lexicographic) product order and restricted order, respectively.*

(e) *The class $\mathcal{P}$ is closed under taking semigroup direct coproducts with the coproduct order (see the proof for the construction).*

Proof. (a). Both of the two conditions on $\mathcal{P}$ follow from the p-idempotent condition $g^p = g$.

(b). Here checking of the two conditions boils down to the facts that, for positive integers m, n, $m > n$ if and only if $pm > pn$, and that $pm > m$.

(c) Let $P \in \mathcal{P}$ and consider the monoid $P \cup \{\iota_P\}$. Since elements in P already satisfy the two conditions for $\mathcal{P}$ and there is no $a \in P$ with $\iota_P > a$, we only need to check that $a > \iota_P$ implies $a^p > \iota_P^p$ and that $\iota_P^p \geqslant \iota_P$, both of which are clear.

(d) holds since the two conditions on $\mathcal{P}$ are preserved by taking finite direct products and subsets.

(e). Let $S, S' \in \mathcal{P}$. The coproduct $C = C(S, S')$ of S and S' is defined by the usual universal property. Explicitly, C is the disjoint union

$$C = (S \times S') \coprod S \coprod S'.$$

Extending the semigroup S (resp. S') to the monoid $S \cup \{\iota_S\}$ (resp. $S' \cup \{\iota_{S'}\}$) by adding an identity ι_S (resp. $\iota_{S'}$). Thus we can rewrite C as the sub-semigroup

$$C = \{(y, g) \in (S \cup \{\iota_S\}) \times (S' \cup \{\iota_{S'}\}) \mid (y, g) \neq (\iota_S, \iota_{S'})\}$$

of the monoid product $(S \cup \{\iota_S\}) \times (S' \cup \{\iota_{S'}\})$. By Item (c), $S \cup \{\iota_S\}$ and $S' \cup \{\iota_{S'}\}$ are in $\mathcal{P}$. Hence by Item (d), $\mathcal{P}$ contains $(S \cup \{\iota_S\}) \times (S' \cup \{\iota_{S'}\})$ with the product order, and then contains $C \subseteq (S \cup \{\iota_S\}) \times (S' \cup \{\iota_{S'}\})$ with the restricted order. □

We next provide some examples and properties of $\mathcal{J}$.

Proposition 3.10. (a) *Let $\mathcal{I}$ be the class in Proposition 3.9.(a). Then $\mathcal{I} \subseteq \mathcal{J}$.*

(b) *$\mathcal{J}$ contains the class $\mathcal{E}$ of pairs $(S, <)$ consisting of a finite abelian group S that is an* **elementary p-group**, *that is, $g^p = e$ for any element in the group. Here e is the identity and $<$ is any choice of well order on S such that e is the smallest element.*

(c) *The class $\mathcal{J}$ is closed under taking finite direct products and sub-objects, with the product order and restricted order, respectively.*

We will use the notations $\mathcal{P}, \mathcal{J}, \mathcal{I}, \mathcal{F}, \mathcal{C}, \mathcal{E}$ with the above meanings in the rest of this paper.

Proof. The verifications of Items (a) and (b) are clear. Item (c) follows since the defining properties of $\mathcal{J}$ are preserved under taking finite direct products and subsets. □

Let a semigroup S be in $\mathcal{P}$ or $\mathcal{J}$. For a word $w = u_1 \otimes \cdots \otimes u_r \in S^{\otimes r} \subseteq M^{\otimes}(S)$, denote

$$w^{\langle p \rangle} = u_1^p \otimes \cdots \otimes u_r^p. \tag{25}$$

Lemma 3.11. *Let $S \in \mathcal{P}$.*

(a) *$a > b \Leftrightarrow a^p > b^p$.*

(b) *$a = b \Leftrightarrow a^p = b^p$.*

(c) *A* word $w \in M^{\otimes}(S)$ is a Lyndon word if and only if $w^{\langle p \rangle}$ is a Lyndon word.

Proof. (a). Suppose $a^p > b^p$ but $a \leqslant b$, then either $a < b$ which implies that $a^p < b^p$, or $a = b$ which implies that $a^p = b^p$. Both are contradictions. So $a > b$. The same argument applies to prove (b).

(c). By Items (a) and (b), the map

$$F : S \to S' := \{g^p \mid g \in S\}, \quad g \mapsto g^p, g \in S,$$

is an isomorphism of the two ordered sets with the order on S' being restricted from S. Since Lyndon words are determined solely by the orders, an order-preserving set map sends a Lyndon word to a Lyndon word. Then Item (c) follows. □

For $S \in \mathcal{P}$ or $\mathcal{J}$, S_1 is a sub-semigroup of S and remains in the same class as S. Define the subset of **p-divisible elements** of S:

$$S_{\mathrm{div}} := \bigcap_{r \geqslant 1} \{u^{p^r} \mid u \in S\}. \tag{26}$$

Lemma 3.12. *Let S be in $\mathcal{P}$.*

(a) *$S_{\mathrm{div}} = S_1$.*

(b) *For $i = 1, 2$, $g \in S_i$ if and only if $g^p \in S_i$.*

Proof. (a). Since clearly $S_{\mathrm{div}} \supseteq S_1$, it remains to show that $S_{\mathrm{div}} \backslash S_1$ is empty. Suppose not, then since S is a well-ordered set, $S_{\mathrm{div}} \backslash S_1$ has a minimal element, denoted by w_0. Then $w_0 \neq w_0^p$ but $w_0 = u^p$ for some $u \in S$. Since w_0 is in S_{div}, there is a u_r for each $r \geqslant 1$ such that $w_0 = u_r^{p^r}$. Then we have $u_1^p = w_0 = (u_r^{p^{r-1}})^p$ for $r \geqslant 2$. By Lemma 3.11.(b),

we get $u_1 = u_r^{p^{r-1}}, r \geqslant 2$. Thus u_1 is in S_{div}. Suppose u_1 is in S_1. Then $u_1 = u_1^p = w_0$. Then $w_0^p = u_1^p = u_1 = w_0$, yielding a contradiction. Therefore, $u_1 \in S_{\mathrm{div}} \backslash S_1$. By the minimality of w_0, we must have $w_0 \leqslant u_1$. By Eq. (24), $w_0 = u_1^p \geqslant u_1$. Thus $w_0 = u_1$, that is, $w_0 = u_1^p = w_0^p$, again a contradiction.

(b). By Lemma 3.11.(b),

$$g \in S_1 \Leftrightarrow g^p = g \Leftrightarrow g^{p^2} = g^p \Leftrightarrow g^p \in S_1.$$

Then the claim for S_2 follows since S_1 and S_2 are disjoint. □

We define the following operators on subsets $W \subseteq M^{\otimes}(S)$.

$$\begin{aligned} W_1 &= \{w \in W \mid w^{\langle p \rangle} = w\}, \\ W_2 &= \{w \in W \mid w^{\langle p \rangle} \neq w\}, \\ \mathrm{E}(W) &= \{w \in W \mid \text{ either } w = w^{\langle p \rangle} \text{ or } w \neq u^{\langle p \rangle} \text{ for any } u \in M^{\otimes}(S)\}. \end{aligned} \tag{27}$$

Clearly $W = W_1 \coprod W_2$. Recall from Eq. (14) that we have also defined the operator

$$\mathrm{T}(W) = \{w^{\otimes p^i} \mid i \in \mathbb{Z}_{\geqslant 0}, w \in W\}.$$

The following lemma shows that the four operators $W \mapsto W_1, W \mapsto W_2, W \mapsto \mathrm{E}(W)$ and $W \mapsto \mathrm{T}(W)$ all commute with one another.

Lemma 3.13. *Let W be any subset of $M^{\otimes}(S)$.*

$$\mathrm{E}(\mathrm{T}(W)) = \mathrm{T}(\mathrm{E}(W)), \quad \mathrm{T}(W_i) = \mathrm{T}(W)_i, \quad i = 1, 2. \tag{28}$$

$$\mathrm{E}(W_1) = W_1 = \mathrm{E}(W)_1, \quad \mathrm{E}(W_2) = \mathrm{E}(W)_2. \tag{29}$$

Proof. Eq. (28) follows easily from the definitions.

For Eq.(29), $\mathrm{E}(W_1) = W_1$ follows from the definitions. Then

$$W_1 = (W_1)_1 = \mathrm{E}(W_1)_1 \subseteq \mathrm{E}(W)_1 \subseteq W_1.$$

Thus $\mathrm{E}(W_2) = \mathrm{E}(W \backslash W_1) = \mathrm{E}(W) \backslash \mathrm{E}(W_1) = \mathrm{E}(W) \backslash \mathrm{E}(W)_1 = \mathrm{E}(W)_2$. □

For notational convenience, we will skip the parentheses in the operators and denote

$$\begin{gathered} \mathrm{E}W = \mathrm{E}(W), \quad \mathrm{T}W = \mathrm{T}(W), \quad \mathrm{TE}W = \mathrm{T}(\mathrm{E}(W)), \\ \mathrm{E}W_i = \mathrm{E}(W_i), \quad \mathrm{T}W_i = \mathrm{T}(W_i), \quad \mathrm{TE}W_i = \mathrm{T}(\mathrm{E}(W_i)), \quad i = 1, 2. \end{gathered}$$

In particular, for $\mathrm{L} = \mathrm{Lyn}(S)$,

$$\begin{gathered} \mathrm{EL} = \mathrm{E}(\mathrm{L}), \quad \mathrm{TL} = \mathrm{T}(\mathrm{L}), \quad \mathrm{TEL} = \mathrm{T}(\mathrm{E}(\mathrm{L})), \\ \mathrm{EL}_i = \mathrm{E}(\mathrm{L}_i), \quad \mathrm{TL}_i = \mathrm{T}(\mathrm{L}_i), \\ \mathrm{TEL}_i = \mathrm{T}(\mathrm{E}(\mathrm{L}_i)) = \{w = u^{\otimes p^r} \mid u \in \mathrm{EL}_i, r \in \mathbb{Z}_{\geqslant 0}\}, \quad i = 1, 2. \end{gathered} \tag{30}$$

By Lemma 3.13, there is no ambiguity in these notations, since, for example,

$$\mathrm{TEL}_1 = \mathrm{T}(\mathrm{E}(\mathrm{L}_1)) = \mathrm{T}(\mathrm{E}(\mathrm{L})_1) = \mathrm{T}(\mathrm{E}(\mathrm{L}))_1 = \mathrm{E}(\mathrm{T}(\mathrm{L}_1)).$$

When S is the free abelian semigroup with one generator, our TL and TEL agree with the sets SL and ESL defined in [28].

