

Free polynomial strong bimonoids

Manfred Droste
Leipzig University, Germany
droste@informatik.uni-leipzig.de

Zoltán Fülöp*
University of Szeged, Hungary
fulop@inf.u-szeged.hu

November 4, 2025

Abstract

Recently, in weighted automata theory the weight structure of strong bimonoids has found much interest; they form a generalization of semirings and are closely related to near-semirings studied in algebra. Here, we define polynomials over a set X of indeterminates as well as an addition and a multiplication. We show that with these operations, they form a right-distributive strong bimonoid, that this polynomial strong bimonoid is free over X in the class of all right-distributive strong bimonoids and that it is both left- and right-cancellative. We show by purely algebraic reasoning that two arbitrary terms are equivalent modulo the laws of right-distributive strong bimonoids if and only if their representing polynomials are equivalent by the laws of only associativity and commutativity of addition and associativity of multiplication. We give effective procedures for constructing the representing polynomials. As a consequence, we obtain that the equivalence of arbitrary terms modulo the laws of right-distributive strong bimonoids can be decided in exponential time. Using term-rewriting methods, we show that each term can be reduced to a unique polynomial as normal form. We also derive corresponding results for the free idempotent right-distributive polynomial strong bimonoid over X . We construct an idempotent strong bimonoid which is weakly locally finite but not locally finite and show an application of it in weighted automata theory.

Keywords: polynomials over semirings, free strong bimonoids, cancellation property, AC-reduction, idempotency, weighted automata

AMSC: 16Y60, 16Y30, 08A40, 08B20, 68Q45, 03D15

1 Introduction

Polynomials are fundamental in many areas of Mathematics. The coefficients of polynomials are often taken from algebraic structures like fields, rings or semirings. With suitable definitions of addition and multiplication, the polynomials then also form rings or semirings, which is crucial for

*Project no TKP2021-NVA-09 has been implemented with the support provided by the Ministry of Culture and Innovation of Hungary from the National Research, Development and Innovation Fund, financed under the TKP2021-NVA funding scheme.

their importance. Already in the last century, in algebra near-fields, which can be viewed as fields satisfying only a one-sided distributivity law, were investigated [Dic05, Zas36]. Subsequently, a theory of near-rings [Pil77] and near-semirings [vHvR67] was developed. Basic examples for such structures are provided by additive monoids of functions with composition as multiplication operation; also, the usual multiplication of ordinal numbers is left- but not right-distributive. Near-rings also occur in operator theory and in mathematical physics [Sch97]. In computer science, one-sided distributivity has been investigated intensively in Structural Operational Semantics and for process algebras, cf. [ACIM12] for a survey and unifying approach. Unification problems in equational theories with only one-sided distributivity have been investigated already in [TA87]; such asymmetric unification arises naturally in symbolic analysis of cryptographic protocols, see [EEK⁺13, MMN15]. Recently, in theoretical computer science weighted automata with weights from strong bimonoids were investigated. Strong bimonoids form an extension of semirings obtained by not requiring the distributivity laws. For weighted automata, right-distributivity of the weight structures is important for the coincidence of different kinds of behaviors of the automata. For a survey on this area in tree automata theory, see [FV24].

Polynomials with coefficients from the semiring of natural numbers (resp., the ring of integers) over a set X of non-commuting variables, with the standard definitions of addition and multiplication, again form a semiring (resp., a ring), which, in fact, is isomorphic to the free semiring (resp., ring) of all terms over X ; moreover, each term can be represented (modulo the semiring laws) by a polynomial. Similar representations by 'polynomial terms' are essential for many fields of algebra, cf. [Grä68].

It is a natural question, both intrinsically and motivated by the above, to consider the effect of missing left- or right-distributivity (or both).

In this paper, we aim to develop strong bimonoids of polynomials, in particular, with the assumption of right-distributivity and possibly idempotence of addition. For this, we will define polynomials as congruence classes of particular terms, with suitable definitions of addition and multiplication.

Our main results are the following; here we concentrate on the right-distributive case. We provide two definitions of the multiplication, an inductive and a direct one, and we show that they yield the same result and that we obtain, in particular, a right-distributive strong bimonoid of polynomials.

We then show that this right-distributive strong bimonoid of polynomials is both left- and right-cancellative. Here, we only have to assume that the two polynomials occurring as right factors have the same size. This provides a crucial difference to the standard semiring of polynomials with natural numbers (or integers) as coefficients, where the analogous result fails. It shows that in our setting we have a basically different multiplication and equality, due to the absence of left-distributivity. Our proof of this general cancellation result proceeds by an analysis of the structure of graphs associated with the polynomials.

Next, we extend the important result that the semiring of polynomials with coefficients in the natural numbers over a set X of non-commuting variables is isomorphic to the free semiring of terms over X into our setting. We will show that our strong bimonoid of polynomials over X is isomorphic to the free right-distributive strong bimonoid of terms over X . Consequently, the polynomials can be seen as concrete representations of the arbitrary terms in the free right-distributive strong bimonoid.

Moreover, we show that two arbitrary terms are equivalent modulo the laws of right-distributive strong bimonoids if and only if their representing polynomials are equivalent by the laws of only associativity and commutativity of addition resp. associativity of multiplication. In the term rewriting literature, this is regarded as an AC-reduction result. This is usually achieved by an involved analysis of critical pairs; here we obtain it by algebraic means. We give effective procedures for constructing the representing polynomials. As a consequence, we obtain that the mentioned equivalence of arbitrary terms can be decided in exponential time. Similar results are obtained for a notion of simple terms and the free semiring of all terms (here, with linear time complexity for the decidability part), and for suitably defined idempotency-reduced polynomials and the free idempotent right-distributive strong bimonoid.

Furthermore, using term-rewriting methods, we show that each term can be reduced to a unique polynomial term as normal form. As a consequence, for the free idempotent right-distributive strong bimonoid, we obtain such a reduction with uniqueness up to additive associativity and commutativity.

Our results have applications in the theory of weighted automata. Recall that a classical automaton either accepts or rejects a given input, so, for a given input, it produces a yes/no- or 1/0-answer. Weighted automata assign to each possible input an element from a more general weight structure; this value may reflect, e.g., the number of possible executions or the minimal or maximal amount of resources needed for the execution of the given input. Here, weight structures of the literature include semirings, lattices and, more generally, strong bimonoids. A central question investigated from the beginnings of weighted automata theory is whether weighted automata produce finitely or infinitely many such values. It is easy to see that if the strong bimonoid B is locally finite (i.e., each finitely generated strong subbimonoid is finite), then each weighted word automaton and each weighted tree automaton over B produces only finitely many values (cf., e.g., [FV24]). Recently, it was shown that if the strong bimonoid B satisfies a weaker local finiteness condition, then each weighted word automaton still produces only finitely many values (cf. [DSV10]). However, assuming B is not locally finite, even if B is right-distributive, there are weighted tree automata which produce infinitely many values, cf. [DFTV24]. Hence the question arises whether there exist such right-distributive weakly locally finite strong bimonoids which are not locally finite. If yes, then we have an essential difference in the computation power of weighted tree automata vs. weighted word automata. This was answered positively in [DFTV24]. As indicated above, calculation of maximal or minimal values are important in various quantitative settings; therefore we wish to incorporate idempotency into our strong bimonoid. Using our previous results, in Section 7, we sharpen the mentioned result of [DFTV24] by constructing an idempotent and right-distributive strong bimonoid which is weakly locally finite but not locally finite.

2 Strong bimonoids and universal algebra background

Strong bimonoids. In this paper, we will consider algebraic structures which comprise the class of semirings and which are defined as follows.

A *strong bimonoid* [DSV10, CDIV10, DV10, DV12] is an algebra $B = (B, \oplus, \otimes, 0, 1)$ such that $(B, \oplus, 0)$ is a commutative monoid, $(B, \otimes, 1)$ is a monoid, and 0 is annihilating with respect to $\otimes$, i.e., $b \otimes 0 = 0 \otimes b = 0$ for all $b \in B$. The operations $\oplus$ and $\otimes$ are called addition and

multiplication, respectively.

A strong bimonoid $B = (B, \oplus, \otimes, 0, 1)$ is

- *commutative* if $\otimes$ is commutative,
- *left-distributive* if $a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$ for all $a, b, c \in B$,
- *right-distributive* if $(a \oplus b) \otimes c = (a \otimes c) \oplus (b \otimes c)$ for all $a, b, c \in B$,
- *idempotent* if $b \oplus b = b$ for all $b \in B$.

A *semiring* [HW93, Gol99] is a distributive strong bimonoid, i.e., a strong bimonoid which is left-distributive and right-distributive. Clearly, a commutative right-distributive strong bimonoid is also left-distributive and hence a semiring.

We give a few examples of semirings, of strong bimonoids without or with only right- (or left-) distributivity, respectively, and of research involving one-sided distributivity.

Example 2.1. (a) Semirings include the Boolean semiring $(\mathbb{B}, \vee, \wedge, 0, 1)$ of truth values, the semiring $(\mathbb{N}, +, \times, 0, 1)$ of natural numbers, all rings and fields, and all distributive lattices $(L, \vee, \wedge, 0, 1)$ with smallest element 0 and greatest element 1.

(b) The plus-min strong bimonoid of extended natural numbers $(\mathbb{N}_\infty, +, \min, 0, \infty)$ where $\mathbb{N}_\infty = \mathbb{N} \cup \{\infty\}$ and $+$ and $\min$ are the usual addition and minimum operations, respectively, on natural numbers including ∞ .

(c) The plus-plus strong bimonoid of natural numbers (cf. [DFTV24, Ex. 2.3]) $(\mathbb{N}_0, \oplus, +, 0, 0)$ with a new zero element $0 \notin \mathbb{N}$. The binary operations $\oplus$ and $+$, if restricted to $\mathbb{N}$, are both the usual addition of natural numbers, and $0 \oplus x = x \oplus 0 = x$ and $0 + x = x + 0 = 0$ for each $x \in \mathbb{N}_0$.

(d) All lattices $(L, \vee, \wedge, 0, 1)$ with smallest element 0 and greatest element 1 are strong bimonoids.

(e) Near-fields, near-rings and near-semirings provide typical examples of right-distributive strong bimonoids, cf. [Pil77, vHvR67, Kri05]. Here, to obtain a right-distributive strong bimonoid, we have to add the natural requirements that the addition operation is commutative, the additively neutral element 0 also acts like a multiplicative zero, and there is a unit element for multiplication.

(f) $\text{Diff}^0(\mathbb{R}) = \{f : \mathbb{R} \rightarrow \mathbb{R} \mid f \text{ is differentiable, } f(0) = 0\}$ with the usual addition and composition of functions forms a right-distributive strong bimonoid.

(g) Let $(\mathbb{N}[x]_0, \oplus, \circ, 0, 1)$ be the set of all polynomials over a variable x with coefficients (e.g.) in $\mathbb{N}$ and with constant term equal to 0, where $\oplus$ is the usual addition of polynomials, multiplication is given by composition, 0 is the zero polynomial and $1 = x$. This strong bimonoid is right-distributive but not left-distributive.

(h) Multiplication of ordinal numbers is left-distributive but not right-distributive over addition (since, e.g. $(1 + 1) \times \omega = \omega \neq 1 \times \omega + 1 \times \omega$). Hence, e.g., the set of all ordinal numbers strictly below ω^ω with the usual addition and multiplication of ordinal numbers forms a left-distributive strong bimonoid.

(i) The strong bimonoid of words $(\Sigma^* \cup \{\infty\}, \wedge, \cdot, \infty, \varepsilon)$ with a new element $\infty \notin \Sigma^*$. For $u, v \in \Sigma^*$, $u \wedge v$ is the greatest common prefix of u and v , and $u \cdot v = uv$ is the usual concatenation of u and v . Moreover, $u \wedge \infty = \infty \wedge u = u$ and $u \cdot \infty = \infty \cdot u = \infty$ for all $u \in \Sigma^* \cup \{\infty\}$. This strong bimonoid has been investigated in [Moh97, section 3.6] for string-to-weight transducers in natural language processing. It is left-distributive, but, if Σ has at least two elements, it is not right-distributive and hence not a semiring.

(j) A survey of and unifying approach for much research in Structural Operational Semantics and process algebras stressing right-distributivity (called 'left-distributivity' in the paper) is given in [ACIM12].

(k) Unification problems in equational theories with only one-sided distributivity have been investigated already in [TA87]. Such asymmetric unification arises naturally in symbolic analysis of cryptographic protocols, see [EEK⁺13, MMN15].

(ℓ) Right-residuated lattices with right-distributivity (which give rise to examples of idempotent right-distributive strong bimonoids investigated here) may also be used to give the semantics of non-commutative substructural logics such as the non-commutative Lambek calculus, cf. [GR04, section 4], [VW24].

(m) Nonlinear operators in functional analysis and mathematical physics, with addition and composition, also give rise to right-distributive strong bimonoids, cf. [Sch97, p.3842]. $\square$

For many further examples of strong bimonoids, we refer to [DSV10, CDIV10] and in particular to [FV24, Ex. 2.7.10, 1-11]), highlighting the theory of weighted tree automata with weights in strong bimonoids.

Our goal is to define notions of polynomials (in non-commuting variables) with values in the natural numbers which extend the standard notions of polynomials in non-commuting variables, and to obtain strong bimonoids of such polynomials over non-commuting variables. For this, we recall basic notions of universal algebra which we will employ subsequently.

General. We denote by $\mathbb{N}$ the set of nonnegative integers and $\mathbb{N}_+ = \mathbb{N} \setminus \{0\}$. For every $k, n \in \mathbb{N}$, we denote by $[k, n]$ the set $\{i \in \mathbb{N} \mid k \leq i \leq n\}$ and we abbreviate $[1, n]$ by $[n]$. Hence $[0] = \emptyset$.

Let A be a set. Then A^* denotes the set of all finite strings over A , and ε denotes the empty string. Any subset $\rho \subseteq A \times A$ is a *(binary) relation on A* . Let ρ be a binary relation on A . As usual ρ^n denotes the n th power of ρ for each $n \in \mathbb{N}$. Moreover, ρ^+ and ρ^* denote the transitive closure, and the reflexive and transitive closure of ρ , respectively¹

Signature and terms. A *signature* is a pair (Σ, ar) , where Σ is a non-empty set and $\text{ar} : \Sigma \rightarrow \mathbb{N}$ is a mapping, called *arity mapping*. For each $k \in \mathbb{N}$, we put $\Sigma^{(k)} = \{\sigma \in \Sigma \mid \text{ar}(\sigma) = k\}$. Usually, we abbreviate (Σ, ar) by Σ . If Σ is finite, then we also call it *ranked alphabet* (cf. e.g. [FV24]).

Let Σ be a signature and X be a set disjoint with Σ . The set of Σ -terms over X , denoted by $T_\Sigma(X)$, is the smallest set T such that (i) $\Sigma^{(0)} \cup X \subseteq T$ and (ii) for every $k \in \mathbb{N}_+$, $\sigma \in \Sigma^{(k)}$, and $t_1, \dots, t_k \in T$, we have $\sigma(t_1, \dots, t_k) \in T$. We abbreviate $T_\Sigma(\emptyset)$ by T_Σ .

The *size* of a term $t \in T_\Sigma(X)$, denoted by $\text{size}(t)$, is the total number of occurrences of elements from $\Sigma \cup X$ in t .

Universal algebra. We assume that the reader is familiar with basic concepts of universal algebra, like subalgebra, subalgebra generated by a subset, homomorphism, congruence relation (for short: congruence), quotient algebra, and free algebra with a generating set [BS81, Wec92], and [BN98].

¹It will always be clear from the context whether ρ^* denotes the reflexive and transitive closure of the relation ρ or the set of all finite sequences over the set ρ .

Let Σ be a signature. We regard the elements of Σ as operation symbols. An *algebra* A of type Σ (Σ -algebra) is a pair $A = (A, \theta)$ where A is a nonempty set and θ is a mapping from Σ to the family of finitary operations on A such that for every $k \in \mathbb{N}$ and $\sigma \in \Sigma^{(k)}$, the operation $\theta(\sigma)$ has arity k . As usual, nullary operations are interpreted as constants.

Let X be a set. The Σ -term algebra over X , denoted by $T_\Sigma(X)$, is the Σ -algebra $T_\Sigma(X) = (T_\Sigma(X), \theta_\Sigma)$ where, for every $k \in \mathbb{N}$, $\sigma \in \Sigma^{(k)}$, and $t_1, \dots, t_k \in T_\Sigma(X)$, we let $\theta_\Sigma(\sigma)(t_1, \dots, t_k) = \sigma(t_1, \dots, t_k)$. The Σ -term algebra, denoted by T_Σ , is the Σ -term algebra over $\emptyset$, i.e., $T_\Sigma = T_\Sigma(\emptyset)$.

Let $\mathcal{K}$ be an arbitrary class of Σ -algebras. Moreover, let $F = (F, \eta)$ be a Σ -algebra in $\mathcal{K}$ and $X \subseteq F$ such that F is generated by X . The algebra F is called *freely generated in $\mathcal{K}$ by X* if, for every Σ -algebra $A = (A, \theta)$ in $\mathcal{K}$ and mapping $f: X \rightarrow A$, there exists an extension of f to a Σ -algebra homomorphism $h: F \rightarrow A$ from F to A . If the extension h exists, then it is unique since X generates F , cf. e.g. [BN98, Lm. 3.3.1]. A Σ -algebra F is *free in $\mathcal{K}$* , if it is freely generated in $\mathcal{K}$ by some subset $X \subseteq F$.