Lemma 3.14. *Let S be in $\mathcal{P}$. Let $\mathrm{L} = \mathrm{Lyn}(S)$ be the set of Lyndon words. Then we have*

$$\mathrm{TL}_1 = \mathrm{TEL}_1, \tag{31}$$

$$\mathrm{L}_1 = \mathrm{Lyn}(S_1). \tag{32}$$

Proof. By Eq. (29) we have $\mathrm{L}_1 = \mathrm{EL}_1$. So applying the operator T, we have $\mathrm{TL}_1 = \mathrm{TEL}_1$.

For Eq. (32), let $w = w_1 \otimes \cdots \otimes w_r \in S^{\otimes r}$ be a Lyndon word. Then

$$(w \in \mathrm{L}_1) \Leftrightarrow (w^{\langle p \rangle} = w) \Leftrightarrow (w_1^p \otimes \cdots \otimes w_r^p = w_1 \otimes \cdots \otimes w_r)$$
$$\Leftrightarrow (w_i^p = w_i, 1 \leqslant i \leqslant r) \Leftrightarrow (w_i \in S_1, 1 \leqslant i \leqslant r) \Leftrightarrow (w \in \mathrm{Lyn}(S_1)).$$

□

Lemma 3.15. *Let $S \in \mathcal{P}$. Then $\mathrm{TL}_2 = \{u^{\langle p^i \rangle} \mid u \in \mathrm{TEL}_2, i \geqslant 0\}$. Further, all the displayed elements are distinct.*

Proof. Note that for any $u^{\langle p^i \rangle}$ in the set of the right hand side, $u = w^{\otimes p^j}$ for some $w \in \mathrm{EL}_2$. Since $(w^{\otimes p^j})^{\langle p^i \rangle} = (w^{\langle p^i \rangle})^{\otimes p^j}$, and $w^{\langle p^i \rangle}$ is also in Lyn_2 by Lemma 3.12.(b), we have $(w^{\langle p^i \rangle})^{\otimes p^j} \in \mathrm{TL}_2$. This proves $\supseteq$.

Conversely, let $v^{\otimes p^j} \in \mathrm{TL}_2$ with $v \in \mathrm{Lyn}_2$. Then a tensor factor of v is in S_2, and hence is not in S_{div} by Lemma 3.12.(a). This means $v = w^{\langle p^i \rangle}$ for some $w \in \mathrm{EL}_2$. This shows that $v^{\otimes p^j} = (w^{\langle p^i \rangle})^{\otimes p^j} = (w^{\otimes p^j})^{\langle p^i \rangle}$ is in $\{u^{\langle p^i \rangle} \mid u \in \mathrm{TEL}_2, i \geqslant 0\}$.

Suppose there are $u, v \in \mathrm{TEL}_2$ and $i, j \geqslant 0$ such that $u^{\langle p^i \rangle} = v^{\langle p^j \rangle}$. Without loss of generality, we can take $i \geqslant j$. Then $(u^{\langle p^{i-j} \rangle})^{\langle p^j \rangle} = v^{\langle p^j \rangle}$. By Lemma 3.11.(b), $u^{\langle p^{i-j} \rangle} = v$. Since $v \in \mathrm{TEL}_2$, we have $v \neq v^{\langle p \rangle}$. Since $v \in \mathrm{TEL}_2 = \mathrm{E}(\mathrm{TL}_2)$ by Eq. (28), from the definition of the operator E in Eq. (27), we have $v \neq w^{\langle p \rangle}$ for any word w. So from $u^{\langle p^{i-j} \rangle} = v$ we obtain $i - j = 0$ and then $u = v$. □

For $S \in \mathcal{J}$, define

$$\begin{aligned} \widetilde{\mathrm{TL}}_2 &:= \widetilde{\mathrm{TL}}_2(S) = \{w - w^{\langle p \rangle} \mid w \in \mathrm{TL}_2\}, \\ \widetilde{\mathrm{TL}} &:= \widetilde{\mathrm{TL}}(S) = \mathrm{TL}_1(S) \cup \widetilde{\mathrm{TL}}_2(S). \end{aligned} \tag{33}$$

3.2.3. *Mixable shuffle algebras of nonzero weight.* We now consider a mixable shuffle algebra $\mathrm{MS}_{\mathbb{F}_p,\lambda}(S)$ on a semigroup S when $\lambda \neq 0$.

Lemma 3.16. *Let $S \in \mathcal{J}$ and let $\lambda \in \mathbb{F}_p$ be non-zero. For any* word $w \in \mathrm{MS}_{\mathbb{F}_p,\lambda}(S)$,

$$(w - w^{\langle p \rangle})^{\diamond_{\lambda p}} = 0. \tag{34}$$

Proof. Let w be in $\mathrm{MS}_{\mathbb{F}_p,\lambda}(S)$. We have

$$\begin{aligned} (w - w^{\langle p \rangle})^{\diamond_{\lambda p}} &= w^{\diamond_{\lambda p}} - (w^{\langle p \rangle})^{\diamond_{\lambda p}} \\ &= \lambda^{(\ell(w)-1)(p-1)} w^{\langle p \rangle} - \lambda^{(\ell(w^{\langle p \rangle})-1)(p-1)} (w^{\langle p \rangle})^{\langle p \rangle} \qquad \text{(by Eq. (12))} \\ &= \lambda^{(\ell(w)-1)(p-1)} w^{\langle p \rangle} - \lambda^{(\ell(w)-1)(p-1)} w^{\langle p^2 \rangle} \qquad (\ell(w^{\langle p \rangle}) = \ell(w)) \\ &= \lambda^{(\ell(w)-1)(p-1)} w^{\langle p \rangle} - \lambda^{(\ell(w)-1)(p-1)} w^{\langle p \rangle}. \qquad \text{(defining property of } \mathcal{J}) \end{aligned}$$

Hence we have the lemma. □

With notations introduced in Eq. (30)and Eq. (33), we can state our main theorem on mixable shuffle algebras with weight $\lambda \neq 0$ and with coefficients in $\mathbb{F}_p$.

Theorem 3.17. *Let $0 \neq \lambda \in \mathbb{F}_p$. We will use the notation from Definition 3.6.*

(a) *For a semigroup S in $\mathcal{P}$, we have*

$$\begin{aligned} \mathrm{MS}_{\mathbb{F}_p,\lambda}(S) &\cong \mathbb{F}_p[\widehat{\mathrm{TEL}}]/\langle \widehat{w}^p - \widehat{w} \mid \widehat{w} \in \widehat{\mathrm{TEL}_1}\rangle \\ &\cong \mathbb{F}_p[\widehat{\mathrm{TEL}_1}]/\langle \widehat{w}^p - \widehat{w} \mid \widehat{w} \in \widehat{\mathrm{TEL}_1}\rangle \otimes \mathbb{F}_p[\widehat{\mathrm{TEL}_2}]. \end{aligned} \tag{35}$$

In particular, for $S \in \mathcal{F}$,

$$\mathrm{MS}_{\mathbb{F}_p,\lambda}(S) \cong \mathbb{F}_p[\widehat{\mathrm{TEL}}].$$

(b) *For S in $\mathcal{J}$, we have*

$$\mathrm{MS}_{\mathbb{F}_p,\lambda}(S) \cong \left(\mathbb{F}_p[\widehat{\mathrm{TL}_1}]/\langle \widehat{w}^p - \widehat{w} \mid \widehat{w} \in \widehat{\mathrm{TL}_1}\rangle\right) \otimes \left(\mathbb{F}_p[\widehat{\widehat{\mathrm{TL}_2}}]/\langle \widehat{w}^p \mid \widehat{w} \in \widehat{\widehat{\mathrm{TL}_2}}\rangle\right). \tag{36}$$

Corollary 3.18. *Let X be a finite ordered set. Let $S = M^{\mathrm{c}}(X)$ be the free abelian monoid generated by X. Then*

$$\mathrm{MS}_{\mathbb{F}_p,\lambda}(\mathbb{F}_p[X]) \cong \mathbb{F}_p[\widehat{\mathrm{TEL}_2}] \otimes \left(\mathbb{F}_p[\widehat{\mathrm{TEL}_1}]/\langle \widehat{w}^p - \widehat{w} \mid \widehat{w} \in \widehat{\mathrm{TEL}_1}\rangle\right). \tag{37}$$

We note that in this case,

$$\mathrm{TEL}_1 = \{1^{\otimes p^i} \mid i \geqslant 0\}. \tag{38}$$

Proof. By Proposition 3.9.(c), $M^{\mathrm{c}}(X)$ is in $\mathcal{P}$. Since $\mathrm{MS}_{\mathbb{F}_p,\lambda}(M^{\mathrm{c}}(X)) = \mathrm{MS}_{\mathbb{F}_p,\lambda}(\mathbb{F}_p[X])$, the corollary follows from Theorem 3.17.(a). □

Proof of Theorem 3.17. (a). We first show the surjectivity of the natural $\mathbb{F}_p$-algebra homomorphism

$$\phi : \mathbb{F}_p[\widehat{\mathrm{TEL}}] \to \mathrm{MS}_{\mathbb{F}_p,\lambda}(S)$$

in Definition 3.6 sending $\widehat{w} \in \widehat{\mathrm{TEL}}$ to $w \in \mathrm{TEL}$.

Let $\mathrm{MS}_{\mathbb{F}_p,\lambda}(S)'$ be the image of ϕ. By Proposition 3.5, we only need to show $\mathrm{TL} \subseteq \mathrm{MS}_{\mathbb{F}_p,\lambda}(S)'$. Let $w \in \mathrm{TL}$. Then either $w \in \mathrm{TL}_1$ or $w \in \mathrm{TL}_2$. If $w \in \mathrm{TL}_1$, then by Eq. (31), $w \in \mathrm{TEL}_1 \subseteq \mathrm{TEL}$ and hence is in $\mathrm{MS}_{\mathbb{F}_p,\lambda}(S)'$. If $w \in \mathrm{TL}_2$, then $w = u^{\langle p^i \rangle}$ for some $u \in \mathrm{TEL}_2$ by Lemma 3.15. By Eq. (12),

$$u^{\diamond_\lambda p^i} = u^{\langle p^i \rangle} = w.$$

So w is in $\mathrm{MS}_{\mathbb{F}_p,\lambda}(S)'$ since $u \in \mathrm{TEL}_2 \subseteq \mathrm{MS}_{\mathbb{F}_p,\lambda}(S)'$. Thus we have shown the surjectivity of ϕ.

To prove the injectivity, first note that, by Eq. (12), $w^{\diamond_\lambda p} = w$ for $w \in \mathrm{TEL}_1$. So the ideal $\langle \widehat{w}^p - \widehat{w} \mid \widehat{w} \in \widehat{\mathrm{TEL}_1}\rangle$ of $\mathbb{F}_p[\widehat{\mathrm{TEL}}]$ is in $\ker(\phi)$. Let

$$\Sigma = \{\sigma = (\sigma_1, \sigma_2) | \sigma_1 : \mathrm{TEL}_1 \to \{0, \cdots, p-1\}, \sigma_2 : \mathrm{TEL}_2 \to \mathbb{Z}_{\geqslant 0}, \text{both with finite supports}\}.$$

Then

$$\widehat{V} := \Big\{ \widehat{z}_\sigma := (\prod_{u\in \mathrm{TEL}_1} \widehat{u}^{\sigma_1(u)})(\prod_{v\in \mathrm{TEL}_2} \widehat{v}^{\sigma_2(v)}) \mid \sigma = (\sigma_1, \sigma_2) \in \Sigma \Big\}$$

is a $\mathbb{F}_p$-basis of $\mathbb{F}_p[\widehat{\mathrm{TEL}}]/\langle \widehat{w}^p - \widehat{w} \mid \widehat{w} \in \widehat{\mathrm{TEL}_1}\rangle$. Further,

$$V := \Big\{ z_\sigma := (\underset{u\in \mathrm{TEL}_1}{\diamond_\lambda} u^{\diamond_\lambda \sigma_1(u)}) \diamond_\lambda (\underset{v\in \mathrm{TEL}_2}{\diamond_\lambda} v^{\diamond_\lambda \sigma_2(v)}) \mid \sigma = (\sigma_1, \sigma_2) \in \Sigma \Big\}$$

is the image of $\widehat{V}$ under ϕ. Thus to prove the injectivity of ϕ we only need to show that V is linearly independent. For this we relate V to the linearly independent subset U defined in Eq. (15).

Let

$$\Gamma = \{\gamma : \mathrm{TL} \to \{0, \cdots, p-1\} \mid \gamma \text{ has finite support } \}.$$

Then we have

$$U = \{w_\gamma := \underset{w\in \mathrm{TL}}{\diamond_\lambda} w^{\diamond_\lambda \gamma(w)} \mid \gamma \in \Gamma\}.$$

We will construct a bijection between Σ and Γ. First note that $\mathrm{TL} = \mathrm{TL}_1 \coprod \mathrm{TL}_2 = \mathrm{TEL}_1 \coprod \mathrm{TL}_2$ by Eq. (31) and

$$\mathrm{TL}_2 = \{v^{\langle p^i\rangle} \mid v \in \mathrm{TEL}_2, i \geqslant 0\}$$

with all displayed elements distinct by Lemma 3.15. Thus we can define

$$\eta : \Sigma \to \Gamma, \quad \sigma \mapsto \gamma_\sigma, \sigma = (\sigma_1, \sigma_2) \in \Sigma$$

by first taking $\gamma_\sigma|_{\mathrm{TEL}_1} = \sigma_1$. Next for any $w = v^{\langle p^i\rangle} \in \mathrm{TL}_2$ with $v \in \mathrm{TEL}_2$, if $\sigma_2(v) = \sum\limits_{j=0}^{\infty} a_j p^j$ with $a_j \in \{0, \cdots, p-1\}$, we define $\gamma_\sigma(w) = a_i$. In the other direction, we define

$$\zeta : \Gamma \to \Sigma, \quad \gamma \mapsto \sigma_\gamma = (\sigma_1, \sigma_2)$$

as follows. If $u \in \mathrm{TEL}_1$, then define $\sigma_1(u) = \gamma(u)$. If $v \in \mathrm{TEL}_2$ then $v^{\langle p^i\rangle} \in \mathrm{TL}_2$ for all $i \geqslant 0$ and we define

$$\sigma_2(v) = \sum_{i=0}^{\infty} \gamma(v^{\langle p^i\rangle}) p^i.$$

¿From the constructions we see that η and ζ are inverse of each other.

Lemma 3.19. *We have $V = U$. More precisely, for any $\sigma \in \Sigma$, we have $z_\sigma = w_{\eta(\sigma)}$.*

Proof. For any $v \in \mathrm{TEL}_2$, by Eq. (12), we have

$$v^{\diamond_\lambda p^j} = \lambda^{j(\ell(v)-1)(p-1)} v^{\langle p^j\rangle} = v^{\langle p^j\rangle}.$$

If $\sigma_2(v) = \sum\limits_{j=0}^{\infty} a_{v,j} p^j$ with $a_{v,j} \in \{0, \cdots, p-1\}$, then

$$v^{\diamond_\lambda \sigma_2(v)} = \underset{j\geqslant 0}{\diamond_\lambda} (v^{\diamond_\lambda p^j})^{\diamond_\lambda a_{v,j}} = \underset{j\geqslant 0}{\diamond_\lambda} (v^{\langle p^j\rangle})^{\diamond_\lambda a_{v,j}}$$

and so

$$\begin{aligned} z_\sigma &= (\underset{u\in \mathrm{TEL}_1}{\diamond_\lambda} u^{\diamond_\lambda \sigma_1(u)}) \diamond_\lambda (\underset{v\in \mathrm{TEL}_2}{\diamond_\lambda} v^{\diamond_\lambda \sigma_2(v)}) \\ &= (\underset{u\in \mathrm{TEL}_1}{\diamond_\lambda} u^{\diamond_\lambda \sigma_1(u)}) \diamond_\lambda (\underset{v\in \mathrm{TEL}_2}{\diamond_\lambda} (v^{\langle p^j\rangle})^{\diamond_\lambda a_{v,j}}) \\ &= w_{\eta(\sigma)}. \end{aligned}$$

□

By Lemma 3.19 and Proposition 3.5.(b), V is linearly independent, as desired.

(b). Now we consider $S \in \mathcal{J}$. Define

$$\phi : \mathbb{F}_p[\widehat{\widetilde{\mathrm{TL}}}] \to \mathrm{MS}_{\mathbb{F}_p,\lambda}(S)$$

to be the natural algebra homomorphism in Definition 3.6 with $Y = \widetilde{\mathrm{TL}}$. Again let $\mathrm{MS}_{\mathbb{F}_p,\lambda}(S)'$ be the image.

We first prove that ϕ is onto. Applying Proposition 3.5.(a) to the semigroup S_1 and noting that $\mathrm{TL}_1 = \mathrm{TL}(S_1)$ by applying T to Eq. (32), we have $\mathrm{MS}_{\mathbb{F}_p,\lambda}(S_1) = \phi(\mathbb{F}_p[\widehat{\mathrm{TL}}_1])$ and hence is in $\mathrm{MS}_{\mathbb{F}_p,\lambda}(S)'$. Now for any $w \in \mathrm{TL}$, either $w \in \mathrm{TL}_1$ or $w = \tilde{w} + w^{\langle p\rangle}$ where $\tilde{w} = w - w^{\langle p\rangle} \in \widetilde{\mathrm{TL}}_2 \subseteq \mathrm{MS}_{\mathbb{F}_p,\lambda}(S)'$ and $w^{\langle p\rangle} \in \mathrm{MS}_{\mathbb{F}_p,\lambda}(S_1) = \phi(\mathbb{F}_p[\widehat{\mathrm{TL}}_1])$. Thus $w \in \mathrm{MS}_{\mathbb{F}_p,\lambda}(S)'$. Then the surjectivity follows from Proposition 3.5.(a).

For $w \in \mathrm{TL}$, define

$$\bar{w} := \begin{cases} w, & w \in \mathrm{TL}_1, \\ w - w^{\langle p\rangle}, & w \in \mathrm{TL}_2. \end{cases}$$

$$\overline{U} := \{1\} \cup \left\{ \bar{w}_1^{\diamond_\lambda i_1} \diamond_\lambda \cdots \diamond_\lambda \bar{w}_r^{\diamond_\lambda i_r} \mid w_i \in \mathrm{TL}, w_1 > \cdots > w_r, 1 \leqslant i_j \leqslant p-1, 1 \leqslant j \leqslant r, r \geqslant 1 \right\}.$$

To prove Eq. (36), we only need to show that $\overline{U}$ is linearly independent.

Recall that the set U in Eq. (15) is just

$$U = \{\ 1\} \cup \left\{ w_1^{\diamond_\lambda i_1} \diamond_\lambda \cdots \diamond_\lambda w_r^{\diamond_\lambda i_r} \mid w_i \in \mathrm{TL}, w_1 > \cdots > w_r, 1 \leqslant i_j \leqslant p-1, 1 \leqslant j \leqslant r, r \geqslant 1 \right\}.$$

By Eq. (20), in terms of the linear representation by the standard basis of pure tensors in $\mathrm{MS}_{\mathbb{F}_p,\lambda}(S)$,

$$w_1^{\diamond_\lambda i_1} \diamond_\lambda \cdots \diamond_\lambda w_r^{\diamond_\lambda i_r} = \mu w_1^{\otimes i_1} \otimes \cdots \otimes w_r^{\otimes i_r} + \text{lower L-order-terms}$$

where μ is a nonzero constant. Since $\bar{w}_i = w_i$ when $w_i \in \mathrm{TL}_1$ and $\bar{w}_i = w_i - w_i^{\langle p\rangle}$ and $w_i^{\langle p\rangle} <_{\mathrm{leng}} w_i$ when $w \in \mathrm{TL}_2$, we also have

$$\bar{w}_1^{\diamond_\lambda i_1} \diamond_\lambda \cdots \diamond_\lambda \bar{w}_r^{\diamond_\lambda i_r} = \mu\, w_1^{\otimes i_1} \otimes \cdots \otimes w_r^{\otimes i_r} + \text{lower L-order-terms}$$

for the same μ as in the last equation. It follows that $\overline{U}$ is linearly independent if and only if U is linearly independent which is Proposition 3.5.(b). □

3.3. **Free Rota-Baxter algebras with coefficients in $\mathbb{F}_p$.** We can now obtain a structure theorem on free commutative Rota-Baxter algebras by extracting information from the structure theorem on mixable shuffle algebras in Theorem 3.7, Theorem 3.17 and Corollary 3.18.