Lemma 2.2. [BN98, Thm. 3.3.3] Let A and B be free Σ -algebras in $\mathcal{K}$, freely generated by the sets X and Y , respectively. If $|X| = |Y|$, then A and B are isomorphic. $\square$

We will use the following well-known result without any reference.

Theorem 2.3. (cf. [BN98, Thm. 3.4.2], [BS81, Thm. II.10.8], [Wec92, p. 18, Thm. 4]) $T_\Sigma(X)$ is a free Σ -algebra in the class of all Σ -algebras, freely generated by the set X . $\square$

In the rest of this section, A denotes an arbitrary Σ -algebra (A, θ) .

Let ρ be a congruence on A . For each $a \in A$, we let $[a]_\rho = \{b \in A \mid a \rho b\}$, the *congruence class of a (modulo ρ)*. For each $B \subseteq A$, we put $B/\rho = \{[a]_\rho \mid a \in B\}$. The *quotient algebra of A by ρ* is the Σ -algebra $A/\rho = (A/\rho, \theta/\rho)$ where, for every $k \in \mathbb{N}$, $\sigma \in \Sigma^{(k)}$, and $a_1, \dots, a_k \in A$, we have $(\theta/\rho)(\sigma)([a_1]_\rho, \dots, [a_k]_\rho) = [\theta(\sigma)(a_1, \dots, a_k)]_\rho$.

Next we wish to consider Σ -identities and the congruence on A induced by a set of such identities. For this, we introduce the necessary concepts.

Let $Z = \{z_1, z_2, \dots\}$ be a set, we call the elements of Z *variables*. For each $n \in \mathbb{N}$, we put $Z_n = \{z_1, \dots, z_n\}$.

An *assignment* is a mapping $\varphi: Z \rightarrow A$. In the sequel, its unique extension to a Σ -algebra homomorphism from $T_\Sigma(Z)$ to A will be denoted also by φ . For an arbitrary $t \in T_\Sigma(Z)$, we call $\varphi(t)$ the *evaluation of t in A by φ* .

A Σ -identity over Z (or: identity) is a pair (ℓ, r) where $\ell, r \in T_\Sigma(Z)$. The Σ -algebra A satisfies the identity (ℓ, r) if, for every assignment $\varphi: Z \rightarrow A$, we have $\varphi(\ell) = \varphi(r)$.

Lemma 2.4. [BS81, Th. II.6.10 and Lm. II.11.3] If A satisfies an identity (ℓ, r) and ρ is a congruence on A , then A/ρ also satisfies the identity (ℓ, r) . $\square$

Let E be a set of identities. The *congruence (relation) on A induced by E* , denoted by $=_E$, is the smallest congruence on A which contains the set

$$E(A) = \{(\varphi(\ell), \varphi(r)) \mid (\ell, r) \in E, \varphi: Z \rightarrow A\}. \quad (1)$$

The following lemma is well-known and can be proven similarly to [Wec92, p. 176, Lm. 24].

Lemma 2.5. Let E be a set of Σ -identities. Then $A/\equiv_E$ satisfies all identities in E . $\square$

Next we extend the well-known syntactic characterization of the congruence on $T_\Sigma(Z)$ induced by a set $E \subseteq T_\Sigma(Z) \times T_\Sigma(Z)$ of Σ -identities, cf. [BN98, Thm. 3.1.12] and [BS81, Thms. II.14.17, II.14.19], to a characterization of the congruence on A induced by E . In fact, this is closely related to a general description of a congruence generated by a binary relation on A , cf. [Wec92, Sect. 2.1.2].

Each element $c \in T_\Sigma(Z)$ in which the variable z_1 occurs exactly once is called a ΣZ -context. We let $C_{\Sigma,Z}$ be the set of all ΣZ -contexts. Given a ΣZ -context c and a term $t \in T_\Sigma(Z)$, we let $c[t] \in T_\Sigma(Z)$ be the term obtained from c by replacing the variable z_1 by t . That is, if $\varphi : Z \rightarrow T_\Sigma(Z)$ is given by $\varphi(z_1) = t$ and $\varphi(z_i) = z_i$ for each $i \geq 2$, then $c[t] = \varphi(c)$.

Let E be a set of Σ -identities. The *reduction relation induced by E on A* , denoted by $\Rightarrow_E$, is the binary relation on A defined as follows: for every $a, b \in A$, we let $a \Rightarrow_E b$ if there exist a ΣZ -context $c \in C_{\Sigma,Z}$, an identity (ℓ, r) in E , and an assignment $\varphi : Z \rightarrow A$ such that $a = \varphi(c[\ell])$ and $b = \varphi(c[r])$. In this case we say that b is obtained from a in a reduction step (using the identity (ℓ, r)).

For an identity $e = (\ell, r)$ we define $e^{-1} = (r, \ell)$ and we let $E^{-1} = \{e^{-1} \mid e \in E\}$. Moreover, we abbreviate $\Rightarrow_{E \cup E^{-1}}$ by $\Leftrightarrow_E$.

The subsequent characterization says that, for any two elements $a, b \in A$, we have $a =_E b$ if and only if, there is a finite sequence of elements $a = a_0, a_1, \dots, a_n = b$ of A for some $n \in \mathbb{N}$ such that for each $i \in [n]$, the element a_i can be obtained from a_{i-1} in a reduction step using an identity in E or the inverse of an identity. For a proof we can follow the proof of [DFTV24, Lm. 2.3], stated for the case that Σ is finite. However, in that proof we do not use the finiteness of Σ .

Lemma 2.6. [Wec92, p. 98, Thm. 6] Let E be a set of Σ -identities and $=_E$ the congruence on A induced by E . Then $=_E = \Leftrightarrow_E^*$. $\square$

3 Free strong bimonoids

In this section, we will shortly consider the free strong bimonoid, the free right-distributive strong bimonoid, and the free idempotent right-distributive strong bimonoid, each freely generated by a nonempty set X of variables.

For this we consider the particular signature

$$\Sigma_{\text{sb}} = \{\hat{+}, \hat{\times}, \hat{0}, \hat{1}\} \text{ with } \text{ar}(\hat{+}) = \text{ar}(\hat{\times}) = 2 \text{ and } \text{ar}(\hat{0}) = \text{ar}(\hat{1}) = 0.$$

(We write $\hat{}$ over the symbols of Σ because later the symbols $+$, $\times$, 0 , and 1 will denote addition, multiplication, zero and one of polynomials in certain algebras, respectively.) We call Σ_{sb} the *strong bimonoid signature*.

Let X be a nonempty set, which we keep fixed throughout the paper.

We consider the Σ_{sb} -term algebra $T_{\Sigma_{\text{sb}}}(X)$ over X . Since we use the signature Σ_{sb} in almost all of the rest of the paper, we drop it from the notation, i.e

$$\text{we abbreviate } T_{\Sigma_{\text{sb}}}(X) = (T_{\Sigma_{\text{sb}}}(X), \theta_{\Sigma_{\text{sb}}}) \text{ by } T(X) = (T(X), \theta).$$

We write elements of $T(X)$ in infix form, e.g. we write $(\hat{1} \hat{+} \hat{1}) \hat{\times} x$ for $\hat{\times}(\hat{+}(\hat{1}, \hat{1}), x)$ where $x \in X$. Moreover, we denote the binary operations $\theta(\hat{+})$ and $\theta(\hat{\times})$ on $T(X)$ by $+'$ and $\times'$, respectively, and we write them in infix form. That is, for every $t_1, t_2 \in T(X)$, we have

$$t_1 +' t_2 = \theta(\hat{+})(t_1, t_2) = t_1 \hat{+} t_2 \quad \text{and} \quad t_1 \times' t_2 = \theta(\hat{\times})(t_1, t_2) = t_1 \hat{\times} t_2 .$$

Also, we have the constants $0' = \theta(\hat{0}) = \hat{0}$ and $1' = \theta(\hat{1}) = \hat{1}$. Hence, we may write $T(X)$ in the form

$$T(X) = (T(X), +', \times', 0', 1').$$

Subsequently, we will consider the following identities:

$$\begin{aligned} e_1 : & (z_1 \hat{+} (z_2 \hat{+} z_3), (z_1 \hat{+} z_2) \hat{+} z_3) & e_3 : & (z \hat{+} \hat{0}, z) \\ e_2 : & (z_1 \hat{+} z_2, z_2 \hat{+} z_1) & e_4 : & (z_1 \hat{\times} (z_2 \hat{\times} z_3), (z_1 \hat{\times} z_2) \hat{\times} z_3) \\ e_5 : & (\hat{1} \hat{\times} z, z) & e_6 : & (z \hat{\times} \hat{1}, z) \\ e_7 : & (z \hat{\times} \hat{0}, \hat{0}) & e_8 : & (\hat{0} \hat{\times} z, \hat{0}) \\ e_9 : & ((z_1 \hat{+} z_2) \hat{\times} z_3, (z_1 \hat{\times} z_3) \hat{+} (z_2 \hat{\times} z_3)) \\ e_{10} : & (z_1 \hat{\times} (z_2 \hat{+} z_3), (z_1 \hat{\times} z_2) \hat{+} (z_1 \hat{\times} z_3)) \\ e_{11} : & ((z \hat{+} z), z) \end{aligned}$$

First, for motivation of the subsequent development in this section, we recall well-known fundamental facts on the free semiring and on polynomials in the present notation.

Let $E_S = \{e_1, \dots, e_{10}\}$ (the set of “semiring axioms”), and let $=_{E_S}$ denote the congruence relation on $T(X)$ generated by E_S . Thus, the quotient algebra of $T(X)$ by $=_{E_S}$ is the algebra

$$T(X)/=_{E_S} = (T(X)/=_{E_S}, +'/=_{E_S}, \times'/=_{E_S}, [0']_{=_{E_S}}, [1']_{=_{E_S}}) .$$

We abbreviate $T(X)/=_{E_S}$ by $FS(X)$ and abbreviate also the components of $T(X)/=_{E_S}$ (i.e. of $FS(X)$) and write the quotient algebra in the form

$$FS(X) = (FS(X), \oplus, \otimes, 0, 1).$$

Moreover, for $t \in T(X)$, we abbreviate the notation $[t]_{=_{E_S}}$ by $[t]_{E_S}$, and we abbreviate $X/_=_{E_S}$ by X/E_S .

Then, e.g., for every $t_1, t_2 \in T(X)$, we have

$$\begin{aligned} [t_1]_{E_S} \oplus [t_2]_{E_S} &= [t_1 +' t_2]_{E_S} \quad \text{and} \quad [t_1]_{E_S} \otimes [t_2]_{E_S} = [t_1 \times' t_2]_{E_S} \\ [t_1]_{E_S} \oplus 0 &= [t_1]_{E_S} \quad \text{and} \quad [t_1]_{E_S} \otimes 0 = 0 \\ [t_1]_{E_S} \otimes 1 &= 1 \otimes [t_1]_{E_S} = [t_1]_{E_S} . \end{aligned}$$

By Lemma 2.5 it follows that the algebra $FS(X)$ satisfies all identities in E_S . In particular,

- identities $e_1 - e_3$ assure that $(FS(X), \oplus, 0)$ is a commutative monoid,
- identities $e_4 - e_6$ assure that $(FS(X), \otimes, 1)$ is a monoid,

- identities $e_7 - e_8$ assure that $\mathbb{0}$ is annihilating with respect to $\otimes$, and
- identities $e_9 - e_{10}$ assure that $\otimes$ distributes over $\oplus$.

Hence $\mathbf{FS}(X)$ is a semiring. In fact, it is well-known that $\mathbf{FS}(X)$ is free with generating set X/E_S in the class of all semirings. Therefore it is called *the free semiring over X* .

Expressions of the form $\sum_{w \in F} n_w w$ where F is a finite subset of X^* and $n_w \in \mathbb{N}$ for each $w \in F$ are called *polynomials* over X . We consider polynomials as terms in $\mathbf{T}(X)$ in the natural way. For instance, the polynomial $2xy + 2$ corresponds to the term $((\hat{1} + \hat{1}) \hat{\times} x) \hat{\times} y + (\hat{1} + \hat{1})$. Let $\mathbb{N}[X]$ be the set of all these polynomials. Then $\mathbb{N}[X] = (\mathbb{N}[X], +, \cdot, 0, 1)$, with the usual addition and multiplication of polynomials, is a semiring. Moreover, it is free with generating set X in the class of all semirings, cf., e.g., [Wec92, Sec. 3.2.2, Ex. 3]. Then the following result is folklore.

Theorem 3.1. *The free semiring $\mathbf{FS}(X)$ over X is isomorphic to the semiring $\mathbb{N}[X]$ of polynomials over X . Moreover, the polynomials form a representation of the semiring terms over X in the sense that for each term $t \in \mathbf{T}(X)$ there is a polynomial $p \in \mathbb{N}[X]$ which is semiring-equivalent to t , i.e., $t =_{E_S} p$. $\square$*

The goal of this paper is to derive analogous results for strong bimonoids, right-distributive strong bimonoids, and idempotent right-distributive strong bimonoids. In the subsequent notation, let rd and id , indicate right-distributivity and idempotence, respectively.

Definition 3.2. (a) Let $E = \{e_1, \dots, e_8\}$ (“strong bimonoid axioms”) and let $\mathbf{FB}(X) = (\mathbf{FB}(X), \oplus, \otimes, \mathbb{0}, \mathbb{1})$ be the quotient algebra of $\mathbf{T}(X)$ by $=_E$.

(b) Let $E_{\text{rd}} = E \cup \{e_9\}$ (axiom of right-distributivity added), and let $\mathbf{FB}_{\text{rd}}(X) = (\mathbf{FB}_{\text{rd}}(X), \oplus_{\text{rd}}, \otimes_{\text{rd}}, \mathbb{0}, \mathbb{1})$ be the quotient algebra of $\mathbf{T}(X)$ by $=_{E_{\text{rd}}}$.

(c) Let $E_{\text{id,rd}} = E_{\text{rd}} \cup \{e_{11}\}$ (axiom of idempotency added), and let $\mathbf{FB}_{\text{id,rd}}(X) = (\mathbf{FB}_{\text{id,rd}}(X), \oplus_{\text{id,rd}}, \otimes_{\text{id,rd}}, \mathbb{0}, \mathbb{1})$ be the quotient algebra of $\mathbf{T}(X)$ by $=_{E_{\text{id,rd}}}$. $\square$

For easier subsequent use, the definition is summarized by the following table.

set of identities	quotient algebra	short notation
$E = \{e_1, \dots, e_8\}$	$\mathbf{T}(X)/=_E$	$\mathbf{FB}(X) = (\mathbf{FB}(X), \oplus, \otimes, \mathbb{0}, \mathbb{1})$
$E_{\text{rd}} = E \cup \{e_9\}$	$\mathbf{T}(X)/=_E$	$\mathbf{FB}_{\text{rd}}(X) = (\mathbf{FB}_{\text{rd}}(X), \oplus_{\text{rd}}, \otimes_{\text{rd}}, \mathbb{0}, \mathbb{1})$
$E_{\text{id,rd}} = E_{\text{rd}} \cup \{e_{11}\}$	$\mathbf{T}(X)/=_E$	$\mathbf{FB}_{\text{id,rd}}(X) = (\mathbf{FB}_{\text{id,rd}}(X), \oplus_{\text{id,rd}}, \otimes_{\text{id,rd}}, \mathbb{0}, \mathbb{1})$

By Lemma 2.5, $\mathbf{FB}(X)$, $\mathbf{FB}_{\text{rd}}(X)$, and $\mathbf{FB}_{\text{id,rd}}(X)$ satisfy all identities in E , E_{rd} , and $E_{\text{id,rd}}$, respectively. Hence $\mathbf{FB}(X)$ is a strong bimonoid, $\mathbf{FB}_{\text{rd}}(X)$ is a right-distributive strong bimonoid and $\mathbf{FB}_{\text{id,rd}}(X)$ is an idempotent right-distributive strong bimonoid.

Given $t \in \mathbf{T}(X)$, we abbreviate the congruence class $[t]_{=E}$ in $\mathbf{FB}(X)$ by $[t]_E$. Similarly, we denote $[t]_{=E_{\text{rd}}}$ and $[t]_{=E_{\text{id,rd}}}$ by $[t]_{\text{rd}}$ and $[t]_{\text{id,rd}}$, respectively.

Moreover, let $X/E = \{[x]_E \mid x \in X\}$, a generating set for $\mathbf{FB}(X)$, $X/\text{rd} = \{[x]_{\text{rd}} \mid x \in X\}$, a generating set for $\mathbf{FB}_{\text{rd}}(X)$, and $X/\text{id,rd} = \{[x]_{\text{id,rd}} \mid x \in X\}$, a generating set for $\mathbf{FB}_{\text{id,rd}}(X)$.

The following result is immediate by [Wec92, Sec. 3.2.4, Cor. 2] or by [BN98, Cor. 3.5.8, Thm. 3.5.14] combined with Lemma 2.6.

Proposition 3.3.