Theorem 3.20. *Let X be a finite ordered set. We will continue to use the $\widehat{\ }$-notation in Definition 3.6.*

(a) *Let $\lambda = 0$ and let $S = M^{\mathrm{c}}(X)$ be the commutative monoid generated by X. Let $\mathrm{TL} = \mathrm{T}(\mathrm{Lyn}(S))$ be defined in Eq. (14). Then*

$$\text{Ш}_{\mathbb{F}_p,\lambda}(\mathbb{F}_p[X]) \cong \mathbb{F}_p[X] \otimes \left(\mathbb{F}_p[\widehat{\mathrm{TL}}]/\langle \widehat{w}^p \mid \widehat{w} \in \widehat{\mathrm{TL}}\rangle\right).$$

(b) *Let $0 \neq \lambda \in \mathbb{F}_p$ and let $S = M^{\mathrm{c}}(X)$. Let TEL_2 be as defined in Eq. (30). Then*

$$\text{Ш}_{\mathbb{F}_p,\lambda}(\mathbb{F}_p[X]) \cong \mathbb{F}_p[X \cup \widehat{\mathrm{TEL}_2}] \otimes \left(\mathbb{F}_p[\widehat{W}]/\langle \widehat{w}^p - \widehat{w} \,|\, \widehat{w} \in \widehat{W}\rangle\right), \quad W = \{1^{\otimes p^i} \,|\, i \geqslant 0\}.$$

(c) *Let $A = \mathbb{F}_p[X]/\langle x^p - x \mid x \in X\rangle$ and $0 \neq \lambda \in \mathbb{F}_p$. Let $S \in \mathcal{P}$ be as defined in Eq. (39) in the proof. Let $\mathrm{TEL} = \mathrm{TEL}(S)$ be defined in Eq. (30). Then*

$$\text{Ш}_{\mathbb{F}_p,\lambda}(A) \cong \mathbb{F}_p[X \cup \widehat{\mathrm{TEL}}]/\langle \widehat{w}^p - \widehat{w} \mid \widehat{w} \in X \cup \widehat{\mathrm{TEL}}\rangle.$$

(d) *Let $A = \mathbb{F}_p[X]/\langle x^p - 1 \mid x \in X\rangle$ and $0 \neq \lambda \in \mathbb{F}_p$. Let $S \in \mathcal{J}$ be the abelian group $\mu_p^{|X|}$ where μ_p is the cyclic multiplicative group of order p. Let $\mathrm{TL}_1 = \mathrm{TL}_1(S)$ be as defined in Eq. (30) and let $\widetilde{\mathrm{TL}}_2 = \widetilde{\mathrm{TL}}_2(S)$ be as defined in Eq. (33). Then*

$$\begin{aligned}\text{Ш}_{\mathbb{F}_p,\lambda}(A) \;\cong\; & (\mathbb{F}_p[X]/\langle x^p - 1 \mid x \in X\rangle) \\ & \otimes \left(\mathbb{F}_p[\widehat{\mathrm{TL}_1}]/\langle w^p - w \mid w \in \widehat{\mathrm{TL}_1}\rangle\right) \otimes \left(\mathbb{F}_p[\widehat{\widetilde{\mathrm{TL}}_2}]/\langle w^p \mid w \in \widehat{\widetilde{\mathrm{TL}}_2}\rangle\right).\end{aligned}$$

Remark 3.21. The four cases in the theorem show quite distinct structures of free commutative Rota-Baxter algebras for different weights and generating algebras A. First of all, when the weight is zero, then the polynomial part of $\text{Ш}_{\mathbb{F}_p,0}(X)$ is $\mathbb{F}_p[X]$ itself. The second tensor factor (the shuffle algebra part) is completely nilpotent.

In the case of $\lambda \neq 0$, when $A = \mathbb{F}_p[X]$, $\text{Ш}_{\mathbb{F}_p,\lambda}(A)$ is basically a free (i.e., polynomial) $\mathbb{F}_p$-algebra except the subalgebra

$$\bigoplus_{k \geqslant 1} \mathbb{F}_p 1^{\otimes k} \cong \mathbb{F}_p[\widehat{W}]/\langle \widehat{w}^p - \widehat{w} \,|\, \widehat{w} \in \widehat{W}\rangle, \quad W = \{1^{\otimes p^i} \,|\, i \geqslant 0\}.$$

When $A = \mathbb{F}_p[x]/\langle x^p - x\rangle$, even though the corresponding free commutative Rota-Baxter algebra does not have any polynomial part, its structure reflects its base algebra in the sense that

$$\text{Ш}_{\mathbb{F}_p,\lambda}(A) \cong \mathbb{F}_p[\{x\} \cup \widehat{\mathrm{TEL}}]/\langle \widehat{w}^p - \widehat{w} \,|\, \widehat{w} \in \{x\} \cup \widehat{\mathrm{TEL}}\rangle \cong \bigotimes_{i \in \{x\} \cup \widehat{\mathrm{TEL}}} A_i, A_i \cong A, \forall i \in \{x\} \cup \widehat{\mathrm{TEL}},$$

is just a tensor product of copies of A. In this sense, when $A = \mathbb{F}_p[x]/\langle x^p - 1\rangle$, the structure of $\text{Ш}_{\mathbb{F}_p,\lambda}(A)$ has completely diverged from A since the only part of $\text{Ш}_{\mathbb{F}_p,\lambda}(A)$ that is isomorphic to A is the first tensor factor contributed from $\text{Ш}_{\mathbb{F}_p,\lambda}(A) = A \otimes \mathrm{MS}_{\mathbb{F}_p,\lambda}(A)$. Such diversities can be expected in other free commutative Rota-Baxter algebras.

Proof. We recall the tensor decomposition of the free commutative Rota-Baxter algebra on an algebra A in Eq. (6):

$$\text{Ш}_{\mathbb{F}_p,\lambda}(A) = A \otimes \mathrm{MS}_{\mathbb{F}_p,\lambda}(A).$$

Then Item (a) follows from Theorem 3.7. Item (b) follows from Corollary 3.18.

For (c), consider the cyclic group of order $p-1$, $\mu_{p-1}=\{\xi,\xi^2,\cdots,\xi^{p-1}\}$ where ξ^{p-1} is the identity. Define $G=\{e\}\cup\mu_{p-1}$ to be the monoid from the unitarization of μ_{p-1}. So the multiplication on G is extended from μ_{p-1} by

$$e\cdot e=e, e\cdot\xi^i=\xi^i=\xi^i\cdot e, 1\leqslant i\leqslant p-1.$$

It is clear that the algebra homomorphism

$$f:\mathbb{F}_p[x]\to\mathbb{F}_pG,\quad x\mapsto\xi$$

has $\langle x^p-x\rangle$ in its kernel. It is surjective since $f(x^i)=\xi^i$, $1\leqslant i\leqslant p-1$, and $f(1)=e$. Then $\mathbb{F}_p[x]/\langle x^p-x\rangle\cong\mathbb{F}_pG$ since both $\mathbb{F}_p$-algebras have the same dimension. Now G, and hence

$$S:=G^{|X|}, \tag{39}$$

are in the class $\mathcal{P}$. Then Item (c) follows from Theorem 3.17.(a).

Finally Item (d) follows from Theorem 3.17.(b). □

4. Structure theorems on $\mathbb{Z}_p$

We now lift our Theorem 3.17 for mixable shuffle algebras in Section 3 from $\mathbb{F}_p$ to $\mathbb{Z}_p$ by the Nakayama Lemma and a topological consideration. We then obtain a canonical polynomial algebra in the free commutative Rota-Baxter $\mathbb{Z}_p$-algebra generated by a finite set.

4.1. **Mixable shuffle algebras with coefficients in $\mathbb{Z}_p$.** We first recall notations and properties of graded sets and their polynomial algebras. Let $Y=\coprod_{n\geq1}Y^{(n)}$ be a graded set. We define the degree of $y\in Y^{(n)}$ by $\deg(y)=n$. Let $F(Y)$ be the free abelian semigroup generated by Y. For $y=y_1\cdots y_k\in F(Y)$ with $y_j\in Y, 1\leqslant j\leqslant k$, define $\deg(y)=\deg(y_1)+\cdots+\deg(y_k)$. In this way, the polynomial algebra $\mathbf{k}[Y]$ over a commutative ring $\mathbf{k}$ becomes a graded algebra: $\mathbf{k}[Y]=\oplus_{n\geq0}\mathbf{k}[Y]^{(n)}$.

Lemma 4.1. *Let $Y=\coprod_{n\geqslant0}Y^{(n)}$ be a graded set.*

(a) *For any $n\geq1$, as a $\mathbf{k}$-module,*

$$\mathbf{k}[Y]^{(n)}=(\sum_{j=1}^{n-1}\mathbf{k}[Y]^{(j)}\mathbf{k}[Y]^{(n-j)})\oplus\mathbf{k}Y^{(n)}.$$

(b) *Let $R=\oplus_{n\geqslant0}R^{(n)}$ be a graded algebra and let T be a graded subset of R. Let $\widehat{T}$ be a set that is in bijection with T and is equipped with the grading from T. Then the homomorphism $\phi:\mathbf{k}[\widehat{T}]\to R$ in Eq. (3.6) is a graded algebra homomorphism.*

Proof. (a). The degree on $F(Y)$ makes $F(Y)$ into a graded semigroup and $\mathbf{k}[Y]^{(n)}=\mathbf{k}F(Y)^{(n)}$. Then the lemma follows from the disjoint union decomposition

$$F(Y)^{(n)}=(\cup_{j=1}^{n-1}F(Y)^{(j)}F(Y)^{(n-j)})\coprod Y^{(n)}$$

of $F(Y)^{(n)}$ into elements of Y and elements which are products of at least two elements of Y.

(b) is the universal property of $\mathbf{k}[\widehat{T}]$ as the free commutative algebra generated by the graded set $\widehat{T}$ [32, Proposition 3.1]. To be explicit, ϕ preserves the gradings when it is restricted to

$\widehat{T}$. Since the grading on any graded algebra is multiplicative, the grading preserving map $\phi : \widehat{T} \to T$ extends to a grading preserving homomorphism $\phi : \mathbb{Q}[\widehat{T}] \to R$. □

Consider $S \in \mathcal{F}$, that is, S is a free abelian semigroup generated by an ordered finite set. We will continue to use the total degree on S defined in Proposition 3.9.(b). For a word $w = w_1 \otimes \cdots \otimes w_r \in S^{\otimes r} \subseteq \mathrm{MS}_{\mathbf{k},\lambda}(S)$, we define the degree of w by

$$\deg(w) = \deg(w_1) + \cdots + \deg(w_r). \tag{40}$$

Then $\mathrm{MS}_{\mathbb{Q},\lambda}(S)$ is a graded algebra by the same argument as that in [31, Theorem 2.1] where the case $\lambda = 1$ is considered. Note that

$$\deg(w^{\langle p \rangle}) = \deg(w^{\otimes p}) = p \deg(w). \tag{41}$$

Let $\mathrm{Lyn}^{(n)} = \mathrm{Lyn}(S)^{(n)}$ be the subset of Lyndon words on S of degree n. Since all elements in S have positive degrees, $\mathrm{Lyn}^{(n)}$ is finite for each $n \geqslant 1$. So we have a graded set $\mathrm{Lyn} = \coprod_{n \geqslant 1} \mathrm{Lyn}^{(n)}$ with each homogeneous component finite. By applying Lemma 4.1.(b), Theorem 2.3 has the following refined form.

Theorem 4.2. *Let S be in $\mathcal{F}$ and let λ be in $\mathbb{Q}$. Then the inclusion map $\mathrm{Lyn}(S) \subseteq \mathrm{MS}_{\mathbb{Q},\lambda}(S)$ induces an isomorphism $f : \mathbb{Q}[\mathrm{Lyn}(S)] \to \mathrm{MS}_{\mathbb{Q},\lambda}(S)$ of graded algebras. Here the grading on $\mathbb{Q}[\mathrm{Lyn}(S)]$ is given by the graded set $\mathrm{Lyn}(S)$.*

Now we consider $\mathrm{MS}_{\mathbb{Z}_p,\lambda}(S)$ defined over $\mathbb{Z}_p$.

Proposition 4.3. *Let λ be a unit in $\mathbb{Z}_p$. For S in $\mathcal{F}$ (resp. in $\mathcal{J}$) from Proposition 3.9 (resp. Definition 3.8), the natural homomorphism from Definition 3.6*

$$\phi : \mathbb{Z}_p[\widehat{\mathrm{TEL}}] \to \mathrm{MS}_{\mathbb{Z}_p,\lambda}(S), \quad \widehat{w} \mapsto w,$$

$$(\textit{resp.} \quad \phi : \mathbb{Z}_p[\widehat{\widetilde{\mathrm{TL}}}] \to \mathrm{MS}_{\mathbb{Z}_p,\lambda}(S), \quad \widehat{w} \mapsto w)$$

is surjective.

Proof. We first consider $S \in \mathcal{F}$. In this case S is the free abelian semigroup generated by a finite set. By Lemma 4.1.(b), ϕ is a homomorphism of graded algebras. Its reduction modulo p gives the graded algebra homomorphism

$$\bar{\phi} : \mathbb{F}_p[\widehat{\mathrm{TEL}}] \to \mathrm{MS}_{\mathbb{F}_p,\bar{\lambda}}(S).$$

Here $\bar{\lambda}$ is $\lambda \mod p$. By Theorem 3.17, $\bar{\phi}$ is an isomorphism. Therefore the map of $\mathbb{F}_p$-vector spaces

$$\bar{\phi}^{(n)} : \mathbb{F}_p[\widehat{\mathrm{TEL}}]^{(n)} \to \mathrm{MS}_{\mathbb{F}_p,\bar{\lambda}}(S)^{(n)}$$

is isomorphic and in particular is surjective. Since for $S \in \mathcal{F}$, the number of elements of fixed degree is finite, the number of words from S of fixed degree is finite. Thus both $\mathbb{Z}_p[\widehat{\mathrm{TEL}}]^{(n)}$ and $\mathrm{MS}_{\mathbb{F}_p,\lambda}(S)^{(n)}$ are of finite rank over $\mathbb{Z}_p$. Then by Nakayama Lemma the map

$$\phi^{(n)} : \mathbb{Z}_p[\widehat{\mathrm{TEL}}]^{(n)} \to \mathrm{MS}_{\mathbb{F}_p,\lambda}(S)^{(n)}$$

is surjective. This implies that ϕ is surjective for $S \in \mathcal{F}$.

We next consider the case of $S \in \mathcal{J}$. Applying Proposition 3.5.(a) to the semigroup S_1 and noting that $\mathrm{TL}_1 = \mathrm{TL}(S_1)$ by applying T to Eq. (32), we have $\mathrm{MS}_{\mathbb{Z}_p,\lambda}(S_1) = \phi(\mathbb{Z}_p[\widehat{\mathrm{TL}}_1])$ and hence is in $\mathrm{MS}_{\mathbb{Z}_p,\lambda}(S)'$. Now for any $w \in \mathrm{TL}$, either $w \in \mathrm{TL}_1$ or $w = \tilde{w} + w^{\langle p \rangle}$

where $\tilde{w} = w - w^{\langle p\rangle} \in \widetilde{\mathrm{TL}}_2 \subseteq \mathrm{MS}_{\mathbb{Z}_p,\lambda}(S)'$ and $w^{\langle p\rangle} \in \mathrm{MS}_{\mathbb{Z}_p,\lambda}(S_1) = \phi(\mathbb{Z}_p[\widehat{\mathrm{TL}}_1])$. Thus $w \in \mathrm{MS}_{\mathbb{Z}_p,\lambda}(S)'$. Then the surjectivity follows from Proposition 3.5.(a). □

For $S \in \mathcal{J}$, let $\widehat{v} \in \widehat{\mathrm{TL}}_1$ and $\widehat{w} \in \widehat{\widetilde{\mathrm{TL}}}_2$. Then by Theorem 3.17 we have

$$\phi(\widehat{v})^{\diamond_{\lambda p}}, \phi(\widehat{w})^{\diamond_{\lambda p}} - \phi(\widehat{w}) \in p\mathrm{MS}_{\mathbb{Z}_p,\lambda}(S).$$

By Proposition 4.3 there are polynomials Q'_v and Q'_w in $\mathbb{Z}_p[\widehat{\widetilde{\mathrm{TL}}}]$ such that

$$\phi(\widehat{v})^{\diamond_{\lambda p}} = p\phi(Q'_v) \quad \phi(\widehat{w})^{\diamond_{\lambda p}} - \phi(\widehat{w}) = p\phi(Q'_w).$$

Thus

$$Q_v := \widehat{v}^p - pQ'_v, \quad Q_w := \widehat{w}^p - \widehat{w} - pQ'_w$$

are in $\ker\phi$. Let I be the ideal of $\mathbb{Z}_p[\widehat{\widetilde{\mathrm{TL}}}]$ generated by the Q_v's and Q_w's. Then $I \subseteq \ker\phi$. Let $\bar{I}$ be the closure of I in $\mathbb{Z}_p[\widehat{\widetilde{\mathrm{TL}}}]$ with respect to the p-adic topology, that is,

$$\bar{I} = \bigcap_{n\geqslant 0}(I + p^n\mathbb{Z}_p[\widehat{\widetilde{\mathrm{TL}}}]).$$

Then the modula $\mathbb{Z}_p[\widehat{\widetilde{\mathrm{TL}}}]/\bar{I}$ is **separated with the p-adic topology**, i.e.

$$\bigcap_{n\geqslant 0} p^n(\mathbb{Z}_p[\widehat{\widetilde{\mathrm{TL}}}]/\bar{I}) = 0.$$

Because $\bar{I} \subset I + p^n\mathbb{Z}_p[\widehat{\widetilde{\mathrm{TL}}}], n \geqslant 0$, we have

$$\phi(\bar{I}) \subseteq p^n\mathrm{MS}_{\mathbb{Z}_p,\lambda}(S).$$

So $\phi(\bar{I}) \subseteq \bigcap_{n\geqslant 0} p^n\mathrm{MS}_{\mathbb{Z}_p,\lambda}(S)$. Since $\mathrm{MS}_{\mathbb{Z}_p,\lambda}(S)$ is a free $\mathbb{Z}_p$-module, we have $\bigcap_{n\geqslant 0} p^n\mathrm{MS}_{\mathbb{Z}_p,\lambda}(S) = 0$. Hence $\phi(\bar{I}) = 0$. Thus ϕ induces a homomorphism

$$\mathbb{Z}_p[\widehat{\widetilde{\mathrm{TL}}}]/\bar{I} \to \mathrm{MS}_{\mathbb{Z}_p,\lambda}(S),$$

which is again denoted by ϕ. We give a lemma before presenting our main theorem in this section.

Lemma 4.4. *Let M be a $\mathbb{Z}_p$-module that is separated for the p-adic topology and let N be a torsion-free $\mathbb{Z}_p$-module. Let $f : M \to N$ be a homomorphism of $\mathbb{Z}_p$-modules. If the induced homomorphism*

$$\bar{f} : M \otimes \mathbb{F}_p \to N \otimes \mathbb{F}_p$$

is injective, then f is also injective.

Proof. Let $m \in \ker(f)$. We prove $m = 0$. Since $\bar{f}$ is an isomorphism, we have $m \in pM$. Write $m = pm_1$. Then $f(pm_1) = pf(m_1) = 0$. Since N is torsion-free, we get $f(m_1) = 0$. So we have $m_1 \in pM$ and $m \in p^2M$. An inductive argument shows that $m \in \bigcap_{n\geqslant 0} p^nM$. Then the condition that M is separated for the p-adic topology implies that $m = 0$. □

Theorem 4.5. *Let $\lambda \in \mathbb{Z}_p$ be a p-adic unit.*

(a) *For $S \in \mathcal{F}$, the natural homomorphism*

$$\phi : \mathbb{Z}_p[\widehat{\mathrm{TEL}}] \to \mathrm{MS}_{\mathbb{Z}_p,\lambda}(S)$$

is an isomorphism of graded $\mathbb{Z}_p$-algebras. In other words, $\mathrm{MS}_{\mathbb{Z}_p,\lambda}(S) = \mathbb{Z}_p[\mathrm{TEL}]$. In particular, there is a natural isomorphism

$$\mathbb{Z}_p\mathrm{TEL}^{(n)} \cong \mathrm{MS}_{\mathbb{Z}_p,\lambda}(S)^{(n)} / \Big(\sum_{i=1}^{n-1} \mathrm{MS}_{\mathbb{Z}_p,\lambda}(S)^{(i)} \mathrm{MS}_{\mathbb{Z}_p,\lambda}(S)^{(n-i)} \Big). \tag{42}$$

Further, the homogeneous component $\mathrm{TEL}^{(n)}$ of TEL of degree n has cardinality $|\mathrm{Lyn}(S)^{(n)}|$, $n \geqslant 1$.

(b) *For a semigroup $S \in \mathcal{J}$, the natural homomorphism*

$$\phi : \mathbb{Z}_p[\widehat{\widetilde{\mathrm{TL}}}]/\bar{I} \to \mathrm{MS}_{\mathbb{Z}_p,\lambda}(S)$$

is an isomorphism.

Proof. Let $S \in \mathcal{F}$ or $\mathcal{J}$. By Proposition 4.3, ϕ is surjective. By Theorem 3.17, $\phi \otimes \mathbb{F}_p$ is an isomorphism. Note that for $S \in \mathcal{F}$ (resp. $S \in \mathcal{J}$), $\mathbb{Z}_p[\widehat{\mathrm{TEL}}]$ (resp. $\mathbb{Z}_p[\widehat{\widetilde{\mathrm{TL}}}]/\bar{I}$) is a $\mathbb{Z}_p$-module separated for the p-adic topology and that $\mathrm{MS}_{\mathbb{Z}_p,\lambda}(S)$ is a free $\mathbb{Z}_p$-module. Applying Lemma 4.4 with $M = \mathbb{Z}_p[\widehat{\mathrm{TEL}}]$ (resp. $M = \mathbb{Z}_p[\widehat{\widetilde{\mathrm{TL}}}]/\bar{I}$) and $N = \mathrm{MS}_{\mathbb{Z}_p,\lambda}(S)$ we obtain the injectivity of ϕ.