- (a) $\text{FB}(X)$ is a free strong bimonoid, freely generated by the set X/E .
- (b) $\text{FB}_{\text{rd}}(X)$ is a free right-distributive strong bimonoid, freely generated by the set X/rd .
- (c) $\text{FB}_{\text{id,rd}}(X)$ is a free idempotent right-distributive strong bimonoids, freely generated by the set $X/\text{id,rd}$. $\square$

4 Strong bimonoids of polynomials

The goal of this section is to develop our new concept of polynomials together with their operations of addition and multiplication. In particular, the aim is that for our polynomials, the multiplication is right-distributive over addition, but otherwise, “as free as possible” (in particular, in general not commutative or left-distributive). For this, we define congruence classes of particular terms, a class of polynomials, and a class of idempotency-reduced polynomials. For each of the three classes, we define an addition and a multiplication, and we show that they form strong bimonoids, right-distributive strong bimonoids, and idempotent right-distributive strong bimonoids, respectively. We also show that the multiplication in the right-distributive strong bimonoids is cancellative both from the right and the left. Then in the next section we will show that our strong bimonoids constitute the free objects in the classes of strong bimonoids, right-distributive strong bimonoids, respectively idempotent right-distributive strong bimonoids.

We start with the definition of particular terms, called simple terms, and the Σ_{sb} -algebra $\text{ST}(X)$ (cf. [DFTV24, Sect. 3]).

We call a term $s \in \text{T}(X)$ *simple*, if

- $s = \hat{0}$ or
- $s \neq \hat{0}$ and it contains neither $\hat{0}$, nor a subterm of the form $\hat{1} \hat{\times} s$, nor a subterm of the form $s \hat{\times} \hat{1}$.

Let $\text{ST}(X)$ denote the set of all simple terms in $\text{T}(X)$. Note that $\hat{1}$ is simple, hence e.g., $\hat{1} \hat{+} s \in \text{ST}(X)$ for each $s \in \text{ST}(X)$.

Next we define the Σ_{sb} -algebra $\text{ST}(X) = (\text{ST}(X), +_{\text{ST}}, \times_{\text{ST}}, \hat{0}, \hat{1})$ as follows:

- for each $s \in \text{ST}(X)$, let $s +_{\text{ST}} \hat{0} = \hat{0} +_{\text{ST}} s = s$ and $s \times_{\text{ST}} \hat{0} = \hat{0} \times_{\text{ST}} s = \hat{0}$,
- for each $s \in \text{ST}(X)$, let $s \times_{\text{ST}} \hat{1} = \hat{1} \times_{\text{ST}} s = s$,
- for every $s, t \in \text{ST}(X) \setminus \{\hat{0}, \hat{1}\}$, let $s +_{\text{ST}} t = s \hat{+} t$ and $s \times_{\text{ST}} t = s \hat{\times} t$.

Thus, on $\text{ST}(X) \setminus \{\hat{0}, \hat{1}\}$, the operations $+_{\text{ST}}$ and $\times_{\text{ST}}$ are the restrictions of $\hat{+}$ respectively $\hat{\times}$, but the rules for $\hat{0}$ and $\hat{1}$ are simplified to satisfy the usual algebraic laws.

Then we consider the set $\text{AC} = \{e_1, e_2, e_4\}$ of identities and the quotient algebra

$$\text{ST}(X)/=_{\text{AC}} = (\text{ST}(X)/=_{\text{AC}}, +_{\text{ST}}/=_{\text{AC}}, \times_{\text{ST}}/=_{\text{AC}}, [\hat{0}]_{=_{\text{AC}}}, [\hat{1}]_{=_{\text{AC}}}).$$

Lastly, we abbreviate the latter notation by $\text{N}_{\text{sb}}[X] = (\text{N}_{\text{sb}}[X], +, \times, 0, 1)$.

The following is immediate by Lemmas 2.4 and 2.5.

Proposition 4.1. The algebra $\text{N}_{\text{sb}}[X] = (\text{N}_{\text{sb}}[X], +, \times, 0, 1)$ is a strong bimonoid. $\square$

To investigate the structure of the elements of the strong bimonoid $\text{N}_{\text{sb}}[X]$, we need to describe structural properties of their representing simple terms. For this, next we consider sum terms and product terms, defined as follows.

Let $s \in \text{ST}(X)$. We say that s is a *sum term* if there are $s_1, s_2 \in \text{ST}(X) \setminus \{\hat{0}\}$ such that $s = s_1 \hat{+} s_2$ and, we say that s is a *product term* if there are $s_1, s_2 \in \text{ST}(X) \setminus \{\hat{0}, \hat{1}\}$ such that $s = s_1 \hat{\times} s_2$.

Subsequently, to describe the structure of sum terms and product terms, the following simplification of notation will be useful.

Let $n \geq 2$ and $s, s_1, \dots, s_n \in \text{ST}(X)$. We will regard the expressions $s_1 \hat{+} \dots \hat{+} s_n$ and $s_1 \hat{\times} \dots \hat{\times} s_n$ as terms where, for notational ease in our denotation, as usual, we left out some parentheses. Moreover, we will write $s = s_1 \hat{+} \dots \hat{+} s_n$ (respectively, $s = s_1 \hat{\times} \dots \hat{\times} s_n$), if $s_1 \hat{+} \dots \hat{+} s_n$ (respectively, $s_1 \hat{\times} \dots \hat{\times} s_n$) is obtained from s in that way. Formally, $s = s_1 \hat{+} \dots \hat{+} s_n$ means that there exists a term $c \in T_{\{\hat{+}\}}(Z_n)$ in which each of the variables in Z_n occurs exactly once and the order of these variables is $z_1, \dots, z_n$, and we obtain s by replacing z_i in c by s_i , for each $i \in [n]$. If this is the case, then we write $s = c[s_1, \dots, s_n]$. We define $s = s_1 \hat{\times} \dots \hat{\times} s_n$ analogously with $c \in T_{\{\hat{\times}\}}(Z_n)$. In fact, $s_1 \hat{+} \dots \hat{+} s_n$ and $s_1 \hat{\times} \dots \hat{\times} s_n$ are similar to the usual flattening of the term s (cf. [BP85, Sect. 5]).

If $s = s_1 \hat{+} \dots \hat{+} s_n$ and, for each $i \in [n]$, the term s_i is a product term or $s_i \in X \cup \{\hat{1}\}$, then we call $s_1 \hat{+} \dots \hat{+} s_n$ a *sum-product decomposition* of s . Analogously, if $s = s_1 \hat{\times} \dots \hat{\times} s_n$ and, for each $i \in [n]$, the term s_i is a sum term or $s_i \in X$, then we call $s_1 \hat{\times} \dots \hat{\times} s_n$ a *product-sum decomposition* of s .

For instance, let $s = ((x \hat{\times} y) \hat{+} \hat{1}) \hat{+} (z \hat{\times} x)$. Then $(x \hat{\times} y) \hat{+} \hat{1} \hat{+} (z \hat{\times} x)$ is a sum-product decomposition of s with $c = (z_1 \hat{+} z_2) \hat{+} z_3$, $s_1 = x \hat{\times} y$, $s_2 = \hat{1}$, and $s_3 = z \hat{\times} x$. Hence we also write $s = (x \hat{\times} y) \hat{+} \hat{1} \hat{+} (z \hat{\times} x)$. Analogously, let $s = (x \hat{\times} (\hat{1} \hat{+} y)) \hat{\times} (x \hat{+} z)$. Then $x \hat{\times} (\hat{1} \hat{+} y) \hat{\times} (x \hat{+} z)$ is a product-sum decomposition of s with $c = (z_1 \hat{\times} z_2) \hat{\times} z_3$, $s_1 = x$, $s_2 = \hat{1} \hat{+} y$, and $s_3 = x \hat{+} z$, i.e., we write $s = x \hat{\times} (\hat{1} \hat{+} y) \hat{\times} (x \hat{+} z)$.

By considering the structure of sum terms and product terms, the following is immediate.

Observation 4.2.

- (a) Each sum term $s \in \text{ST}(X)$ has a unique sum-product decomposition $s = s_1 \hat{+} \dots \hat{+} s_n$.
- (b) Each product term $s \in \text{ST}(X)$ has a unique product-sum decomposition $s = s_1 \hat{\times} \dots \hat{\times} s_n$. □

Lemma 4.3. For every $s, t \in \text{ST}(X) \setminus \{\hat{0}, \hat{1}\}$, we have $s =_{\text{AC}} t$ if and only if one of the following two conditions hold:

- (a) both s and t are sum terms, and if $s = s_1 \hat{+} \dots \hat{+} s_n$ and $t = t_1 \hat{+} \dots \hat{+} t_k$ are their sum-product decompositions, then we have $k = n$ and there is a permutation $\varphi : [n] \rightarrow [n]$ such that $s_i =_{\text{AC}} t_{\varphi(i)}$ for each $i \in [n]$.
- (b) both s and t are product terms, and if $s = s_1 \hat{\times} \dots \hat{\times} s_n$ and $t = t_1 \hat{\times} \dots \hat{\times} t_k$ are their product-sum decompositions, then we have $k = n$ and $s_i =_{\text{AC}} t_i$ for each $i \in [n]$.

Proof. By Lemma 2.6, $s =_{\text{AC}} t$ is equivalent to $s \Leftrightarrow_{\text{AC}}^* t$. We will use this fact in the rest of the proof.

It is clear that any of the conditions (a) and (b) implies $s \Leftrightarrow_{\text{AC}}^* t$ and hence $s =_{\text{AC}} t$.

Now assume that $s \Leftrightarrow_{\text{AC}}^* t$. First we claim that either both s and t are sum terms or they are both product terms. For this, let $s_1, s_2, t_1, t_2 \in \text{ST}(X)$ such that $s = s_1 \hat{+} s_2$ and $t = t_1 \hat{\times} t_2$. Then $s_1 \hat{+} s_2 \Leftrightarrow_{\text{AC}}^* t_1 \hat{\times} t_2$ is impossible because by using identities of AC, we cannot change the root symbol $\hat{+}$ of $s_1 \hat{+} s_2$ to $\hat{\times}$. Our claim follows.

We continue the proof with case distinction. First we consider the case that both s and t are sum terms. Consider their sum-product decompositions $s = s_1 \hat{+} \dots \hat{+} s_n$ and $t = t_1 \hat{+} \dots \hat{+} t_k$. By our assumption, we have

$$s = s_1 \hat{+} \dots \hat{+} s_n \Leftrightarrow_{AC}^* t_1 \hat{+} \dots \hat{+} t_k = t . \quad (2)$$

Each s_i is a product term or is in $X \cup \{\hat{1}\}$. Hence, if we apply the identities of AC inside some term s_i , then this cannot change the root of s_i , hence the result is again a product term (or the same element of $X \cup \{\hat{1}\}$). The only other way to apply an identity of AC to the term $s_1 \hat{+} \dots \hat{+} s_n$ is to use identity e_1 (associativity of sum) to change the parenthesizing of this sum or to use identity e_2 (commutativity of sum) to interchange some summands s_i, s_j . In each case, we obtain again a sum-product decomposition with the same number of summands. Thus $k = n$, and the identities e_1, e_2 can change the order of the summands. Therefore, (2) implies also that there is a permutation $\varphi : [n] \rightarrow [n]$ such that $s_i \Leftrightarrow_{AC}^* t_{\varphi(i)}$ for each $i \in [n]$. Hence condition (a) holds.

Now we consider the case that both s and t are product terms. Similarly as in the previous case, consider their product-sum decompositions $s = s_1 \hat{\times} \dots \hat{\times} s_n$ and $t = t_1 \hat{\times} \dots \hat{\times} t_k$.

If we apply the identities of AC inside some term s_i , then, by what we noted above, the result is again a sum term (or the same element of X). The only other way to apply an identity of AC to the term $s_1 \hat{\times} \dots \hat{\times} s_n$ is to use identity e_4 (associativity of product) to change the parenthesizing of the product. In each case, we obtain again a product-sum decomposition with the same number of factors. Thus $k = n$, the identity e_4 can change the parenthesizing of the product-sum decomposition, and $s_i \Leftrightarrow_{AC}^* t_i$ for each $i \in [n]$. Hence condition (b) holds. $\square$

Since in all of the following, AC-equivalence of simple terms will be very important for us, we include a further graph-theoretic characterization, also for later use for decision algorithms (see Lemma 6.1 and Corollaries 6.3 and 6.6). We will represent simple terms as labeled trees (i.e., particular labeled and directed graphs, cf. [AHU74]) as follows.

Let $\boxplus$ and $\boxtimes$ be two symbols with $\boxplus, \boxtimes \notin X \cup \{\hat{0}, \hat{1}\}$. For each simple term $s \in \text{ST}(X)$, we define the labeled tree $\bar{s}$ *corresponding to* s by case distinction and induction on $\text{size}(s)$ as follows.

- (a) If $s \in X \cup \{\hat{0}, \hat{1}\}$, then $\bar{s}$ is the tree with one node labeled by s .
- (b) Let s be a sum term with sum-product decomposition $s = s_1 \hat{+} \dots \hat{+} s_n$ and let $\bar{s}_1, \dots, \bar{s}_n$ the trees which correspond to $s_1, \dots, s_n$, respectively. Then $\bar{s}$ is the tree whose root is labeled by $\boxplus$ and for each $i \in [n]$ there is an edge from this root to the root of $\bar{s}_i$.
- (c) Let s be a product term with product-sum decomposition $s = s_1 \hat{\times} \dots \hat{\times} s_n$ and let $\bar{s}_1, \dots, \bar{s}_n$ the trees which correspond to $s_1, \dots, s_n$, respectively. Moreover, for each $i \in [n]$, let s'_i be the tree obtained from $\bar{s}_i$ by replacing its root label $y \in X \cup \{\hat{+}\}$ by the pair (i, y) . Then $\bar{s}$ is the tree consisting of its root and the trees $s'_1, \dots, s'_n$, where the root is labeled by $\boxtimes$ and for each $i \in [n]$ there is an edge from this root to the root of s'_i .

Clearly, for each $s \in \text{ST}(X)$, we can construct $\bar{s}$ in $O(n)$ time, where $n = \text{size}(s)$.

An *isomorphism* of two labeled trees is, as usual, a bijection preserving the labeling and the edge relation [AHU74]. Above, in (c), the particular relabeling of the roots will ensure that isomorphisms of trees have to preserve the order of the factors in product-sum decompositions.

The following result is well-known in the area of term rewriting (cf., e.g., [BKN87, AJTT17]). We include a short proof for completeness and ease of the reader.

Proposition 4.4. Let $s, t \in \text{ST}(X)$ be simple terms. Then $s =_{\text{AC}} t$ if and only if $\bar{s}$ is isomorphic to $\bar{t}$.

Proof. We proceed by induction on $\text{size}(s)$ and case distinction. If $s \in X \cup \{\hat{0}, \hat{1}\}$, the result is immediate.

Therefore assume now that s is a sum term with sum-product decomposition $s = s_1 \hat{+} \dots \hat{+} s_n$. First assume that $s =_{\text{AC}} t$. Then, by Lemma 4.3(a), t is a sum term with a sum-product decomposition $t = t_1 \hat{+} \dots \hat{+} t_n$ and there is a bijection $\varphi : [n] \rightarrow [n]$ such that $s_i =_{\text{AC}} t_{\varphi(i)}$ for each $i \in [n]$. By induction hypothesis, for each $i \in [n]$, there is an isomorphism ψ_i from $\bar{s}_i$ to $\bar{t}_i$. Let ψ be the mapping which maps the root of $\bar{s}$ to the root of $\bar{t}$ and is the joint extension of the mappings ψ_i ($i \in [n]$). Then ψ is an isomorphism from $\bar{s}$ to $\bar{t}$.

Second, assume there is an isomorphism ψ from $\bar{s}$ to $\bar{t}$. Then ψ maps the root of $\bar{s}$ to $\bar{t}$. Hence these two roots are both labeled with $\boxplus$, and t is a sum term with a sum-product decomposition $t = t_1 \hat{+} \dots \hat{+} t_k$. Since ψ maps $\bar{s}$ isomorphically to $\bar{t}$, we obtain $k = n$, and ψ induces a bijection $\varphi : [n] \rightarrow [n]$ such that for each $i \in [n]$, ψ maps $\bar{s}_i$ to $\bar{t}_{\varphi(i)}$. By induction hypothesis, we obtain $s_i =_{\text{AC}} t_{\varphi(i)}$ for each $i \in [n]$. Then Lemma 4.3(a) implies $s =_{\text{AC}} t$.

Next, let s be a product term with product-sum decomposition $s = s_1 \hat{\times} \dots \hat{\times} s_n$. If $s =_{\text{AC}} t$, we proceed similarly as above, using Lemma 4.3(b), and we obtain that $\bar{s}$ is isomorphic to $\bar{t}$.

Conversely, assume there is an isomorphism ψ from $\bar{s}$ to $\bar{t}$. Now the roots of $\bar{s}$ and $\bar{t}$ are both labeled with $\boxtimes$ and correspond to each other by ψ . Hence t is a product term with a product-sum decomposition $t = t_1 \hat{\times} \dots \hat{\times} t_k$.