This proves Item (b) and a part of Item (a). To finish the proof of Item (a), let $S \in \mathcal{F}$. By Lemma 4.1.(b), the algebra isomorphism ϕ is graded. Since the grading on $\widehat{\mathrm{TEL}}$ is obtained from TEL, $\mathrm{MS}_{\mathbb{Z}_p,\lambda}(S) = \mathbb{Z}_p[\mathrm{TEL}]$ as a graded algebra. Thus $\mathrm{MS}_{\mathbb{Z}_p,\lambda}(S)^{(n)} = \mathbb{Z}_p[\mathrm{TEL}]^{(n)}, n \geqslant 0$. So by Lemma 4.1.(a) we have

$$\begin{aligned} \mathbb{Z}_p\mathrm{TEL}^{(n)} &\cong \mathbb{Z}_p[\mathrm{TEL}]^{(n)} / \Big(\sum_{i=1}^{n-1} \mathbb{Z}_p[\mathrm{TEL}]^{(i)} \mathbb{Z}_p[\mathrm{TEL}]^{(n-i)} \Big) \\ &= \mathrm{MS}_{\mathbb{Z}_p,\lambda}(S)^{(n)} / \Big(\sum_{i=1}^{n-1} \mathrm{MS}_{\mathbb{Z}_p,\lambda}(S)^{(i)} \mathrm{MS}_{\mathbb{Z}_p,\lambda}(S)^{(n-i)} \Big). \end{aligned}$$

Since

$$\mathrm{TEL} = \{u^{\otimes p^i} \mid u \in \mathrm{EL}, i \geqslant 0\}, \quad \mathrm{Lyn} = \{u^{\langle p^i \rangle} \mid u \in \mathrm{EL}, i \geqslant 0\}$$

by Lemma 3.11.(c), and

$$\deg(u^{\otimes p^i}) = p^i \deg(u) = \deg(u^{\langle p^i \rangle})$$

by Eq. (41), we have $|\mathrm{TEL}^{(n)}| = |\mathrm{Lyn}^{(n)}|$. □

4.2. **Free Rota-Baxter algebras with coefficients in $\mathbb{Z}_p$.**

Theorem 4.6. *Let X be a finite set and let S be the free abelian semigroup generated by X. Let $\mathrm{TEL} = \mathrm{TEL}(S)$. Let $\lambda \in \mathbb{Z}_p$ be a p-adic unit. Then there is a canonical subalgebra of $\text{Ш}_{\mathbb{Z}_p,\lambda}(\mathbb{Z}_p[X])$ that is isomorphic to $\mathbb{Z}_p[X \cup \widehat{\mathrm{TEL}}]$.*

Proof. By Theorem 4.5, $\mathrm{MS}_{\mathbb{Z}_p,\lambda}(S) \cong \mathbb{Z}_p[\widehat{\mathrm{TEL}}]$. The inclusion of S into the free abelian monoid $M^{\mathrm{c}}(X)$ induces the inclusion $\mathrm{MS}_{\mathbb{Z}_p,\lambda}(S) \subseteq \mathrm{MS}_{\mathbb{Z}_p,\lambda}(M^{\mathrm{c}}(X))$. Then we have

$$\begin{aligned}\mathbb{Z}_p[X \cup \widehat{\mathrm{TEL}}] &\cong \mathbb{Z}_p[X] \otimes \mathbb{Z}_p[\widehat{\mathrm{TEL}}] \cong \mathbb{Z}_p[X] \otimes \mathrm{MS}_{\mathbb{Z}_p,\lambda}(S)\\ &\subseteq \mathbb{Z}_p[X] \otimes \mathrm{MS}_{\mathbb{Z}_p,\lambda}(M^{\mathrm{c}}(X)) = Ш_{\mathbb{Z}_p,\lambda}(\mathbb{Z}_p[X]).\end{aligned}$$

□

5. Structure theorems on $\mathbb{Z}$

We now study mixable shuffle algebras with coefficients in $\mathbb{Z}$ by generalizing the work of Hazewinkel [28] on the Ditters Conjecture (Theorem 2.2.(c). We first extract from his proof a general principle (Theorem 5.2) showing that a compatible system of local polynomial conditions implies a global one. This result will then be combined with our result on the local case in Section 4 and be applied to mixable shuffle algebras and free commutative Rota-Baxter algebras.

5.1. **Mixable shuffle algebras with coefficients in $\mathbb{Z}$.** The following lemma is well-known but we include a short proof for the lack of references.

Lemma 5.1. (a) *A finitely generated abelian group M is free of rank k if $M \otimes \mathbb{Z}_p \cong \mathbb{Z}_p^k$ for all prime numbers p.*

(b) *A homomorphism of finitely generated free abelian groups $f : M_1 \to M_2$ is injective and identifies M_1 with a direct summand of M_2 if for every prime p, the homomorphism $f \otimes \mathbb{Z}_p : M_1 \otimes \mathbb{Z}_p \to M_2 \otimes \mathbb{Z}_p$ is injective and identifies $M_1 \otimes \mathbb{Z}_p$ with a direct summand of $M_2 \otimes \mathbb{Z}_p$ as a $\mathbb{Z}_p$-module.*

Proof. (a) follows from the fundamental theorem of finitely generated abelian groups.

(b). Since $f \otimes \mathbb{Z}_p$ is injective, $\ker(f \otimes \mathbb{Z}_p) = \ker(f) \otimes \mathbb{Z}_p$ is the free $\mathbb{Z}_p$-module of rank 0. Thus by Item (a), $\ker f$ is the free abelian group of rank 0, so is 0. Since $(f \otimes \mathbb{Z}_p)(M_1 \otimes \mathbb{Z}_p)$ is a direct summand of the free $\mathbb{Z}_p$-module $M_2 \otimes \mathbb{Z}_p$, the quotient $(M_2 \otimes \mathbb{Z}_p)/(f \otimes \mathbb{Z}_p)(M_1 \otimes \mathbb{Z}_p) = (M_2/f(M_1)) \otimes \mathbb{Z}_p$ is a free $\mathbb{Z}_p$-module whose $\mathbb{Z}_p$-rank is

$$\mathrm{rank}_{\mathbb{Z}_p}(M_2 \otimes \mathbb{Z}_p) - \mathrm{rank}_{\mathbb{Z}_p}(M_1 \otimes \mathbb{Z}_p) = \mathrm{rank}_{\mathbb{Z}}(M_2) - \mathrm{rank}_{\mathbb{Z}}(M_1).$$

So by Item (a), $M_2/f(M_1)$ is free. Therefore, $f(M_1)$ is a direct summand of M_2. □

In the following theorem, we denote $\mathrm{Spec}(\mathbb{Z}) = \{0\} \cup \{p \mid p \text{ a prime of } \mathbb{Z}\}$. Also denote $\mathbb{Z}_0 = \mathbb{Q}$ for ease of notations.

Theorem 5.2. *Let $R = \oplus_{n \geqslant 0} R^{(n)}$ be a commutative graded $\mathbb{Z}$-algebra with each homogenous piece $R^{(n)}$ a free $\mathbb{Z}$-module. Suppose that, for each $\ell \in \mathrm{Spec}(\mathbb{Z})$, there exists a graded subset $Y_\ell = \coprod_{n \geqslant 1} Y_\ell^{(n)}$ of $R \otimes \mathbb{Z}_\ell$ with the following properties.*

(a) *For a fixed $n \geq 0$, $|Y_\ell^{(n)}|$ is finite with the same cardinality when $\ell \in \mathrm{Spec}(\mathbb{Z})$ varies;*

(b) *For every $\ell \in \mathrm{Spec}(\mathbb{Z})$, $R \otimes \mathbb{Z}_\ell = \mathbb{Z}_\ell[Y_\ell]$ as a graded $\mathbb{Z}_\ell$-algebra.*

Then there is a graded subset $Y = \coprod_{n \geq 0} Y^{(n)}$ of R such that

(i) *$|Y^{(n)}| = |Y_0^{(n)}|$ for all $n \geqslant 0$;*

(ii) *$R \cong \mathbb{Z}[Y]$ as a graded algebra.*

Proof. Fix $n \geq 1$. Consider the right exact sequence

$$\bigoplus_{j=1}^{n-1}(R^{(j)} \otimes R^{(n-j)}) \xrightarrow{\mu_n} R^{(n)} \xrightarrow{\pi_n} G^{(n)} \to 0 \tag{43}$$

where μ_n is the multiplication map and $G^{(n)}$ is the cokernel of μ_n. For any $\ell \in \mathrm{Spec}(\mathbb{Z})$, by Property (b) and the right exactness of tensoring with $\mathbb{Z}_\ell$, we obtain the right exact sequence

$$\bigoplus_{j=1}^{n-1}(\mathbb{Z}_\ell[Y_\ell]^{(j)} \otimes \mathbb{Z}_\ell[Y_\ell]^{(n-j)}) \xrightarrow{\mu_{n,\ell}} \mathbb{Z}_\ell[Y_\ell]^{(n)} \xrightarrow{\pi_{\ell,n}} G^{(n)} \otimes \mathbb{Z}_\ell \to 0, \tag{44}$$

where $\mu_{n,\ell}$ is again the multiplication map. By Lemma 4.1.(a) we get $\mathbb{Z}_\ell[Y_\ell]^{(n)} = \mathrm{im}(\mu_{n,\ell}) \oplus \mathbb{Z}_\ell Y_\ell^{(n)}$. Thus $G^{(n)} \otimes \mathbb{Z}_\ell \cong \mathbb{Z}_\ell^{|Y_\ell^{(n)}|}$ is a free $\mathbb{Z}_\ell$-module. By Property (a) and Lemma 5.1.(a), $G^{(n)}$ is a free abelian group of rank $|Y_\ell^{(n)}|$. Thus the right exact sequence in Eq. (43) splits and we have $R^{(n)} = \mathrm{im}(\mu_n) \oplus R^{(n)\prime}$ for a free abelian group $R^{(n)\prime} \subseteq R^{(n)}$ of rank $|Y_\ell^{(n)}|$ such that $R^{(n)\prime} \cong G^{(n)}$ under π_n. Let $Y^{(n)}$ be a $\mathbb{Z}$-basis of $R^{(n)\prime}$, $n \geqslant 1$, and let $Y = \cup_{n\geqslant 1} Y^{(n)}$. Let R'' be the subalgebra of R generated by Y and let $R^{(n)\prime\prime} = R'' \cap R^{(n)}, n \geqslant 1$. Let $W = \coprod_{n\geq 1} W^{(n)}$ be a graded set such that $W^{(n)}$ is in bijection with $Y^{(n)}$ through a map $\tau_n : W^{(n)} \to Y^{(n)}$. Define the $\mathbb{Z}$-algebra homomorphism

$$\alpha : \mathbb{Z}[W] \to R, \quad w \mapsto \tau_n(w), w \in W^{(n)}, n \geq 1.$$

It is a graded algebra homomorphism since it is defined piece by piece on each homogeneous subgroup. We have $R'' = \mathrm{im}(\alpha)$.

We next prove $R'' = R$ by claiming that $R^{(n)} \subseteq R''$ for all $n \geq 1$ by induction on n. When $n = 1$, $R^{(1)} = \mathbb{Z}Y^{(1)}$, so the claim is clear. Suppose $R^{(k)} \subseteq R''$ for $k < n$. Then since

$$R^{(n)} = \mathrm{im}(\mu_n) + \mathbb{Z}Y^{(n)} = \big(\sum_{j=1}^{n-1} R^{(j)}R^{(n-j)}\big) + \mathbb{Z}Y^{(n)},$$

we again have $R^{(n)} \subseteq R''$ by the induction hypothesis. Therefore α is a surjective homomorphism of graded algebras. Thus α restricts to give a surjection

$$\alpha_n : \mathbb{Z}[W]^{(n)} \to R^{(n)}$$

for any $n \geq 1$.

For each $n \geqslant 1$, $W^{(n)}$ is in bijection with $Y^{(n)}$. Also $Y^{(n)}$, as a $\mathbb{Z}$-basis of $R^{(n)\prime}$ of rank $|Y_0^{(n)}|$, is in bijection with $Y_0^{(n)}$. So $W \cong Y_0$ as graded sets and $\mathbb{Q}[W] \cong \mathbb{Q}[Y_0]$ as graded algebras. Hence $\mathbb{Q}[Y_0]^{(n)}$ has the same $\mathbb{Q}$-dimension as that of $\mathbb{Q}[W]^{(n)}$. Also by Property (b), $R^{(n)} \otimes \mathbb{Q}$ has the same $\mathbb{Q}$-dimension as that of $\mathbb{Q}[Y_0]^{(n)}$. Therefore $R^{(n)} \otimes \mathbb{Q}$ and $\mathbb{Q}[W]^{(n)}$ have the same $\mathbb{Q}$-dimension. Thus the free abelian groups $R^{(n)}$ and $\mathbb{Z}[W]^{(n)}$ have the same rank. Thus α_n is an isomorphism for every $n \geq 1$ and hence α is an isomorphism. □

Theorem 5.3. *Let S be a finitely generated free abelian semigroup. Then for $\lambda = \pm 1$, $\mathrm{MS}_{\mathbb{Z},\lambda}(S)$ is a polynomial algebra $\mathbb{Z}[Y]$, where $Y = \coprod_{n\geqslant 1} Y^{(n)}$ is a graded set whose homogeneous component $Y^{(n)}$ has cardinality $|\mathrm{Lyn}(S)^{(n)}|$. Here $\mathrm{Lyn}(S)^{(n)}$ is the set of Lyndon words on S of degree n.*

Proof. We apply Theorem 5.2 to the graded algebra $R = \mathrm{MS}_{\mathbb{Z},\lambda}(S)$ where the grading is defined by the degree on words in Eq.(40). For $\ell \in \mathrm{Spec}(\mathbb{Z})$, define

$$Y_\ell = \begin{cases} \mathrm{Lyn}(S), & \ell = 0, \\ \mathrm{TEL}(S)(\ell), & \ell \neq 0. \end{cases}$$

with their grading restricted from $\mathrm{MS}_{\mathbb{Z},\lambda}(S)$. Then by Theorem 4.2, $R \otimes \mathbb{Q} \cong \mathbb{Q}[Y_0]$ as graded algebras. By Theorem 4.5, for $\ell \neq 0$, $R \otimes \mathbb{Z}_\ell = \mathbb{Z}_\ell[Y_\ell]$ as graded algebras. Further, by Theorem 4.5.(a) and its proof, $|Y_\ell^{(n)}| = |Y_0^{(n)}|, n \geqslant 1$. Then our proof is completed by Theorem 5.2. □

5.2. **Weight λ mixable shuffle algebras for countably generated free abelian semigroups.** We now extend Theorem 5.3 to the countably infinite generators.

Theorem 5.4. *Let X be a countable set. Let $F(X)$ be the free abelian semigroup generated by X. Then the algebra $\mathrm{MS}_{\mathbb{Z},\lambda}(F(X))$, $\lambda = \pm 1$, is a polynomial $\mathbb{Z}$-algebra.*

Proof. We denote $S = F(X)$ in this proof. First we fix an order on X such that $X = \{x_1, x_2, x_3, \cdots\}$ with $x_1 < x_2 < x_3 < \cdots$. Then we define a degree and an order on S as before. For every $k \geqslant 1$ we write $X_k = \{x_1, \cdots, x_k\}$ and let S_k be the free abelian semigroup generated by X_k that can be considered as a subgroup of S. Then we form a direct system $\{\mathrm{MS}_{\mathbb{Z},\lambda}(S_k)\}_{k\geqslant 1}$ and we have

$$\mathrm{MS}_{\mathbb{Z},\lambda}(S) = \varinjlim \mathrm{MS}_{\mathbb{Z},\lambda}(S_k).$$

By Theorem 5.3 for every $k \geqslant 1$, $\mathrm{MS}_{\mathbb{Z},\lambda}(S_k)$ is a graded polynomial algebra

$$\mathrm{MS}_{\mathbb{Z},\lambda}(S_k) = \mathbb{Z}\Big[\coprod_{n\geqslant 1} Y_k^{(n)}\Big], \tag{45}$$

where $Y_k^{(n)}$ is a lifting of a basis of the quotient

$$G_k^{(n)} = \mathrm{MS}_{\mathbb{Z},\lambda}(S_k)^{(n)} / \sum_{1\leqslant i<n} \mathrm{MS}_{\mathbb{Z},\lambda}(S_k)^{(i)} \mathrm{MS}_{\mathbb{Z},\lambda}(S_k)^{(n-i)}$$

to $\mathrm{MS}_{\mathbb{Z},\lambda}(S_k)^{(n)}$. Let $\pi_k^{(n)}$ denote the quotient map

$$\mathrm{MS}_{\mathbb{Z},\lambda}(S_k)^{(n)} \to G_k^{(n)}.$$

For our purpose we need to choose a special lifting $Y_k^{(n)}$ so that $\{Y_k^{(n)}\}_{k\geqslant 1}$ form an increasing sequence of subsets for every fixed n. For this we need the following lemma.

Lemma 5.5. *For $n, k \geqslant 1$, $G_k^{(n)}$ is a direct summand of $G_{k+1}^{(n)}$.*

Proof. For a fixed prime ℓ, we have the following commutative diagram

$$\begin{array}{ccc} \mathbb{Z}_\ell \mathrm{TEL}(\ell)(S_k)^{(n)} & \longrightarrow & \mathbb{Z}_\ell \mathrm{TEL}(\ell)(S_{k+1})^{(n)} \\ \Big\downarrow{\scriptstyle \pi^n_{\ell,k}}\simeq & & \Big\downarrow{\scriptstyle \pi^n_{\ell,k+1}}\simeq \\ G_k^{(n)} \otimes \mathbb{Z}_\ell & \longrightarrow & G_{k+1}^{(n)} \otimes \mathbb{Z}_\ell. \end{array}$$

The two vertical reduction maps are isomorphisms by Eq. (42). The homomorphism in the top row of the above diagram is induced by the inclusion of sets

$$\mathrm{TEL}(\ell)(S_k)^{(n)} \to \mathrm{TEL}(\ell)(S_{k+1})^{(n)}$$

and hence is injective and identifies the source with a direct summand of the target. Then the homomorphism $G_k^{(n)} \otimes \mathbb{Z}_\ell \to G_{k+1}^{(n)} \otimes \mathbb{Z}_\ell$ in the bottom row is also injective and identifies $G_k^{(n)} \otimes \mathbb{Z}_\ell$ with a direct summand of $G_{k+1}^{(n)} \otimes \mathbb{Z}_\ell$. By Lemma 5.1.(b) we obtain the lemma. □

Now we choose our $Y_k^{(n)}$ by induction on $k \geqslant 1$. We first fix a lifting $Y_1^{(n)}$. For a given $k \geqslant 1$, suppose we have chosen $Y_k^{(n)}$. Then $\pi_k^{(n)}(Y_k^{(n)})$ is a basis of $G_k^{(n)}$. By Lemma 5.5, $G_k^{(n)}$ is a direct summand of $G_{k+1}^{(n)}$. In other words, we may write

$$G_{k+1}^{(n)} = G_k^{(n)} \oplus G_{k+1}^{\prime(n)}.$$

Then $G_{k+1}^{\prime(n)}$ is a free abelian group and let $B_{k+1}^{\prime(n)}$ be a basis of $G_{k+1}^{\prime(n)}$. Let $Y_{k+1}^{\prime(n)}$ be a lifting of $B_{k+1}^{\prime(n)}$ to $\mathrm{MS}_{\mathbb{Z}_p,\lambda}(S_{k+1})^{(n)}$. Then we can define $Y_{k+1}^{(n)}$ to be the disjoint union $Y_k^{(n)} \coprod Y_{k+1}^{\prime(n)}$ since $\pi_{k+1}^{(n)}(Y_k^{(n)} \coprod Y_{k+1}^{\prime(n)})$ is a basis of the free abelian group $G_{k+1}^{(n)}$. This completes the induction.

Let

$$Y_k = \coprod_{n \geqslant 1} Y_k^{(n)}.$$

Then Y_k is a subset of Y_{k+1}. From the construction and Eq. (45) we obtain

$$\mathrm{MS}_{\mathbb{Z},\lambda}(S_k) = \mathbb{Z}[Y_k].$$

Therefore

$$\mathrm{MS}_{\mathbb{Z},\lambda}(S) = \varinjlim \mathrm{MS}_{\mathbb{Z},\lambda}(S_k) = \varinjlim \mathbb{Z}[Y_k] = \mathbb{Z}[\cup_{k \geqslant 1} Y_k]$$

is a polynomial $\mathbb{Z}$-algebra, as expected. □

5.3. **Free commutative Rota-Baxter algebras with coefficients in $\mathbb{Z}$.**

Theorem 5.6. *Let X be a at most countably many set. Let $F(X)$ be the free abelian semigroup generated by X. Let $\lambda = \pm 1$. Then there is a set Ω of variables such that*

$$\text{Ш}_{\mathbb{Z},\lambda}(\mathbb{Z}[X]) \cong \mathbb{Z}[\Omega] \oplus N \tag{46}$$

where $N = N_S$ is the subgroup of $\text{Ш}_{\mathbb{Z},\lambda}(\mathbb{Z}[X])$ spanned by pure tensors of the form

$$w_0 \otimes \cdots \otimes w_r, w_i \in \{1\} \cup F(X), 1 \leqslant i \leqslant r, w_i = 1 \text{ for some } 1 \leqslant i \leqslant r, r \geqslant 1.$$

When X is finite. Then $\Omega = X \cup Y$, where Y is a graded set in bijection with the graded set $\mathrm{Lyn}(F(X))$ of Lyndon words.