Consider the trees $\bar{s}_i, s'_i$ ($i \in [n]$) and the trees $\bar{t}_j, t'_j$ ($j \in [k]$) occurring in the constructions of $\bar{s}$ and $\bar{t}$. Since ψ maps $\bar{s}$ isomorphically to $\bar{t}$, we obtain $k = n$ and that there is a bijection $\varphi : [n] \rightarrow [n]$ such that for each $i \in [n]$, ψ maps s'_i isomorphically to $t'_{\varphi(i)}$. Since ψ preserves the labelings, it follows that $i = \varphi(i)$, for each $i \in [n]$. Moreover, $\bar{s}_i$ is isomorphic to $\bar{t}_i$, and by induction hypothesis we obtain that $s_i =_{\text{AC}} t_i$, for each $i \in [n]$. Then Lemma 4.3(b) implies $s =_{\text{AC}} t$. $\square$

Next we turn to our investigation of the strong bimonoid $\mathbb{N}_{\text{sb}}[X]$. Since in $\mathbb{N}_{\text{sb}}[X]$ the addition is associative and commutative and the multiplication is associative, in the following as usual we will write sums and (ordered) products of several elements of $\mathbb{N}_{\text{sb}}[X]$ often without parentheses, where multiplication binds stronger than addition.

In the following, we abbreviate $X =_{\text{AC}}$ by X/AC and $[s]_{=\text{AC}}$ by $[s]_{\text{AC}}$ for each $s \in \text{ST}(X)$. Hence $X/\text{AC} = \{[x]_{\text{AC}} \mid x \in X\}$, where $[x]_{\text{AC}} = \{x\}$ for each $x \in X$.

The elements of $\mathbb{N}_{\text{sb}}[X]$ are AC-congruence classes of simple terms. Therefore we name them *simple term classes*. For the following, it will be important to have uniqueness results for the representation of these simple term classes. We will employ sum terms and product terms and their congruence classes, called, respectively, sum classes and product classes: A simple term class $p \in \mathbb{N}_{\text{sb}}[X]$ is a *sum class* (*product class*) if there is a sum term (product term) $u \in \text{ST}(X)$ such that $p = [u]_{\text{AC}}$. Clearly, for each $p \in \mathbb{N}_{\text{sb}}[X]$, the following holds: if p is a sum class (product class), then there are $q, r \in \mathbb{N}_{\text{sb}}[X] \setminus \{0\}$ ($q, r \in \mathbb{N}_{\text{sb}}[X] \setminus \{0, 1\}$) such that $p = q + r$ ($p = q \times r$).

Let $n \geq 2$ and $p, p_1, \dots, p_n \in \mathbb{N}_{\text{sb}}[X]$. If $p = p_1 + \dots + p_n$, and, for each $i \in [n]$, p_i is a product class or $p_i \in X/\text{AC} \cup \{1\}$, then we call $p_1 + \dots + p_n$ a *sum-product decomposition* of p . If $p = p_1 \times \dots \times p_n$, and, for each $i \in [n]$, p_i is a sum class or $p_i \in X/\text{AC}$, then we call $p_1 \times \dots \times p_n$

a *product-sum decomposition* of p . Now we can show the following.

Lemma 4.5. (a) Each simple term class $p \in \mathbb{N}_{\text{sb}}[X] \setminus (X/\text{AC} \cup \{0, 1\})$ is either a sum class or a product class (but not both).

(b) Each sum class $p \in \mathbb{N}_{\text{sb}}[X]$ has a sum-product decomposition $p = p_1 + \dots + p_n$. Moreover, for every sum-product decomposition $p = q_1 + \dots + q_k$ of p we have $k = n$ and the sequence $q_1, \dots, q_n$ constitutes a permutation of $p_1, \dots, p_n$.

(c) Each product class $p \in \mathbb{N}_{\text{sb}}[X]$ has a unique product-sum decomposition $p = p_1 \times \dots \times p_n$.

Proof. Let $p \in \mathbb{N}_{\text{sb}}[X] \setminus (X/\text{AC} \cup \{0, 1\})$.

(a) Clearly, p is sum class or a product class. Assume that it is both a sum class and a product class. Then there is a sum term $s \hat{+} t$ and a product term $s' \hat{\times} t'$ in $\text{ST}(X)$ such that $[s \hat{+} t]_{\text{AC}} = p = [s' \hat{\times} t']_{\text{AC}}$. By Lemma 4.3, this is a contradiction.

(b) Let p be a sum class, i.e., let $p = [s]_{\text{AC}}$ for some sum term $s \in \text{ST}(X)$. Let $s = s_1 \hat{+} \dots \hat{+} s_n$ be the sum-product decomposition of s and, for each $i \in [n]$, let $p_i = [s_i]_{\text{AC}}$. Then we have $p = p_1 + \dots + p_n$, and this sum constitutes a sum-product decomposition of p .

We show that n is unique and the sequence $p_1, \dots, p_n$ is also unique up to a permutation.

For this, assume there $p = q_1 + \dots + q_k$ is a further sum-product decomposition of p , i.e., q_i is a product class or $q_i \in X/\text{AC} \cup \{1\}$ for each $i \in [k]$. Choose terms $t_1, \dots, t_k \in \text{ST}(X)$ such that, for each $i \in [k]$, $q_i = [t_i]_{\text{AC}}$ and t_i is a product term or $t_i \in X \cup \{\hat{1}\}$. Let $t \in \text{ST}(X)$ be a term with sum-product decomposition $t = t_1 \hat{+} \dots \hat{+} t_k$. Then $p = [t]_{\text{AC}}$. Hence $s =_{\text{AC}} t$. Since s and t sum terms, by Lemma 4.3(a) we obtain that $k = n$ and $t_1, \dots, t_n$ is, up to AC-equivalence of the summands, a permutation of $s_1, \dots, s_n$. Consequently, $q_1, \dots, q_n$ is a permutation of $p_1, \dots, p_n$. This proves (b).

(c) Now assume that p is a product class, i.e., there exists a product term $s \in \text{ST}(X)$ with $p = [s]_{\text{AC}}$. Let $s = s_1 \hat{\times} \dots \hat{\times} s_n$ be the product-sum decomposition of s and, for each $i \in [n]$, let $p_i = [s_i]_{\text{AC}}$. Then we have $p = p_1 \times \dots \times p_n$, and this constitutes a product-sum decomposition of p .

We show that n is unique and also the sequence $p_1, \dots, p_n$ is unique.

For this, let $p = q_1 \times \dots \times q_k$ be a further product-sum decomposition of p . Choose terms $t_1, \dots, t_k \in \text{ST}(X)$ such that, for each $i \in [k]$, $q_i = [t_i]_{\text{AC}}$ and the term t_i is a sum term or $t_i \in X$. Let $t \in \text{ST}(X)$ be a term with product-sum decomposition $t = t_1 \hat{\times} \dots \hat{\times} t_k$. Then $p = [t]_{\text{AC}}$. Hence $s =_{\text{AC}} t$. So, since s and t are product terms, by Lemma 4.3(b), we obtain that $k = n$ and $s_i =_{\text{AC}} t_i$ for each $i \in [n]$. Hence, also $p_i = q_i$ for each $i \in [n]$. This proves (c). $\square$

Clearly, if s, t are simple terms and $s =_{\text{AC}} t$, then by Lemma 2.6, we have $\text{size}(s) = \text{size}(t)$. Hence for each $p \in \mathbb{N}_{\text{sb}}[X]$ we define *the size of p* by $\text{size}(p) = \text{size}(s)$, where s is a term in $\text{ST}(X)$ with $p = [s]_{\text{AC}}$. Subsequently, in our proofs for a simple class $p \in \mathbb{N}_{\text{sb}}[X]$ we will often proceed by an induction over $\text{size}(p)$.

Next, we will define the subclass of polynomial terms in $\text{ST}(X)$ and then the corresponding subclass of polynomials in $\mathbb{N}_{\text{sb}}[X]$. This is motivated by the usual definition of polynomials in the free ring or semiring over X . More precisely, we want to capture those terms which we obtain from arbitrary simple terms by applying repeatedly right-distributivity, but not left-distributivity, of multiplication over addition (combined with associativity of multiplication).

First we define monomial terms and monomials. For this, we recall that the elements of $T_{\{\hat{\times}\}}(X)$ can be viewed as products of elements only from X , with any kind of parenthesizing.

Definition 4.6. The set of *monomial terms* is the set $T_{\{\hat{\times}\}}(X)$.

For each monomial term $t \in T_{\{\hat{\times}\}}(X)$, we call its congruence class $[t]_{AC}$ a *monomial*. The set of all monomials is the set

$$\{[x_1]_{AC} \times \dots \times [x_n]_{AC} \mid n \in \mathbb{N}_+ \text{ and } x_1, \dots, x_n \in X\}.$$

□

Definition 4.7. The set of *polynomial terms*, denoted by $PT(X)$, is the smallest subset U of $ST(X)$ satisfying the following conditions:

- (a) $\hat{0}$, $\hat{1}$, and all monomial terms are in U .
- (b) If $s, t \in U$ with $s \neq \hat{0} \neq t$, then $s \hat{+} t$ is in U .
- (c) If s is a monomial term and $t \in U$ with $t \notin \{\hat{0}, \hat{1}\}$, then $s \hat{\times} t$ is in U .

□

For every $s, t \in PT(X)$ with $s \neq \hat{0} \neq t$, the term $s \hat{+} t$ is called a *sum polynomial term*, and for every monomial term s and $t \in PT(X)$ with $t \notin \{\hat{0}, \hat{1}\}$, the term $s \hat{\times} t$ is called a *product polynomial term*.

For each polynomial term (respectively, sum polynomial term, product polynomial term) $t \in PT(X)$, we call its congruence class $[t]_{AC}$ a *polynomial* (respectively, a *sum polynomial*, a *product polynomial*).

Now, we let

$$\mathbb{N}_{rd}[X] = PT(X)/=_{AC} = \{[t]_{AC} \mid t \in PT(X)\},$$

and call $\mathbb{N}_{rd}[X]$ the set of all polynomials in $\mathbb{N}_{sb}[X]$. In particular, $0, 1 \in \mathbb{N}_{rd}[X]$. Subsequently, our goal is to obtain a right-distributive strong bimonoid structure on $\mathbb{N}_{rd}[X]$; this explains the subscript *rd*.

Observation 4.8. The set $\mathbb{N}_{rd}[X]$ is the smallest subset U of $\mathbb{N}_{sb}[X]$ satisfying the following conditions:

- (a) $0, 1$, and all monomials are in U .
- (b) If $p, q \in U$ with $p \neq 0 \neq q$, then $p + q$ is in U .
- (c) If m is a monomial and $q \in U$ with $q \notin \{0, 1\}$, then $m \times q$ is in U .

□

Clearly, for each $p \in \mathbb{N}_{rd}[X]$, the following holds: if p is a sum polynomial (product polynomial), then there are $q, r \in \mathbb{N}_{rd}[X] \setminus \{0\}$ (a monomial m and $q \in \mathbb{N}_{rd}[X] \setminus \{0, 1\}$) such that $p = q + r$ ($p = m \times q$, respectively).

The next lemma is analogous to Lemma 4.5 and states existence and uniqueness results for the representation of polynomials of $\mathbb{N}_{rd}[X]$.

Lemma 4.9. (a) Each polynomial $p \in \mathbb{N}_{rd}[X] \setminus (X/AC \cup \{0, 1\})$ is either a sum polynomial or a product polynomial (but not both).

(b) Each sum polynomial $p \in \mathbb{N}_{rd}[X]$ has a sum-product decomposition, $p = p_1 + \dots + p_n$, such that, for each $i \in [n]$, p_i is a product polynomial or $p_i \in X/AC \cup \{1\}$. Moreover, for every sum-product decomposition $p = q_1 + \dots + q_k$, we have $k = n$ and $q_1, \dots, q_n$ constitutes a permutation of $p_1, \dots, p_n$.

(c) For each product polynomial $p \in \mathbb{N}_{\text{rd}}[X]$ either of the following two conditions holds: p is a monomial or there are a unique monomial m and a unique sum polynomial q such that $p = m \times q$.

Proof. (a), (b) These parts are straightforward by induction on $\text{size}(p)$, using Lemma 4.5.

(c) By Observation 4.8, the set $\mathbb{N}_{\text{rd}}$ of polynomials can be obtained by closing the set containing $0, 1$ and all monomials under sums and under products from the left with monomials. Let $p \in \mathbb{N}_{\text{rd}}[X]$ be a product polynomial. By the above and Lemma 4.5, we have $p = m \times q$ for some monomial m and a polynomial q . We proceed by case distinction and induction on $\text{size}(p)$. If q is a monomial, we are done. If q is a sum polynomial, then the uniqueness of m and q follows from Lemma 4.5. Now assume that q is a product polynomial. By induction hypothesis, we have $q = m' \times q'$ for some monomial m' and a sum polynomial q' . Hence $p = (m \times m') \times q'$ as required. The uniqueness part follows again by Lemma 4.5. $\square$

Next we show that the set $\text{PT}(X)$ of polynomial terms is closed under AC-equivalence.

Lemma 4.10. For every $s \in \text{PT}(X)$ and $t \in \text{ST}(X)$, if $s =_{\text{AC}} t$, then also $t \in \text{PT}(X)$.

Proof. We proceed by case distinction and induction on $\text{size}(s)$. For this, assume that $t \in \text{ST}(X)$ with $s =_{\text{AC}} t$.

The statement obviously holds for $s = \hat{0}$ ($s = \hat{1}$) because in this case $t = \hat{0}$ ($t = \hat{1}$).

If s is a monomial term, then by Lemma 4.3, t is also a monomial term.

Now assume that s is a sum polynomial term. Then s has a sum-product decomposition $s = s_1 \hat{+} \dots \hat{+} s_n$ such that each s_i ($i \in [n]$) is an element of $X \cup \{\hat{1}\}$ or a product polynomial term. By Lemma 4.3, there is a sum-product decomposition $t = t_1 \hat{+} \dots \hat{+} t_n$ and, moreover, for each t_i there is an s_j with $s_j =_{\text{AC}} t_i$. By the induction hypothesis, each t_i is a polynomial term, hence t is a sum polynomial term.

Lastly, assume that s is a product polynomial term which is not a monomial term. By Lemma 4.9(c), there are a unique monomial m and a sum polynomial q with $[s]_{\text{AC}} = m \times q$. Hence there are a monomial term s' and a sum polynomial term s'' such that $m = [s']_{\text{AC}}$ and $q = [s'']_{\text{AC}}$. Then $t =_{\text{AC}} s =_{\text{AC}} s' \hat{\times} s''$. By Lemma 4.3(b), t is a product term and it has a product-sum decomposition $t = t' \hat{\times} t''$ with $s' =_{\text{AC}} t'$ and $s'' =_{\text{AC}} t''$. Hence, t' is a monomial term and t'' is a sum term and by induction hypothesis a polynomial term. Thus $t \in \text{PT}(X)$. $\square$

In an equivalent formulation, Lemma 4.10 says that if $s \in \text{PT}(X)$, then $[s]_{\text{AC}} \subseteq \text{PT}(X)$.

We note that $\mathbb{N}_{\text{rd}}[X]$ is closed under the addition $+$. However, it is not closed under the multiplication $\times$, since, e.g., for each $x \in X$, $p = 1 + [x]_{\text{AC}}$ and $q = [x]_{\text{AC}}$ are polynomials, but $p \times q = (1 + [x]_{\text{AC}}) \times [x]_{\text{AC}}$ is not a polynomial. Therefore, to equip $\mathbb{N}_{\text{rd}}[X]$ with a strong bimonoid structure, we can take the restriction of $+$ to $\mathbb{N}_{\text{rd}}[X]$, but we define a new multiplication $\times_{\text{rd}}$ on $\mathbb{N}_{\text{rd}}[X]$ so that, together with the $+$, we will obtain a right-distributive strong bimonoid. We define the operation $\times_{\text{rd}}$ as follows.

Definition 4.11. Let $q, r \in \mathbb{N}_{\text{rd}}[X]$. We define $q \times_{\text{rd}} r$ by case distinction and induction on $\text{size}(q)$ as follows. We put $q \times_{\text{rd}} 0 = 0 = 0 \times_{\text{rd}} q$ and $q \times_{\text{rd}} 1 = q = 1 \times_{\text{rd}} q$. Now let q, r be different from 0 and 1.

- (a) If q is a monomial, we let $q \times_{\text{rd}} r = q \times r$, a product polynomial.
- (b) Let q be a sum polynomial. By Lemma 4.9(b), we can write $q = q_1 + \dots + q_n$ where $n \geq 2$ and each q_i is 1, a monomial, or a product polynomial. By induction hypothesis, $q_i \times_{\text{rd}} r$ is already defined for each $i \in [n]$. Then we define $q \times_{\text{rd}} r = q_1 \times_{\text{rd}} r + \dots + q_n \times_{\text{rd}} r$. Note that the description of q as a sum of n number of 1's, monomials, or product polynomials is unique in the sense of Lemma 4.9(b). Therefore $q \times_{\text{rd}} r$ is well-defined, and it is a sum polynomial.
- (c) Let q be product polynomial which is not a monomial. By Lemma 4.9(c), there are a unique monomial m and a sum polynomial q' with $q = m \times q'$. By induction hypothesis, $q' \times_{\text{rd}} r$ is already defined. We define $q \times_{\text{rd}} r = m \times (q' \times_{\text{rd}} r)$. Since m and q' are unique, the product $q \times_{\text{rd}} r$ is well-defined and it is a product polynomial. $\square$

Given $q, r \in \mathbb{N}_{\text{rd}}[X]$ and polynomial terms $s, t \in \text{PT}(X)$ with $q = [s]_{\text{AC}}$ and $r = [t]_{\text{AC}}$, we have $q \times_{\text{rd}} r \in \mathbb{N}_{\text{rd}}[X]$. Hence, by the definition of $\mathbb{N}_{\text{rd}}[X]$, there is a polynomial term $u \in \text{PT}(X)$ such that $q \times_{\text{rd}} r = [u]_{\text{AC}}$. We could find such a polynomial term u by following the inductive procedure described above in Definition 4.11.

Next we wish to give a *direct* one-step construction for finding this polynomial term u from s and t . We call an element of $X \cup \{\hat{1}\}$ which occurs as a subterm of s also a *leaf of s* . Intuitively, we will perform the multiplication with the term t at all occurrences of the leaf $\hat{1}$ in s and at particular occurrences of leaves from X in s .

Formally, for any polynomial terms $s, t \in \text{PT}(X) \setminus \{\hat{0}\}$, we define the term $s\langle \hat{x}t \rangle$.

For this, first we define two auxiliary concepts. A subterm s' of s is called a *sum subterm of s* if s' is a sum term. Next, let v be a monomial term. We say that v *occurs as a summand in s* , if $s = v$ or v is a summand in a sum subterm of s , i.e., v is a child of a $\hat{+}$ -symbol of s . We note that if $\hat{1}$ occurs in s , then it occurs as a summand in s in the above sense.

Now we define $s\langle \hat{x}t \rangle$ as follows. We put $\hat{1}\langle \hat{x}t \rangle = t$ and $s\langle \hat{x}\hat{1} \rangle = s$. If $s \in X$ and $t \neq \hat{1}$, then we put $s\langle \hat{x}t \rangle = s\hat{x}t$.

If $\text{size}(s) \geq 2$, then we let $s\langle \hat{x}t \rangle$ be the term obtained from s as follows:

- whenever $\hat{1}$ occurs in s , then we replace this leaf $\hat{1}$ by t ,
- whenever $x \in X$ is the rightmost factor of a monomial term which occurs as a summand in s , then we replace this leaf x by $x\hat{x}t$.

We give some examples:

- $(x\hat{+}y)\langle \hat{x}t \rangle = (x\hat{x}t)\hat{+}(y\hat{x}t)$ and $(x\hat{x}y)\langle \hat{x}t \rangle = x\hat{x}(y\hat{x}t)$,
- $\left((x\hat{x}y)\hat{x}(\hat{1}\hat{+}(y\hat{x}z))\right)\langle \hat{x}t \rangle = (x\hat{x}y)\hat{x}(t\hat{+}(y\hat{x}(z\hat{x}t)))$,
- $\left((x\hat{x}(y\hat{+}z))\hat{+}(y\hat{+}(x\hat{x}y))\right)\langle \hat{x}t \rangle = (x\hat{x}((y\hat{x}t)\hat{+}(z\hat{x}t)))\hat{+}((y\hat{x}t)\hat{+}(x\hat{x}(y\hat{x}t)))$,
- $\left(x\hat{x}\left((y\hat{+}\hat{1})\hat{+}(\hat{1}\hat{+}(x\hat{x}y))\right)\right)\langle \hat{x}t \rangle = x\hat{x}\left(((y\hat{x}t)\hat{+}t)\hat{+}(t\hat{+}(x\hat{x}(y\hat{x}t)))\right)$.

Note that in the construction of $s\langle \hat{x}t \rangle$, the structure of s determines which occurrences of leaves of s get replaced; in particular, this does not depend on t . Clearly, $s\langle \hat{x}t \rangle$ is a simple term.

Observe that in case s is a sum term with sum-product decomposition $s = s_1\hat{+}\dots\hat{+}s_n$, then $s\langle \hat{x}t \rangle = s_1\langle \hat{x}t \rangle\hat{+}\dots\hat{+}s_n\langle \hat{x}t \rangle$.

In case s is a product term such that $s = s_1\hat{x}s_2$ with a monomial term s_1 and a polynomial sum term s_2 , the product-sum decomposition of $s = s_1\hat{x}s_2$ has the sum term s_2 as its rightmost

factor. Consequently, all leaves of s which are rightmost factors of some monomial term occurring as a summand in s , are leaves of s_2 . Hence $s\langle\hat{\times}t\rangle = s_1\hat{\times}(s_2\langle\hat{\times}t\rangle)$.

Now we can show that in the setting above, we obtain our goal with the polynomial term $u = s\langle\hat{\times}t\rangle$:

Lemma 4.12. Let $s, t \in \text{PT}(X) \setminus \{\hat{0}\}$. Then $s\langle\hat{\times}t\rangle \in \text{PT}(X)$ and $[s]_{\text{AC}} \times_{\text{rd}} [t]_{\text{AC}} = [s\langle\hat{\times}t\rangle]_{\text{AC}}$.

Proof. We proceed by induction on the size of s . If $s = \hat{1}$ or $t = \hat{1}$, the result is clear. Now we assume that $s \neq \hat{1} \neq t$. If $s \in X$, we have $[s]_{\text{AC}} \times_{\text{rd}} [t]_{\text{AC}} = [s]_{\text{AC}} \times [t]_{\text{AC}} = [s\hat{\times}t]_{\text{AC}} = [s\langle\hat{\times}t\rangle]_{\text{AC}}$. Hence let $\text{size}(s) \geq 2$.

First, assume that s is a monomial term, so $s = x_1\hat{\times}\dots\hat{\times}x_n$ for some $n \geq 2$ and $x_i \in X$ for each $i \in [n]$. Then $[s]_{\text{AC}} \times_{\text{rd}} [t]_{\text{AC}} = [s]_{\text{AC}} \times [t]_{\text{AC}} = [s\hat{\times}t]_{\text{AC}} = [x_1\hat{\times}\dots\hat{\times}x_{n-1}\hat{\times}(x_n\hat{\times}t)]_{\text{AC}} = [s\langle\hat{\times}t\rangle]_{\text{AC}}$, as claimed.

Next, assume that s is a sum term with sum-product decomposition $s = s_1\hat{+}\dots\hat{+}s_n$ and polynomial terms $s_1, \dots, s_n$. Then $s\langle\hat{\times}t\rangle = s_1\langle\hat{\times}t\rangle\hat{+}\dots\hat{+}s_n\langle\hat{\times}t\rangle$ and by our induction assumption we obtain $s_i\langle\hat{\times}t\rangle \in \text{PT}(X)$ and $[s_i]_{\text{AC}} \times_{\text{rd}} [t]_{\text{AC}} = [s_i\langle\hat{\times}t\rangle]_{\text{AC}}$ for each $i \in [n]$. So, $s\langle\hat{\times}t\rangle \in \text{PT}(X)$ and

$$\begin{aligned} [s]_{\text{AC}} \times_{\text{rd}} [t]_{\text{AC}} &= [s_1]_{\text{AC}} \times_{\text{rd}} [t]_{\text{AC}} + \dots + [s_n]_{\text{AC}} \times_{\text{rd}} [t]_{\text{AC}} = [s_1\langle\hat{\times}t\rangle]_{\text{AC}} + \dots + [s_n\langle\hat{\times}t\rangle]_{\text{AC}} \\ &= [s_1\langle\hat{\times}t\rangle\hat{+}\dots\hat{+}s_n\langle\hat{\times}t\rangle]_{\text{AC}} = [s\langle\hat{\times}t\rangle]_{\text{AC}}. \end{aligned}$$

Finally, let $s = s_1\hat{\times}s_2$ with a monomial term s_1 and a polynomial sum term s_2 . By applying our induction hypothesis to s_2 , we obtain $[s]_{\text{AC}} \times_{\text{rd}} [t]_{\text{AC}} = [s_1]_{\text{AC}} \times ([s_2]_{\text{AC}} \times_{\text{rd}} [t]_{\text{AC}}) = [s_1]_{\text{AC}} \times [s_2\langle\hat{\times}t\rangle]_{\text{AC}}$. On the other hand, as noted above we have $s\langle\hat{\times}t\rangle = (s_1\hat{\times}s_2)\langle\hat{\times}t\rangle = s_1\hat{\times}(s_2\langle\hat{\times}t\rangle)$. Thus $[s\langle\hat{\times}t\rangle]_{\text{AC}} = [s_1\hat{\times}(s_2\langle\hat{\times}t\rangle)]_{\text{AC}} = [s_1]_{\text{AC}} \times [s_2\langle\hat{\times}t\rangle]_{\text{AC}}$, and the result follows. $\square$

Next we show that the direct one-step construction $..\langle\hat{\times}..\rangle$, as a binary operation, is associative.

Lemma 4.13. For every $s, t, u \in \text{PT}(X) \setminus \{\hat{0}\}$, we have $s\langle\hat{\times}(t\langle\hat{\times}u\rangle)\rangle = (s\langle\hat{\times}t\rangle)\langle\hat{\times}u\rangle$.

Proof. The statement is obvious if some of s, t and u are equal to $\hat{1}$.

Therefore assume that $s, t, u \in \text{PT}(X) \setminus \{\hat{0}, \hat{1}\}$. We observe that the leaves of s which get replaced in the construction of $s\langle\hat{\times}t\rangle$ are the same as those leaves of s which get replaced in the construction of $s\langle\hat{\times}(t\langle\hat{\times}u\rangle)\rangle$. Moreover, the leaves of t which get replaced in the construction of $t\langle\hat{\times}u\rangle$ correspond to those leaves of copies of t in $s\langle\hat{\times}t\rangle$ which get replaced in the construction of $(s\langle\hat{\times}t\rangle)\langle\hat{\times}u\rangle$. This implies the statement. $\square$

Now we can show one of our main results.

Theorem 4.14. $\mathbb{N}_{\text{rd}}[X] = (\mathbb{N}_{\text{rd}}[X], +, \times_{\text{rd}}, 0, 1)$ is a right-distributive strong bimonoid.

Proof. Since $\mathbb{N}_{\text{rd}}[X]$ is closed under addition by $+$, $(\mathbb{N}_{\text{rd}}[X], +, 0)$ is a commutative monoid.

Now let $p, q, r \in \mathbb{N}_{\text{rd}}[X]$. We claim that $p \times_{\text{rd}} (q \times_{\text{rd}} r) = (p \times_{\text{rd}} q) \times_{\text{rd}} r$. We may assume that $p, q, r \neq 0$ because otherwise the statement is trivial. Choose polynomial terms $s, t, u \in \text{PT}(X)$ with $p = [s]_{\text{AC}}$, $q = [t]_{\text{AC}}$ and $r = [u]_{\text{AC}}$. By Lemmas 4.12 and 4.13, we obtain

$$\begin{aligned} p \times_{\text{rd}} (q \times_{\text{rd}} r) &= [s]_{\text{AC}} \times_{\text{rd}} [t\langle\hat{\times}u\rangle]_{\text{AC}} = [s\langle\hat{\times}(t\langle\hat{\times}u\rangle)\rangle]_{\text{AC}} = [(s\langle\hat{\times}t\rangle)\langle\hat{\times}u\rangle]_{\text{AC}} = [s\langle\hat{\times}t\rangle]_{\text{AC}} \times_{\text{rd}} r \\ &= (p \times_{\text{rd}} q) \times_{\text{rd}} r, \end{aligned}$$

as needed. Thus $(\mathbb{N}_{\text{rd}}[X], \times_{\text{rd}}, 1)$ is a monoid.

For right-distributivity, we have to show that $(p + q) \times_{\text{rd}} r = p \times_{\text{rd}} r + q \times_{\text{rd}} r$. We may assume that $p, q, r \neq 0$. Choose polynomial terms $s, t, u \in \text{PT}(X)$ with $p = [s]_{\text{AC}}, q = [t]_{\text{AC}}$ and $r = [u]_{\text{AC}}$. By Lemma 4.12, we obtain

$$\begin{aligned} (p + q) \times_{\text{rd}} r &= ([s + t]_{\text{AC}}) \times_{\text{rd}} [u]_{\text{AC}} = [(s + t) \langle \hat{\times} u \rangle]_{\text{AC}} = [s \langle \hat{\times} u \rangle + t \langle \hat{\times} u \rangle]_{\text{AC}} = [s \langle \hat{\times} u \rangle]_{\text{AC}} + [t \langle \hat{\times} u \rangle]_{\text{AC}} \\ &= (p \times_{\text{rd}} r) + (q \times_{\text{rd}} r), \end{aligned}$$

as needed. Hence $\mathbb{N}_{\text{rd}}[X]$ is a right-distributive strong bimonoid. $\square$

In the following, we will prove a general cancellativity result for the multiplication $\times_{\text{rd}}$ of the right-distributive strong bimonoid $\mathbb{N}_{\text{rd}}[X]$. As preparation, we begin with a natural particular case. For a simple term class $p \in \mathbb{N}_{\text{sb}}[X]$ and $n \in \mathbb{N}$, we let $n \cdot p = p + \dots + p$ (n summands). First we show:

Lemma 4.15. Let $p, q \in \mathbb{N}_{\text{sb}}[X]$ and $n \in \mathbb{N}_+$. Then $n \cdot p = n \cdot q$ implies $p = q$.

Proof. Assume $n \cdot p = n \cdot q$. First, consider that $p \in X$ or p is a product class. Then $n \cdot p = p + \dots + p$ is the sum-product decomposition of $n \cdot p$. If q was a sum class, the sum-product decomposition of $n \cdot q$ would contain at least $2n$ summands. This contradicts Lemma 4.5(b). Hence also $q \in X$ or q is a product class. Then $n \cdot q = q + \dots + q$ is the sum-product decomposition of $n \cdot q$. Then Lemma 4.5(b) implies $p = q$.

Therefore we may assume that p and q are sum classes. Let $p = p_1 + \dots + p_k$ and $q = q_1 + \dots + q_{k'}$ be their sum-product decompositions. Then $n \cdot p$ and $n \cdot q$ have sum-product decompositions with $n \cdot k$ resp. $n \cdot k'$ summands. Then by Lemma 4.5(b), we have $k = k'$ and there is a bijection π from the summands of the sum-product decomposition $n \cdot p = n \cdot p_1 + \dots + n \cdot p_k$ to the summands of the sum-product decomposition $n \cdot q = n \cdot q_1 + \dots + n \cdot q_k$ preserving and reflecting equality of the summands. Let $I \subseteq \{1, \dots, k\}$ such that the classes p_i ($i \in I$) are pairwise different and $\{p_i \mid i \in I\} = \{p_1, \dots, p_k\}$. Then also the elements $\pi(p_i)$ ($i \in I$) are pairwise different and $\{\pi(p_i) \mid i \in I\} = \{q_1, \dots, q_k\}$. It follows that for each $i \in I$ we have $|\{j \in \{1, \dots, k\} \mid p_j = p_i\}| = |\{j \in \{1, \dots, k\} \mid q_j = \pi(p_i)\}|$. Thus $p = p_1 + \dots + p_k = q_1 + \dots + q_k = q$, as claimed. $\square$

Next, we prove the following general cancellation result for the strong bimonoid of polynomials. Note that usually in such cancellativity results one considers two products where either the two left factors or the two right factors are equal; here we only require the much weaker property that the two right factors r, r' have the same size. In the semiring $\mathbb{N}[X] = (\mathbb{N}[X], +, \cdot, 0, 1)$, the result corresponding to Theorem 4.16 clearly does not hold, since, e.g., $(x + 1)(x + x) = xx + xx + x + x = (x + x)(x + 1)$ and $\text{size}(x + x) = \text{size}(x + 1)$. Note that, due to the left-distributivity, the multiplication and the equality in $\mathbb{N}[X]$ are different from the one in $\mathbb{N}_{\text{rd}}[X]$; this explains why the stronger result of Theorem 4.16 does not hold in $\mathbb{N}[X]$.

Theorem 4.16. Let $p, q, r, r' \in \mathbb{N}_{\text{rd}}[X] \setminus \{0\}$ with $r \neq 1 \neq r'$ such that $p \times_{\text{rd}} r = q \times_{\text{rd}} r'$ and $\text{size}(r) = \text{size}(r')$. Then $p = q$ and $r = r'$.

Proof. We proceed by induction on p . If $p \neq 1$, by $r \neq 1$ we obtain $\text{size}(p \times_{\text{rd}} r) > \text{size}(r)$. Together with the assumption that $\text{size}(r) = \text{size}(r')$, this implies that $p = 1$ if and only if $q = 1$. Hence we may assume that $p \neq 1 \neq q$.