Proof. By Theorem 5.3 and Theorem 5.4, $\mathrm{MS}_{\mathbb{Z},\lambda}(F(X)) = \mathbb{Z}_p[Y]$ for a set Y of variables. Let $M^{\mathrm{c}}(X)$ be the free commutative monoid generated by X. Then $M^{\mathrm{c}}(X) = \{1\} \cup F(X)$. So a word in $\mathrm{MS}_{\mathbb{Z},\lambda}(M^{\mathrm{c}}(X))$ is of the form $w = w_1 \otimes \cdots \otimes w_r$ where either each w_i is in $F(X)$ or at least one of w_i is 1. A word w is in $\mathrm{MS}_{\mathbb{Z},\lambda}(F(X))$ precisely when it is of the first form. We denote N^+ to be the subgroup of $\mathrm{MS}_{\mathbb{Z},\lambda}(M^{\mathrm{c}}(X))$ generated by elements of the second form. Then we have

$$\mathrm{MS}_{\mathbb{Z},\lambda}(M^{\mathrm{c}}(X)) = \mathrm{MS}_{\mathbb{Z},\lambda}(F(X)) \oplus N^+ \cong \mathbb{Z}[Y] \oplus N^+.$$

Since $\mathbb{Z}[X] = \mathbb{Z}M^{\mathrm{c}}(X)$, we have

$$\begin{aligned} Ш_{\mathbb{Z},\lambda}(\mathbb{Z}[X]) &= \mathbb{Z}[X] \otimes \mathrm{MS}_{\mathbb{Z},\lambda}(M^{\mathrm{c}}(X)) \cong \mathbb{Z}[X] \otimes (\mathrm{MS}_{\mathbb{Z},\lambda}(F(X)) \oplus N^+) \\ &\cong \mathbb{Z}[X] \otimes (\mathbb{Z}[Y] \oplus N^+) \cong \mathbb{Z}[X \cup Y] \oplus (\mathbb{Z}[X] \otimes N^+). \end{aligned}$$

Then we just need to take $\Omega = X \cup Y$ and $N = \mathbb{Z}[X] \otimes N^+$ to get the direct sum decomposition in Eq. (46).

When X is finite, by Theorem 4.5, we have Y in the specified form as prescribed. □

As a final note, we elaborate on the significance of Theorem 5.6. By Theorem 2.4, $Ш_{\mathbb{Q},\lambda}(A(X))$ is a polynomial $\mathbb{Q}$-algebra generated by $\overline{\mathrm{Lyn}}(X) := X \cup \{1 \otimes w \mid w \in \mathrm{Lyn}(M^{\mathrm{c}}(X))\}$. Since $\overline{\mathrm{Lyn}}(X)$ is a part of a $\mathbb{Z}$-basis of $Ш_{\mathbb{Z},\lambda}(A(X))$, it follows that $\overline{\mathrm{Lyn}}(X)$ generates a polynomial $\mathbb{Z}$-subalgebra of $Ш_{\mathbb{Z},\lambda}(A(X))$. There is no inclusion relation between the polynomial generating set Y in Theorem 5.6 and $\overline{\mathrm{Lyn}}(X)$ in Theorem 2.4 since Y is not the set of Lyndon words, only in bijection with this set. However, the polynomial subalgebra $\mathbb{Z}[X \cup Y]$ in Theorem 5.6 can be more useful in studying the structure of $Ш_{\mathbb{Z},\lambda}(A(X))$ because of the direct sum decomposition in Eq. (46). This is similar to the importance of studying direct summands of abelian groups. It is easy to obtain free subgroups in a torsion-free abelian group, such as $\mathbb{Q}$, but it is more useful to obtain a direct summand that is free. Similarly, there are many polynomial subalgebras in a free commutative Rota-Baxter algebra $Ш(A)$, but it is more useful to have such a subalgebra that is also a direct summand. For example, in $Ш_{\mathbb{Z},0}(\mathbb{Z})$ which is just the divided power algebra $\oplus_{n\geqslant 0}\mathbb{Z}x_n$ with $x_m x_n = \binom{m+n}{m} x_{m+n}$, the subalgebra generated by any $f \notin \mathbb{Z}$ is a polynomial algebra, but the algebra itself is not a polynomial algebra, none does it have a polynomial subalgebra as a direct summand. In the case we consider, it would be interesting to find out whether the polynomial algebra summand in Eq. (46) can be extended to a larger such summand.

References

[1] M. Aguiar, On the associative analog of Lie bialgebras, *J. Algebra*, **244** (2001), 492-532.

[2] G. E. Andrews, L. Guo, W. Keigher and K. Ono, Baxter algebras and Hopf algebras, *Trans. Amer. Math. Soc.* **355** (2003), 4639-4656, arXiv:math/0407181.

[3] C. Bai, A unified algebraic approach to classical Yang-Baxter equations, to appear in *Jour. Phys. A*, arXiv:0707.4226[math.QA].

[4] G. Baxter, An analytic problem whose solution follows from a simple algebraic identity, *Pacific J. Math.* **10** (1960), 731–742.

[5] P. Cartier, On the structure of free Baxter algebras, *Adv. Math.* **9** (1972), 253-265.

[6] A. Connes and D. Kreimer, Renormalization in quantum field theory and the Riemann-Hilbert problem. I. The Hopf algebra structure of graphs and the main theorem, *Comm. Math. Phys.*, **210**, (2000), no. 1, 249-273.

[7] E. J. Ditters, Curves and formal (co)groups, *Invent. Math.* **17** (1972), 1-20.

[8] K. Ebrahimi-Fard and L. Guo, Free Rota-Baxter algebras and dendriform algebras, *J. Pure Appl. Algebra*, **212** (2008), 320-339, arXiv:math.RA/0503647

[9] K. Ebrahimi-Fard and L. Guo, Quasi-shuffles, mixable shuffles and Hopf algebras, *J. Algebraic Combinatorics,* **24**, (2006), 83-101, arXiv:math.RA/0506418.

[10] K. Ebrahimi-Fard and L. Guo, Rota-Baxter algebras in renormalization of perturbative quantum field theory, in: *Universality and Renormalization*, I. Binder and D. Kreimer, editors, Fields Institute Communications v. 50, AMS, 2007, 47-105, arXiv:hep-th/0604116.

[11] K. Ebrahimi-Fard, L. Guo and D. Kreimer, Spitzer's Identity and the Algebraic Birkhoff Decomposition in pQFT, *J. Phys. A: Math. Gen.* **37** (2004) 11037-11052. arXiv:hep-th/0407082.

[12] K. Ebrahimi-Fard, L. Guo and D. Manchon, Birkhoff type decompositions and the Baker-Campbell-Hausdorff recursion, *Comm. in Math. Phys.* **267** (2006) 821-845, arXiv: math-ph/0602004.
[13] R. Ehrenborg, On postes and Hopf algebras, *Adv. Math.* **119** (1996), 1-25.
[14] I. M. Gessel, Multipartite P-partitions and inner product of skew Schur functions, in Contemporary Mathematics, **34**, American Mathematical Society, Providence, RI, 1984, 289301.
[15] L. Guo, Properties of free Baxter algerbas, *Adv. Math.* **151** (2000), 346-374.
[16] L. Guo, Baxter algebra and differential algebra, in: Differential Algebra and Related Topics, World Scientific Publishing Company, (2002), 281-305. arXiv:math.RA/0407180
[17] L. Guo, Algebraic Birkhoff Decomposition and Its Applications, to appear in: Automorphic Forms and the Langlands Program, International Press, arXiv:0807.2266[math.RA].
[18] L. Guo, Baxter algebras and the umbral calculus, *Adv. in Appl. Math.,* **27** (2001), 405-426.
[19] L. Guo, Baxter algebras, Stirling numbers and partitions, *J. Algebra Appl.* **4** (2005), 153-164.
[20] L. Guo, W. Keigher, Baxter algebras and shuffle products, *Adv. Math.*, **150**, (2000), 117-149.
[21] L. Guo and W. Keigher, On free Baxter algebras: completions and the internal construction, *Adv. in Math.,* **151** (2000), 101-127.
[22] L. Guo and W. Keigher, On differential Rota-Baxter algebras, *J. Pure Appl. Algebra*, **212** (2008), 522-540, arXiv: math.RA/0703780.
[23] L. Guo and W. Yu Sit, Enumenation of Rota-Baxter words, Proceedings ISSAC 2006, Genoa, Italy, ACM Press, 124-131, arXiv: math.RA/0602449.
[24] L. Guo and B. Xie, p-adic and integral properties of extended double shuffle relations, in preparation.
[25] L. Guo and B. Zhang, Renormalization of multiple zeta values, *J. Algebra*, **319** (2008), 3770-3809, arXiv:math.NT/0606076.
[26] L. Guo and B. Zhang, Differential Algebraic Birkhoff Decomposition and renormalization of multiple zeta values, *J. Number Theory*, **128** (2008), 2318-2339, arXiv:0710.0432(math.NT).
[27] M. Hazewinkel, The Leibniz-Hopf algebra and Lyndon words, preprint, CWI, Amsterdam, 1996.
[28] M. Hazewinkel, The algebra of quasi-symmetric functions in free over the integers, *Adv. Math.* **164** (2001), 283-300.
[29] M. Hazewinkel, Generalized overlapping shuffle algebras, *J. Math. Sci.* **106** (2001), 3168-3186.
[30] M. E. Hoffman, Multiple harmonic series *Pacific J. Math.* **152** (1992), 275-290.
[31] M. Hoffman, Quasi-shuffle products, *J. Algebraic Combin.*, **11** (2000), 49-68.
[32] S. MacLane, Homology, Springer, 1995.
[33] H. N. Minh and M. Petitot, Lyndon words, polylogarithms and the Riemann ζ function, *Discrete Math.* **217** (2000), 273-292.
[34] Y. Ohno and W. Zudilin, Zeta stars, to appear in *Commun. Number Theory Phys.*
[35] G. Racinet, Doubles mélanges des polylogarithmes multiples aux racines de l'unité, *Pub. Math. IHES*, **95** (2002), 185-231.
[36] D. E. Radford, A natural ring basis for the shuffle algebra and an application to group schemes, *J. Alg.* **58** (1979), 432-454.
[37] C. Reutenauer, Free Lie Algebras, Oxford University Press, Oxford, UK, 1993.
[38] G.-C. Rota, Baxter algebras and combinatorial identities I, II, *Bull. Amer. Math. Soc.* **75** (1969), 325–329, 330–334.
[39] G.-C. Rota, Baxter operators, an introduction, In: "Gian-Carlo Rota on Combinatorics, Introductory papers and commentaries", Joseph P.S. Kung, Editor, Birkhäuser, Boston, 1995.

Department of Mathematics and Computer Science, Rutgers University, Newark, NJ 07102
E-mail address: liguo@newark.rutgers.edu

Department of Mathematics, Peking University, Beijing, China
E-mail address: byhsie@math.pku.edu.cn