First assume that $p \in X/\text{AC}$ or p is a product polynomial. Then $p \times_{\text{rd}} r$, hence also $q \times_{\text{rd}} r'$, is a product polynomial. Thus also $q \in X/\text{AC}$ or q is a product polynomial. We write $p = [x]_{\text{AC}} \times p'$ and $q = [y]_{\text{AC}} \times q'$ with $x, y \in X$ and $p', q' \in \mathbb{N}_{\text{rd}}[X] \setminus \{0\}$ (possibly, $p' = 1$ or $q' = 1$). Then $p \times_{\text{rd}} r = [x]_{\text{AC}} \times (p' \times_{\text{rd}} r)$ and $q \times_{\text{rd}} r' = [y]_{\text{AC}} \times (q' \times_{\text{rd}} r')$. Choose $u, v \in \text{PT}(X)$ with $p' \times_{\text{rd}} r = [u]_{\text{AC}}$ and $q' \times_{\text{rd}} r' = [v]_{\text{AC}}$. We have $\overline{p \times_{\text{rd}} r} = \overline{[x \hat{\times} u]_{\text{AC}}}$ and $\overline{q \times_{\text{rd}} r'} = \overline{[y \hat{\times} v]_{\text{AC}}}$. By Proposition 4.4, there is an isomorphism φ from $\overline{x \hat{\times} u}$ onto $\overline{y \hat{\times} v}$. The labeled graph $\overline{x \hat{\times} u}$ has $\boxtimes$ as a root and children depending on the structure of u . If u is a sum term, the children of $\boxtimes$ in $\overline{x \hat{\times} u}$ are labeled with $(1, x)$ and $(2, \boxplus)$. If $u \in X$, the children of $\boxtimes$ are labeled with $(1, x)$ and $(2, u)$. If u is a product polynomial term with product-sum decomposition $u = u_1 \hat{\times} \dots \hat{\times} u_n$, then $\boxtimes$ has $n + 1$ children. The first child is labeled with $(1, x)$. If u is a monomial, then the further n children are labeled with $(2, u_1), \dots, (n + 1, u_n)$, otherwise, u_n is a sum term and the children are labeled with $(2, u_1), \dots, (n, u_{n-1}), (n + 1, \boxplus)$.

We have a similar description of the labeled graph $\overline{y \hat{\times} v}$. It follows that φ maps the child of the root of $\overline{x \hat{\times} u}$ labeled with $(1, x)$ onto the child of the root of $\overline{y \hat{\times} v}$ labeled with $(1, y)$ and that φ induces an isomorphism from $\bar{u}$ onto $\bar{v}$. Thus $x = y$, and by Proposition 4.4, we obtain $[u]_{\text{AC}} = [v]_{\text{AC}}$. Hence $p' \times_{\text{rd}} r = [u]_{\text{AC}} = [v]_{\text{AC}} = q' \times_{\text{rd}} r'$. By our induction hypothesis, we obtain $p' = q'$ and $r = r'$, showing also $p = q$, as claimed.

Second, assume that p , and by the above hence also q , is a sum polynomial. Write $p = p_1 + \dots + p_k$ and $q = q_1 + \dots + q_n$ where $k, n \geq 2$ and for each $i \in [k]$ and $j \in [n]$, p_i and q_j are product polynomials or elements of $X/\text{AC} \cup \{1\}$. Then $p \times_{\text{rd}} r = p_1 \times_{\text{rd}} r + \dots + p_k \times_{\text{rd}} r$ and $q \times_{\text{rd}} r' = q_1 \times_{\text{rd}} r' + \dots + q_n \times_{\text{rd}} r'$.

Now consider the sum-product decomposition of $p_1 \times_{\text{rd}} r + \dots + p_k \times_{\text{rd}} r$ and the sum-product decomposition of $q_1 \times_{\text{rd}} r' + \dots + q_n \times_{\text{rd}} r'$. Note that if $i \in [k]$ and $p_i = 1$, then $p_i \times_{\text{rd}} r = r$. Moreover, if $i \in [k]$ and $p_i \neq 1$, then $p_i \in X/\text{AC}$ or p_i is a product polynomial, hence, using $r \neq 1$ in case $p_i \in X/\text{AC}$, we obtain that $p_i \times_{\text{rd}} r$ is a product polynomial and thus appears as a summand in the sum-product decomposition of $p_1 \times_{\text{rd}} r + \dots + p_k \times_{\text{rd}} r$ and that $\text{size}(p_i \times_{\text{rd}} r) > \text{size}(r)$. A similar observation holds for the sum-product decomposition of $q_1 \times_{\text{rd}} r' + \dots + q_n \times_{\text{rd}} r'$.

By Lemma 4.9(b), there is a bijection φ which maps the summands of the first sum-product decomposition onto equal summands of the second sum-product decomposition. By the above size considerations and $\text{size}(r) = \text{size}(r')$, it follows that φ maps the set $\{p_i \times_{\text{rd}} r \mid p_i \neq 1, i \in [k]\}$ bijectively onto the set $\{q_j \times_{\text{rd}} r' \mid q_j \neq 1, j \in [n]\}$ (preserving the possible multiplicities of the summands contained in these sets). Moreover, if $i \in [k]$, $j \in [n]$ with $p_i \neq 1 \neq q_j$ and $\varphi(p_i \times_{\text{rd}} r) = q_j \times_{\text{rd}} r'$, then $p_i \times_{\text{rd}} r = q_j \times_{\text{rd}} r'$, so $p_i = q_j$ by our induction hypothesis, and, provided that there are such $i \in [k]$ and $j \in [n]$ as described, we also obtain $r = r'$ by our induction hypothesis. Consequently, $\sum_{i \in [k], p_i \neq 1} p_i = \sum_{j \in [n], q_j \neq 1} q_j$.

Now let $k_1 = |\{i \in [k] \mid p_i = 1\}|$ and $n_1 = |\{j \in [n] \mid q_j = 1\}|$. Then φ also maps the sum-product decomposition of $k_1 \cdot r$ onto the sum-product decomposition of $n_1 \cdot r'$. Thus $k_1 \cdot r = n_1 \cdot r'$. Hence $k_1 \cdot \text{size}(r) + (k_1 - 1) = \text{size}(k_1 \cdot r) = \text{size}(n_1 \cdot r') = n_1 \cdot \text{size}(r') + (n_1 - 1)$, showing $k_1 = n_1$ since $\text{size}(r) = \text{size}(r')$. Thus $k_1 \cdot r = n_1 \cdot r' = k_1 \cdot r'$. Then, provided that $k_1 \neq 0$, Lemma 4.15 implies $r = r'$. Hence, in each case we have $r = r'$. As shown above, we have $|\{i \in [k] \mid p_i \neq 1\}| = |\{j \in [n] \mid q_j \neq 1\}|$. Together with $k_1 = n_1$, this implies $k = n$. Consequently, $p = p_1 + \dots + p_k = q_1 + \dots + q_k = q$, as claimed. $\square$

Clearly, Theorem 4.16 does not hold if $r = 1$ and $r' \neq 1$, or vice versa, because $[x] \times_{\text{rd}} 1 = 1 \times_{\text{rd}} [x]$ and $\text{size}(1) = \text{size}([x])$, but $1 \neq [x]$.

We note that Theorem 4.16 generalizes the following (almost trivial) observation on non-commutative free monoids:

If $p, q, r, r' \in X^*$ such that $pr = qr'$ and $\text{size}(r) = \text{size}(r')$, then $p = q$ and $r = r'$.

Indeed, the above observation is contained in Theorem 4.16, because the free monoid X^* is isomorphic to the monoid generated by X/AC in $\mathbb{N}_{\text{rd}}[X]$ with $\times_{\text{rd}}$.

Now we can show that the multiplication $\times_{\text{rd}}$ in $\mathbb{N}_{\text{rd}}[X]$ is cancellative both from the left and the right. We will use right cancellativity later in the proof of Lemma 4.23 and Theorem 4.26, and then also in Lemma 7.6.

Corollary 4.17. Let $p, q, r, r' \in \mathbb{N}_{\text{rd}}[X] \setminus \{0\}$.

- (a) If $p \times_{\text{rd}} r = p \times_{\text{rd}} r'$, then $r = r'$.
- (b) If $p \times_{\text{rd}} r = q \times_{\text{rd}} r$, then $p = q$.

Proof. (a) Assume that $p \times_{\text{rd}} r = p \times_{\text{rd}} r'$. Choose $s, u, v \in \text{PT}(X)$ with $p = [s]_{\text{AC}}$, $r = [u]_{\text{AC}}$, and $r' = [v]_{\text{AC}}$. By Lemma 4.12, we obtain $s\langle \hat{\times} u \rangle =_{\text{AC}} s\langle \hat{\times} v \rangle$, so $\text{size}(s\langle \hat{\times} u \rangle) = \text{size}(s\langle \hat{\times} v \rangle)$. It follows that $u = \hat{1}$ if and only if $v = \hat{1}$. Therefore we may assume that $u \neq \hat{1} \neq v$.

Let m_1 be the number of the occurrences of leaves $x \in X$ of s which, in the construction of $s\langle \hat{\times} u \rangle$, we replace by $x\hat{\times}u$, and let m_2 be the number of the occurrences of the leaf $\hat{1}$ in s . These occurrences of the leaves in $X \cup \{\hat{1}\}$ of s play the same role in the construction of $s\langle \hat{\times} v \rangle$.

Hence we have $\text{size}(s\langle \hat{\times} u \rangle) = \text{size}(s) + m_1 \cdot (\text{size}(u) + 1) + m_2 \cdot (\text{size}(u) - 1)$ and similarly $\text{size}(s\langle \hat{\times} v \rangle) = \text{size}(s) + m_1 \cdot (\text{size}(v) + 1) + m_2 \cdot (\text{size}(v) - 1)$. Hence $\text{size}(u) = \text{size}(v)$, so $\text{size}(r) = \text{size}(r')$. Then Theorem 4.16 implies $r = r'$.

(b) Immediate by Theorem 4.16. □

Next we wish to obtain a right-distributive strong bimonoid of polynomials which is idempotent. The main difference as compared to $\mathbb{N}_{\text{rd}}[X]$ is that in all sums of the form $p_1 + \dots + p_n$ where for every $i \in [n]$, p_i is a product polynomial or an element of $X/\text{AC} \cup \{1\}$, each of these polynomials p_i occurs only once, i.e., the polynomials $p_1, \dots, p_n$ are pairwise different.

We begin with defining, slightly more general also for later purposes, *idempotency-reduced* (for short *id-reduced*) terms as follows.

Definition 4.18. The set of *id-reduced terms*, denoted by $\text{ST}_{\text{id}}(X)$ is the smallest subset U of $\text{ST}(X)$ satisfying the following conditions:

- (a) $\hat{0}$, $\hat{1}$, and all monomial terms are in U ,
- (b) if $t \in \text{ST}(X)$ is a sum term and it has a sum-product decomposition $t = t_1 \hat{+} \dots \hat{+} t_n$ such that $t_1, \dots, t_n \in U$ and $t_i \neq_{\text{AC}} t_j$ for every $1 \leq i < j \leq n$, then $t \in U$,
- (c) if $s, t \in U \setminus \{\hat{0}, \hat{1}\}$, then the product term $s\hat{\times}t$ is in U .

We put $\text{PT}_{\text{id}}(X) = \text{PT}(X) \cap \text{ST}_{\text{id}}(X)$, the set of all polynomial terms which are id-reduced. □

Now we show that we obtain id-reduced polynomial terms in the following way.

Lemma 4.19. The set $\text{PT}_{\text{id}}(X)$ of id-reduced polynomial terms is the smallest subset U of $\text{ST}(X)$ satisfying the following conditions:

- (a) $\hat{0}$, $\hat{1}$, and all monomial terms are in U ,
- (b) if $t \in \text{ST}(X)$ is a sum term and it has a sum-product decomposition $t = t_1 \hat{+} \dots \hat{+} t_n$ such that $t_1, \dots, t_n \in U$ and $t_i \neq_{\text{AC}} t_j$ for every $1 \leq i < j \leq n$, then $t \in U$,
- (c) if s is a monomial term and $t \in U \setminus \{\hat{0}, \hat{1}\}$, then the product term $s \hat{\times} t$ is in U .

Proof. Let U be defined as described above. The closure condition (c) of the Lemma is weaker than (c) of Definition 4.18, and the closure condition (b) of the Lemma is weaker than (b) of Definition 4.7. This shows that $U \subseteq \text{ST}_{\text{id}}(X) \cap \text{PT}(X)$.

To prove the converse, let $s \in \text{ST}_{\text{id}}(X) \cap \text{PT}(X)$. We show by induction on $\text{size}(s)$ that $s \in U$. This is trivial if $s \in \{\hat{0}, \hat{1}\}$ or if s is a monomial term.

Now let s be a sum term. By $s \in \text{ST}_{\text{id}}(X) \cap \text{PT}(X)$ and Lemma 4.3(a), it follows that s has a sum-product decomposition $s = t_1 \hat{+} \dots \hat{+} t_n$ where $t_1, \dots, t_n$ are id-reduced and polynomial terms and $t_i \neq_{\text{AC}} t_j$ for every $1 \leq i < j \leq n$. By the induction hypothesis, we have $t_1, \dots, t_n \in U$. Then, by condition (b), we obtain that $s \in U$.

Finally, let s be a product term, but not a monomial term. By $s \in \text{ST}_{\text{id}}(X) \cap \text{PT}(X)$ and Lemma 4.3(b), it follows that $s = s' \hat{\times} t$, where s' is a monomial term and t is id-reduced and a sum polynomial term. By induction hypothesis, then $t \in U$ and hence $s \in U$ by condition (c). $\square$

Next we show an analogous result as Lemma 4.10:

Lemma 4.20. For every $s \in \text{PT}_{\text{id}}(X)$ and $t \in \text{ST}(X)$, if $s =_{\text{AC}} t$, then also $t \in \text{PT}_{\text{id}}(X)$.

Proof. We can follow the proof of Lemma 4.10 almost verbatim, observing the additional property of s given by Definition 4.18(b). $\square$

In an equivalent formulation, Lemma 4.20 says that if $s \in \text{PT}_{\text{id}}(X)$, then $[s]_{\text{AC}} \subseteq \text{PT}_{\text{id}}(X)$.

For each id-reduced polynomial term $t \in \text{PT}_{\text{id}}(X)$ (respectively, id-reduced sum polynomial term, id-reduced product polynomial term), we call its congruence class $[t]_{\text{AC}}$ an *id-reduced polynomial* (respectively, an *id-reduced sum polynomial*, an *id-reduced product polynomial*).

Now, we let

$$\mathbb{B}_{\text{id}, \text{rd}}[X] = \text{PT}_{\text{id}}(X) / \equiv_{\text{AC}} = \{[t]_{\text{AC}} \mid t \in \text{PT}_{\text{id}}(X)\},$$

so $\mathbb{B}_{\text{id}, \text{rd}}[X]$ is the set of all id-reduced polynomials in $\mathbb{N}_{\text{rd}}[X]$. In particular, $0, 1 \in \mathbb{B}_{\text{id}, \text{rd}}[X]$. Our next goal is to obtain an idempotent and right-distributive strong bimonoid structure on $\mathbb{B}_{\text{id}, \text{rd}}[X]$, this explains the index id. The following is straightforward.

Observation 4.21. The set $\mathbb{B}_{\text{id}, \text{rd}}[X]$ of *id-reduced polynomials* is the smallest subset U of $\mathbb{N}_{\text{sb}}[X]$ satisfying the following conditions:

- (a) $0, 1$, and all monomials (defined above) are in U .
- (b) If $p \in \mathbb{N}_{\text{sb}}[X]$ is a sum class and it has a sum-product decomposition $p = p_1 + \dots + p_n$ with pairwise different $p_1, \dots, p_n \in U$, then $p \in U$.
- (c) If m is a monomial and $q \in U$ is a polynomial, then the product polynomial $m \times q$ is in U .

$\square$

We show a decomposition of the elements of $\mathbb{B}_{\text{id,rd}}[X] \setminus \{0\}$ that we will use later without any reference.

Observation 4.22. For each $p \in \mathbb{B}_{\text{id,rd}}[X] \setminus \{0\}$ we have $p = p_1 + \dots + p_n$ for some $n \geq 1$, where each of $p_1, \dots, p_n$ is 1, a monomial, or an id-reduced product polynomial. Moreover, if $n \geq 2$, then $p_1, \dots, p_n$ are pairwise different.

Proof. By Observation 4.21, the elements of $\mathbb{B}_{\text{id,rd}}[X]$ can be obtained by starting with the elements described in Observation 4.21(a) and then closing this set by the sum and product operations described in (b) and (c), respectively. We show by induction that our statement holds for all the elements $p \in \mathbb{B}_{\text{id,rd}}[X] \setminus \{0\}$ obtained in this way.

If p has the form described in Observation 4.21(a), then the statement is immediate with $n = 1$ and $p_1 = p$. If p is obtained by applying Observation 4.21(b), then $p = p_1 + \dots + p_n$ is a sum-product decomposition, and each p_i is an id-reduced polynomial by the construction hypothesis. Hence p has the required form (with $n \geq 2$). If p is obtained by applying Observation 4.21(c), then it is an id-reduced product polynomial. Hence the statement holds again with $n = 1$ and $p_1 = p$. $\square$

Next we will define an addition operation and a multiplication operation on $\mathbb{B}_{\text{id,rd}}[X]$. As preparation, we show the following.

Lemma 4.23. $\mathbb{B}_{\text{id,rd}}[X]$ is closed under $\times_{\text{rd}}$.

Proof. Let $q, r \in \mathbb{B}_{\text{id,rd}}[X]$. We show that $q \times_{\text{rd}} r \in \mathbb{B}_{\text{id,rd}}[X]$ by induction on the structure of q . We proceed by case distinction and induction on $\text{size}(q)$.

If $q \in \{0, 1\}$, the statement is obvious.

Next let q be a monomial. Then $q \times_{\text{rd}} r = q \times r$, and $q \times r$ is id-reduced by Observation 4.21(c).

Secondly, let $q = q_1 + \dots + q_n$ where $n \geq 2$, and each q_i is 1, a monomial, or an id-reduced product polynomial, and $q_1, \dots, q_n$ are pairwise different. Then, by Corollary 4.17(b), the product polynomials $q_1 \times_{\text{rd}} r, \dots, q_n \times_{\text{rd}} r$ are also pairwise different and, by the induction hypothesis, they are id-reduced polynomials. Hence, by Observation 4.21(b), $q \times_{\text{rd}} r = q_1 \times_{\text{rd}} r + \dots + q_n \times_{\text{rd}} r$ is an id-reduced polynomial.

Finally, let $q = m \times q'$, where m is a monomial and q' is an id-reduced sum polynomial. Then, by Definition 4.11(b), $q' \times_{\text{rd}} r$ is a sum polynomial and, by induction hypothesis, it is id-reduced. By Definition 4.11(c), we have $q \times_{\text{rd}} r = m \times (q' \times_{\text{rd}} r)$, where by Observation 4.21(c) the product polynomial in the right-hand side is id-reduced. $\square$

As a consequence, we deduce that $\text{PT}_{\text{id}}(X)$ is closed under the product operation $\cdot\langle\hat{\times}\cdot\rangle$ and hence we may compute the product of idempotent polynomial terms in one step precisely as for polynomial terms.

Corollary 4.24. Let $s, t \in \text{PT}_{\text{id}}(X)$. Then $s\langle\hat{\times}t\rangle \in \text{PT}_{\text{id}}(X)$ and $[s]_{\text{AC}} \times_{\text{rd}} [t]_{\text{AC}} = [s\langle\hat{\times}t\rangle]_{\text{AC}}$.

Proof. Clearly, we have $s\langle\hat{\times}t\rangle \in \text{PT}(X)$. By Lemma 4.12 and Lemma 4.23, we get $[s\langle\hat{\times}t\rangle]_{\text{AC}} = [s]_{\text{AC}} \times_{\text{rd}} [t]_{\text{AC}}$ and $[s]_{\text{AC}} \times_{\text{rd}} [t]_{\text{AC}} \in \mathbb{B}_{\text{id,rd}}[X]$. Hence, $[s]_{\text{AC}} \times_{\text{rd}} [t]_{\text{AC}} = [t']_{\text{AC}}$ for some $t' \in \text{PT}_{\text{id}}(X)$. Then $t' =_{\text{AC}} s\langle\hat{\times}t\rangle$, so by Lemma 4.20 we obtain $s\langle\hat{\times}t\rangle \in \text{PT}_{\text{id}}(X)$ as needed. $\square$

strong bimonoid	carrier set
$\mathbf{N}_{\text{sb}}[X] = (\mathbb{N}_{\text{sb}}[X], +, \times, 0, 1)$ strong bimonoid (cf. Proposition 4.1)	$\mathbb{N}_{\text{sb}}[X] = \text{ST}(X)/\equiv_{\text{AC}}$ $\text{ST}(X)$ is the set of simple terms $\text{ST}(X) \subseteq \text{T}(X)$
$\mathbf{N}_{\text{rd}}[X] = (\mathbb{N}_{\text{rd}}[X], +, \times_{\text{rd}}, 0, 1)$ right-distributive strong bimonoid (cf. Theorem 4.14)	$\mathbb{N}_{\text{rd}}[X] = \text{PT}(X)/\equiv_{\text{AC}}$ $\text{PT}(X)$ is the set of polynomial terms $\text{PT}(X) \subseteq \text{ST}(X)$
$\mathbf{B}_{\text{id,rd}}[X] = (\mathbb{B}_{\text{id,rd}}[X], +_{\text{id}}, \times_{\text{rd}}, 0, 1)$ idempotent right-distr. strong bimonoid (cf. Theorem 4.26)	$\mathbb{B}_{\text{id,rd}}[X] = \text{PT}_{\text{id}}(X)/\equiv_{\text{AC}}$ $\text{PT}_{\text{id}}(X)$ is the set of id-reduced terms $\text{PT}_{\text{id}}(X) \subseteq \text{PT}(X)$

$\text{AC} = \{e_1, e_2, e_4\}$ is the set of identities for associativity of $+$ and $\times$, and commutativity of $+$.

Figure 1: An overview of the free strong bimonoids described in Section 4.

Recall that when passing from $\mathbf{N}_{\text{sb}}[X]$ to $\mathbf{N}_{\text{rd}}[X]$, we could keep the addition but had to adjust the multiplication operation. Now, when passing from $\mathbf{N}_{\text{rd}}[X]$ to $\mathbf{B}_{\text{id,rd}}[X]$, by Lemma 4.23 we can take as multiplication the restriction of $\times_{\text{rd}}$ to $\mathbb{B}_{\text{id,rd}}[X]$, but we have to adjust the addition $+$ in order to obtain its idempotency. We define the operation addition $+_{\text{id}}$ on $\mathbb{B}_{\text{id,rd}}[X]$ as follows.

Definition 4.25. Let $q, r \in \mathbb{B}_{\text{id,rd}}[X]$. We put $q +_{\text{id}} 0 = q = 0 +_{\text{id}} q$.

Now let us assume that $q \neq 0 \neq r$. Then $q = q_1 + \dots + q_k$, where $k \geq 1$, $q_1, \dots, q_k$ are pairwise different and each of them is 1, a monomial, or an id-reduced product polynomial, and $r = r_1 + \dots + r_n$ with $n \geq 1$ and the corresponding conditions for $r_1, \dots, r_n$. Then we define $q +_{\text{id}} r = q_1 + \dots + q_k + r_{i_1} + \dots + r_{i_\ell}$, where $\ell \geq 0$ and $\{i_1, \dots, i_\ell\}$ is the maximal subset of $\{1, \dots, n\}$ (with respect to inclusion) such that $\{q_1, \dots, q_k\} \cap \{r_{i_1}, \dots, r_{i_\ell}\} = \emptyset$. $\square$

Now we can show the following result.

Theorem 4.26. $\mathbf{B}_{\text{id,rd}}[X] = (\mathbb{B}_{\text{id,rd}}[X], +_{\text{id}}, \times_{\text{rd}}, 0, 1)$ is an idempotent right-distributive strong bimonoid.

Proof. It is immediate from the definition that the operation $+_{\text{id}}$ is idempotent. To check associativity, let $p, q, r \in \mathbb{B}_{\text{id,rd}}[X] \setminus \{0\}$. We claim that $p +_{\text{id}} (q +_{\text{id}} r) = (p +_{\text{id}} q) +_{\text{id}} r$. Each of the three polynomials is either 1, a monomial, an id-reduced product polynomial or it is a sum of pairwise different monomials, id-reduced product polynomials, or 1's. On the right-hand side of the equation we obtain the sum of all these monomials, id-reduced product polynomials or 1 of p , then those ones of q added which are different from the ones of p , and then those of r added which are different from the ones of both p and q . This equals the left-hand side of the equation. This proves our claim.

Similarly, it is easy to see that the addition operation $+_{\text{id}}$ is commutative.

By Lemma 4.23 and Theorem 4.14, the operation $\times_{\text{rd}}$ is associative. To show that $\times_{\text{rd}}$ is right-distributive over $+_{\text{id}}$, we can follow the argument for the corresponding statements of Theorem 4.14, but using id-reduced polynomials and the operations $+_{\text{id}}$ and $\times_{\text{rd}}$; all corresponding sums of monomials, id-reduced product polynomials, or 1s have each summand occurring only once. Here we use Corollary 4.17(b) again.

This shows that $\mathbf{B}_{\text{id,rd}}[X]$ is an idempotent right-distributive strong bimonoid. $\square$

We just note that the strong bimonoid $\mathbf{B}_{\text{id,rd}}[X]$ has the same right- and left-cancellation properties as shown in Theorem 4.16 and Corollary 4.17 for $\mathbf{N}_{\text{rd}}[X]$; this is immediate from the two mentioned results, since the multiplication $\times_{\text{rd}}$ in $\mathbf{B}_{\text{id,rd}}[X]$ is the restriction of the multiplication of $\mathbf{N}_{\text{rd}}[X]$.

In Figure 1 we show the three strong bimonoids $\mathbf{N}_{\text{sb}}[X]$, $\mathbf{N}_{\text{rd}}[X]$, and $\mathbf{B}_{\text{id,rd}}[X]$ defined in this section and the definition of their carrier sets. In the following section we will show that they are free in their respective classes of strong bimonoids. The reader interested only in the construction of a right-distributive and weakly locally finite strong bimonoid that is not locally finite may directly proceed to Section 7.

5 The polynomial strong bimonoids are free

In this section we will first prove the result indicated in the title, i.e., we will show that the strong bimonoids of polynomials $\mathbf{N}_{\text{sb}}[X]$, $\mathbf{N}_{\text{rd}}[X]$, and $\mathbf{B}_{\text{id,rd}}[X]$ are, respectively, a free strong bimonoid, a free right-distributive strong bimonoid, and a free idempotent right-distributive strong bimonoid. This is analogous to Theorem 3.1 that the semiring $\mathbf{N}[X]$ of all polynomials in non-commuting variables with coefficients from $\mathbb{N}$ is free in the class of all semirings. Then, we deduce consequences of this result on representing arbitrary terms by simple terms, by polynomial terms and by id-reduced polynomial terms. First we show the following result.

Theorem 5.1. *$\mathbf{N}_{\text{sb}}[X]$ is a free strong bimonoid, freely generated by X/AC .*

Proof. By Proposition 4.1, $\mathbf{N}_{\text{sb}}[X]$ is a strong bimonoid. Clearly, $\mathbf{N}_{\text{sb}}[X]$ is generated by X/AC . Let $\mathbf{A} = (A, \oplus, \otimes, 0_{\mathbf{A}}, 1_{\mathbf{A}})$ be any strong bimonoid, and let $h : X/\text{AC} \rightarrow A$ be a mapping. We have to show that h extends to a strong bimonoid homomorphism from $\mathbf{N}_{\text{sb}}[X]$ to $\mathbf{A}$.

First, recall the Σ_{sb} -algebra $\mathbf{ST}(X) = (\mathbf{ST}(X), +_{\mathbf{ST}}, \times_{\mathbf{ST}}, \hat{0}, \hat{1})$ from Section 4. By a straightforward induction, we obtain a Σ_{sb} -algebra homomorphism h' from $\mathbf{ST}(X)$ to the strong bimonoid $\mathbf{A}$ satisfying $h'(x) = h([x]_{\text{AC}})$ for each $x \in X$. We define a mapping $h'' : \mathbf{N}_{\text{sb}}[X] \rightarrow A$ by putting $h''([t]_{\text{AC}}) = h'(t)$ for each $t \in \mathbf{ST}(X)$. We claim that h'' is well-defined and a strong bimonoid homomorphism; then our result follows.

To show that h'' is well defined, let $t, t' \in \mathbf{ST}(X)$ with $t =_{\text{AC}} t'$. We have to show that $h'(t) = h'(t')$. By Lemma 2.6, we have $t \Leftrightarrow_{\text{AC}}^* t'$. By symmetry and transitivity of equality, it suffices to consider the case that $t \Rightarrow_{\text{AC}} t'$. So assume that t' is obtained from t in a reduction step using one of the identities e_1, e_2 or e_4 . Then t' is obtained from t by replacing a subterm u of t by a term u' such that $h'(u) = h'(u')$. For instance, if we use e_2 , then $u = u_1 \hat{+} u_2$ and $u' = u_2 \hat{+} u_1$. Clearly, $h'(u) = h'(u_1) \oplus h'(u_2) = h'(u_2) \oplus h'(u_1) = h'(u')$ because h' is a Σ_{sb} -algebra

homomorphism and $\oplus$ is commutative. We obtain $h'(u) = h'(u')$ in the other two cases similarly. Using again that h' is a homomorphism, it follows that $h'(t) = h'(t')$. Hence h'' is well-defined.

It remains to show that h'' is a strong bimonoid homomorphism. Clearly, $h''([\hat{0}]_{AC}) = h'(\hat{0}) = 0_A$ and $h''([\hat{1}]_{AC}) = h'(\hat{1}) = 1_A$. If $t, t' \in ST(X)$, we have $h''([t]_{AC} + [t']_{AC}) = h''([t +_{ST} t']_{AC}) = h'(t +_{ST} t') = h'(t) \oplus h'(t') = h''([t]_{AC}) \oplus h''([t']_{AC})$, as needed; the case of multiplication is analogous. The result follows. $\square$

Next, we can prove the corresponding result for right-distributive resp. idempotent right-distributive strong bimonoids.

Theorem 5.2.

- (a) $N_{rd}[X]$ is a free right-distributive strong bimonoid, freely generated by X/AC .
- (b) $B_{id,rd}[X]$ is a free idempotent right-distributive strong bimonoid, freely generated by X/AC .

Proof. (a) By Theorem 4.14, $N_{rd}[X]$ is a right-distributive strong bimonoid. Clearly, $N_{rd}[X]$ is generated by X/AC . Let $A = (A, \oplus, \otimes, 0_A, 1_A)$ be a right-distributive strong bimonoid and $h : X/AC \rightarrow A$ a mapping. By Theorem 5.1, h extends to a strong bimonoid homomorphism h' from $N_{sb}[X]$ to A . Note that $N_{rd}[X] \subseteq N_{sb}[X]$. We claim that h' , restricted to $N_{rd}[X]$, also constitutes a strong bimonoid homomorphism from $N_{rd}[X]$ to A . Then the result follows.

Let $q, r \in N_{rd}[X] \setminus \{0\}$. Clearly, we have $h'(q+r) = h'(q) \oplus h'(r)$ because h' is a homomorphism from $N_{sb}[X]$ to A .

Next, we claim that $h'(q \times_{rd} r) = h'(q) \otimes h'(r)$. Clearly, we may assume that $q, r \neq 1$.

We proceed by case distinction and induction on the size of q .

First, assume q is a monomial. Then $q \times_{rd} r = q \times r$ and we obtain $h'(q \times_{rd} r) = h'(q \times r) = h'(q) \otimes h'(r)$ as claimed.

Secondly, let q be a sum polynomial, with sum-product decomposition $q = q_1 + \dots + q_n$, say. In this case we have $q \times_{rd} r = q_1 \times_{rd} r + \dots + q_n \times_{rd} r$, a sum polynomial. By induction hypothesis, we can assume that $h'(q_i \times_{rd} r) = h'(q_i) \otimes h'(r)$ for each $i \in [n]$. Then we obtain

$$\begin{aligned}
h'(q \times_{rd} r) &= h'(q_1 \times_{rd} r + \dots + q_n \times_{rd} r) \\
&= h'(q_1 \times_{rd} r) \oplus \dots \oplus h'(q_n \times_{rd} r) && \text{(since } h' \text{ is a homomorphism from } N_{sb}[X] \text{ to } A) \\
&= h'(q_1) \otimes h'(r) \oplus \dots \oplus h'(q_n) \otimes h'(r) && \text{(by induction hypothesis)} \\
&= (h'(q_1) \oplus \dots \oplus h'(q_n)) \otimes h'(r) && \text{(since } A \text{ is right-distributive)} \\
&= h'(q_1 + \dots + q_n) \otimes h'(r) && \text{(since } h' \text{ is a homomorphism from } N_{sb}[X] \text{ to } A) \\
&= h'(q) \otimes h'(r).
\end{aligned}$$

Thirdly, let q be a product polynomial of the form $q = m \times s$ with a monomial m and a sum polynomial s (cf. Lemma 4.9). In this case, we have $q \times_{rd} r = m \times (s \times_{rd} r)$. By induction

hypothesis, we have $h'(s \times_{\text{rd}} r) = h'(s) \otimes h'(r)$. Then

$$\begin{aligned}
& h'(q \times_{\text{rd}} r) = h'(m \times (s \times_{\text{rd}} r)) \\
& = h'(m) \otimes h'(s \times_{\text{rd}} r) && \text{(since } h' \text{ is a homomorphism from } \mathbb{N}_{\text{sb}}[X] \text{ to } \mathbf{A}) \\
& = h'(m) \otimes (h'(s) \otimes h'(r)) && \text{(by induction hypothesis)} \\
& = (h'(m) \otimes h'(s)) \otimes h'(r) \\
& = h'(m \times s) \otimes h'(r) && \text{(since } h' \text{ is a homomorphism from } \mathbb{N}_{\text{sb}}[X] \text{ to } \mathbf{A}) \\
& = h'(q) \otimes h'(r).
\end{aligned}$$

Hence h' is a strong bimonoid homomorphism as claimed, and the result follows.

(b) By Theorem 4.26, $\mathbb{B}_{\text{id,rd}}[X]$ is an idempotent right-distributive strong bimonoid. Clearly, $\mathbb{B}_{\text{id,rd}}[X]$ is generated by X/AC . We consider a mapping $h : X/\text{AC} \rightarrow \mathbf{A}$, where $\mathbf{A} = (A, \oplus, \otimes, 0_{\mathbf{A}}, 1_{\mathbf{A}})$ is an idempotent right-distributive strong bimonoid. By (a), we can extend h to a homomorphism h' from $\mathbb{N}_{\text{rd}}[X]$ to $\mathbf{A}$. We claim h' , restricted to the subset $\mathbb{B}_{\text{id,rd}}[X]$ of $\mathbb{N}_{\text{rd}}[X]$, constitutes a strong bimonoid homomorphism from $\mathbb{B}_{\text{id,rd}}[X]$ to $\mathbf{A}$.

Let $q, r \in \mathbb{B}_{\text{id,rd}}[X] \setminus \{0\}$. First we show that $h'(q +_{\text{id}} r) = h'(q) \oplus h'(r)$.

We have $q = q_1 + \dots + q_k$ and $r = r_1 + \dots + r_n$ where $k, n \geq 1$ and $q_1, \dots, q_k, r_1, \dots, r_n$ are 1's, monomials, or id-reduced product polynomials. Moreover, if $k \geq 2$ ($n \geq 2$), then the polynomials $q_1, \dots, q_k$ ($r_1, \dots, r_n$, respectively) are pairwise different. Then $q +_{\text{id}} r$ is the sum of all these polynomials, but with each polynomial occurring only once. So, $q +_{\text{id}} r = q_1 + \dots + q_k + r_{i_1} + \dots + r_{i_\ell}$, where $\ell \geq 0$ and $\{i_1, \dots, i_\ell\}$ is the maximal subset of $\{1, \dots, n\}$ such that $\{q_1, \dots, q_k\} \cap \{r_{i_1}, \dots, r_{i_\ell}\} = \emptyset$. Thus

$$\{q_1, \dots, q_k, r_{i_1}, \dots, r_{i_\ell}\} = \{q_1, \dots, q_k, r_1, \dots, r_n\} . \quad (3)$$

Then $h'(q) = h'(q_1) \oplus \dots \oplus h'(q_k)$, similarly $h'(r) = h'(r_1) \oplus \dots \oplus h'(r_n)$, and

$$\begin{aligned}
& h'(q +_{\text{id}} r) = h'(q_1) \oplus \dots \oplus h'(q_k) \oplus h'(r_{i_1}) \oplus \dots \oplus h'(r_{i_\ell}) \\
& = h'(q_1) \oplus \dots \oplus h'(q_k) \oplus h'(r_1) \oplus \dots \oplus h'(r_n) && \text{(since } \mathbf{A} \text{ is idempotent and by (3))} \\
& = h'(q) \oplus h'(r).
\end{aligned}$$

Second, by (a) we have $h'(q \times_{\text{rd}} r) = h'(q) \otimes h'(r)$. Hence h' is a strong bimonoid homomorphism as claimed, and the result follows. $\square$

Now we obtain the following further description of our strong bimonoids of polynomials. Its proof is immediate by Theorems 5.1, 5.2, Proposition 3.3 and the uniqueness of free structures (cf. Lemma 2.2).

Corollary 5.3.

- (a) The strong bimonoids $\text{FB}(X)$ and $\mathbb{N}_{\text{sb}}[X]$ are isomorphic.
- (b) The strong bimonoid $\text{FB}_{\text{rd}}(X)$ and the strong bimonoid $\mathbb{N}_{\text{rd}}[X]$ of polynomials are isomorphic.
- (c) The strong bimonoid $\text{FB}_{\text{id,rd}}(X)$ and the strong bimonoid $\mathbb{B}_{\text{id,rd}}[X]$ of idempotent polynomials are isomorphic. $\square$

Next we investigate the different congruence relations and their relationships for simple terms, for polynomial terms and for id-reduced polynomial terms.

Theorem 5.4.

- (a) Let $t, t' \in \text{ST}(X)$. Then $[t]_E = [t']_E$ in $\text{FB}(X)$ implies $t =_{\text{AC}} t'$ in $\text{ST}(X)$.
- (b) Let $t, t' \in \text{PT}(X)$. Then $[t]_{\text{rd}} = [t']_{\text{rd}}$ in $\text{FB}_{\text{rd}}(X)$ implies $t =_{\text{AC}} t'$ in $\text{ST}(X)$.
- (c) Let $t, t' \in \text{PT}_{\text{id}}(X)$. Then $[t]_{\text{id,rd}} = [t']_{\text{id,rd}}$ in $\text{FB}_{\text{id,rd}}(X)$ implies $t =_{\text{AC}} t'$ in $\text{ST}(X)$.

Proof. First, observe that for $x \in X$ we have $[x]_{\text{AC}} = \{x\}$, but $[x]_E$ is infinite, as it contains x , $x \hat{+} \hat{0}$, $x \hat{\times} \hat{1}$, etc.

(a) We define two mappings $f : X/\text{AC} \rightarrow X/E$ and $g : X/E \rightarrow X/\text{AC}$ by putting $f([x]_{\text{AC}}) = [x]_E$ and $g([x]_E) = [x]_{\text{AC}}$ for each $x \in X$; note that g is well-defined as $[x]_E \cap X = \{x\}$.

By Theorem 5.1 and Proposition 3.3(a), f and g extend to homomorphisms $f' : \mathbb{N}_{\text{sb}}[X] \rightarrow \text{FB}(X)$ and $g' : \text{FB}(X) \rightarrow \mathbb{N}_{\text{sb}}[X]$, respectively.

Moreover, we can show that

$$f'([t]_{\text{AC}}) = [t]_E \text{ for each } t \in \text{ST}(X) \quad (4)$$

by induction on the size of t .

Then $g' \circ f' : \mathbb{N}_{\text{sb}}[X] \rightarrow \mathbb{N}_{\text{sb}}[X]$ is a homomorphism which acts like the identity on X/AC . Since X/AC generates $\mathbb{N}_{\text{sb}}[X]$, we obtain that $g' \circ f'$ is the identity on $\mathbb{N}_{\text{sb}}[X]$. Then f' is injective, and together with (4) this implies the result.

(b) We define the mappings $f : X/\text{AC} \rightarrow X/\text{rd}$ and $g : X/\text{rd} \rightarrow X/\text{AC}$ analogously to (a). By Theorem 5.2(a) and Proposition 3.3(b), f and g extend to homomorphisms $f' : \mathbb{N}_{\text{rd}}[X] \rightarrow \text{FB}_{\text{rd}}(X)$ and $g' : \text{FB}_{\text{rd}}(X) \rightarrow \mathbb{N}_{\text{rd}}[X]$, respectively.

Now we claim that

$$f'([t]_{\text{AC}}) = [t]_{\text{rd}} \text{ for each } t \in \text{PT}(X). \quad (5)$$

We proceed by case distinction according to Definition 4.7 and induction on the size of t . We only consider case (c) of that definition, as the cases (a) and (b) are similar and easier. Assume that $t = s \hat{\times} t'$, where s is a monomial term for which we have proved the claim and $t' \in \text{PT}(X)$ for which the claim holds by induction hypothesis. Then, using Definition 4.11(a) and that f' is a homomorphism, we obtain

$$\begin{aligned} f'([s \hat{\times} t']_{\text{AC}}) &= f'([s]_{\text{AC}} \times [t']_{\text{AC}}) = f'([s]_{\text{AC}} \times_{\text{rd}} [t']_{\text{AC}}) = \\ &= f'([s]_{\text{AC}}) \otimes_{\text{rd}} f'([t']_{\text{AC}}) = [s]_{\text{rd}} \otimes_{\text{rd}} [t']_{\text{rd}} = [s \hat{\times} t']_{\text{rd}}, \end{aligned}$$

as claimed. Then we can proceed as for the proof of (a) of our theorem.

(c) Here we proceed analogously to (a) and (b), but using Theorem 5.2(b) and Proposition 3.3(c), with the homomorphisms $f' : \text{B}_{\text{id,rd}}[X] \rightarrow \text{FB}_{\text{id,rd}}(X)$ and $g' : \text{FB}_{\text{id,rd}}(X) \rightarrow \text{B}_{\text{id,rd}}[X]$. Now we claim that

$$f'([t]_{\text{AC}}) = [t]_{\text{id,rd}} \text{ for each } t \in \text{PT}_{\text{id}}(X). \quad (6)$$

For the proof we follow Lemma 4.19 and Definition 4.25. $\square$

Here, for instance, Theorem 5.4(b) says the following. If a polynomial term t can be transformed into a polynomial term t' via the identities given in E_{rd} , then we can transform t

into t' by just using the identities in AC, i.e., the identities for associativity and commutativity of addition and associativity of multiplication. In the term rewriting literature, this is regarded as an AC-reduction result, cf. [BP85, GL86], cf. also [BN98, Sec. 11.1]. This is usually achieved by an involved analysis of critical pairs; here we obtained it by algebraic means.

An immediate consequence of Theorem 5.4 is the following. If a term $t \in T(X)$ is "represented" by a polynomial term $t' \in PT(X)$ meaning that $t =_{E_{rd}} t'$, then t' is unique up to AC-equivalence. Now we will see that such representations exist. This provides the analogy of the second statement in Theorem 3.1 for representations of terms here by simple terms, by polynomial terms and by id-reduced polynomial terms.

Theorem 5.5. *Given $t \in T(X)$, there are $t_1 \in ST(X)$, $t_2 \in PT(X)$, and $t_3 \in PT_{id}(X)$ with $t =_E t_1$, $t =_{E_{rd}} t_2$, and $t =_{E_{id,rd}} t_3$.*

Proof. The simple term t_1 is easy to obtain. In t , we replace all occurrences of subterms $t' \hat{+} \hat{0}$ or $\hat{0} \hat{+} t'$ by t' , of $t' \hat{\times} \hat{0}$ or $\hat{0} \hat{\times} t'$ by $\hat{0}$, and of $t' \hat{\times} \hat{1}$ or $\hat{1} \hat{\times} t'$ by t' , in any order, continuing until all such subterms are eliminated. The resulting term t_1 is simple, has size at most $\text{size}(t)$ and satisfies $t =_E t_1$.

For the second assertion concerning the existence of t_2 , we follow the proof of Theorem 5.4(b). We consider the two mappings $f : X/AC \rightarrow X/rd$ and $g : X/rd \rightarrow X/AC$ given by $f([x]_{AC}) = [x]_{rd}$ and $g([x]_{rd}) = [x]_{AC}$ for each $x \in X$. They extend to homomorphisms $f' : \mathbb{N}_{rd}[X] \rightarrow FB_{rd}(X)$ and $g' : FB_{rd}(X) \rightarrow \mathbb{N}_{rd}[X]$, respectively, and f' satisfies equation (5). Then $f' \circ g' : FB_{rd}(X) \rightarrow FB_{rd}(X)$ is a homomorphism which acts like the identity on X/rd . Since X/rd generates $FB_{rd}(X)$, we obtain that $f' \circ g'$ is the identity on $FB_{rd}(X)$. Given $t \in T(X)$, choose $t_2 \in PT(X)$ with $g'([t]_{rd}) = [t_2]_{AC}$. Then $[t]_{rd} = (f' \circ g')([t]_{rd}) = f'([t_2]_{AC}) = [t_2]_{rd}$ by equation (5). Thus $t =_{E_{rd}} t_2$ as claimed.

For the third claim, we start with mappings $f : X/AC \rightarrow X/id,rd$ and $g : X/id,rd \rightarrow X/AC$ as in the proof of Theorem 5.4(c) and follow the above argument to obtain homomorphisms $f' : B_{id,rd}[X] \rightarrow FB_{id,rd}(X)$ and $g' : FB_{id,rd}(X) \rightarrow B_{id,rd}[X]$ such that $f' \circ g'$ is the identity on $FB_{id,rd}(X)$. Given $t \in T(X)$, choose $t_3 \in PT_{id}(X)$ with $g'([t]_{id,rd}) = [t_3]_{AC}$. Then $[t]_{id,rd} = (f' \circ g')([t]_{id,rd}) = f'([t_3]_{AC}) = [t_3]_{id,rd}$ by equation (6). Thus $t =_{E_{id,rd}} t_3$ as claimed. $\square$

6 Decision and construction procedures for simple and polynomial terms

In this section, we turn to algorithms for deciding the equivalence of terms modulo our congruences, as indicated by Theorem 5.4, and for constructing representations of terms as stated in Theorem 5.5.

First, we give an algorithm for deciding the equivalence of simple terms modulo AC-equivalence. For the decision algorithm we will represent simple terms as labeled trees (cf. Section 3) and employ the well-known result that isomorphism of labeled trees is decidable in linear time (cf. [AHU74, Sect. 3.2]).

Lemma 6.1. For every $s, t \in ST(X)$ it is decidable in linear time $O(n)$, where $n = \max\{\text{size}(s), \text{size}(t)\}$, whether $s \Leftrightarrow_{AC}^* t$.

Proof. By Proposition 4.4, two simple terms s and t are AC-equivalent if and only if there is an isomorphism between the labeled trees $\bar{s}$ and $\bar{t}$. For s and t we can construct the labeled trees $\bar{s}$ and $\bar{t}$ in $O(n)$ time. Then it can be decided if $\bar{s}$ and $\bar{t}$ are isomorphic in $O(n)$ time by [AHU74, Cor. p.86]. $\square$

We will also need the following algorithm for constructing id-reduced terms. This may be known in the literature, but we could not find a reference. We define

$$\text{AC}_{\text{id}} = \text{AC} \cup \{e_{11}\}.$$

Lemma 6.2. For each simple term s with $n = \text{size}(s)$ we can find in linear time $O(n)$ an id-reduced term t with $s =_{\text{AC}_{\text{id}}} t$.

Proof. Given s , we construct the labeled tree $\bar{s}$ in time $O(n)$. Then we traverse the labeled tree $\bar{s}$ as described in [AHU74, Example 3.2, pp. 85,86] and assign the tuples and numbers to its nodes also as described, in time $O(n)$.

Then we traverse the labeled tree a second time, starting with vertices at level 1 and working up towards the root. At each node d labeled by $\boxplus$, we consider the list of numbers $i_1, i_2, \dots, i_k$ associated to the children $d_1, d_2, \dots, d_k$ of d , and we check whether $i_j = i_{j+1}$, for $j = 1, \dots, k-1$. If $i_j = i_{j+1}$, i.e., the subtrees with root d_j and d_{j+1} are isomorphic, then we delete the subtree having the vertex d_{j+1} as its root. It is important to note that if two subtrees with root d and d' at a level i are isomorphic before the possible deletion of some of their subtrees, i.e., the same number is assigned to both, then they remain isomorphic after the deletion. So there is no need to change the number assigned to them. The second traversal can also be done in time $O(n)$.

Let T be the labeled tree obtained by the above construction. We construct a simple term t with $\bar{t} = T$ by induction as follows. We show only the induction step. If the root of T is $\boxplus$ or $\boxtimes$ with children $T_1, \dots, T_k$, then by induction hypothesis simple terms $t_1, \dots, t_k$ can be constructed such that $\bar{t}_i = T_i$ for each $i \in [k]$. If the root is $\boxplus$, then each t_i is a product term or an element of $X \cup \{\hat{1}\}$. Then t can be any sum term of which the sum-product decomposition is $t_1 \hat{+} \dots \hat{+} t_k$. If the root is $\boxtimes$, each t_i is a sum term or an element of X . Then t can be any product term of which the product-sum decomposition is $t_1 \hat{\times} \dots \hat{\times} t_k$. This can also be done in time $O(n)$, resulting in total time complexity $O(n)$ for the algorithm.

This algorithm has the effect that for each subterm s' of s with a sum-product decomposition $s' = s'_1 \hat{+} \dots \hat{+} s'_m$, say, we delete all summands s'_j occurring more than once. Therefore, $s =_{\text{AC}_{\text{id}}} t$, as can be shown again by induction on the size of s . $\square$

As a consequence, we obtain algorithms for deciding the equivalence of polynomial terms modulo our congruences $=_{E_{\text{rd}}}$ and $=_{E_{\text{id,rd}}}$.

Corollary 6.3. It is decidable, given $s, t \in \text{PT}(X)$ and $n = \max\{\text{size}(s), \text{size}(t)\}$, in linear time $O(n)$ whether $s =_{E_{\text{rd}}} t$ and whether $s =_{E_{\text{id,rd}}} t$.

Proof. For the first claim, we apply Theorem 5.4(b) and Lemma 6.1. For the second claim, using Lemma 6.2 we construct $s', t' \in \text{PT}_{\text{id}}(X)$, each of size at most n , with $s =_{E_{\text{id,rd}}} s'$ and $t =_{E_{\text{id,rd}}} t'$ in $O(n)$ steps. Then we have $s =_{E_{\text{id,rd}}} t$ if and only if $s' =_{E_{\text{id,rd}}} t'$ if and only if $s' =_{\text{AC}} t'$, where the latter equivalence follows from Theorem 5.4(c). By Lemma 6.1, this latter AC-equivalence can be decided with a number of steps linear in the sizes of s', t' . $\square$

Now we turn to algorithms for constructing representations of terms as described in Theorem 5.5. We will determine the total number of operations needed. But, since we consider an application of right-distributivity as the possibly 'most complex' operation, we also describe the possible number of uses of right-distributivity, i.e., the application of the identity

$$e_9 : ((z_1 \hat{+} z_2) \hat{\times} z_3, (z_1 \hat{\times} z_3) \hat{+} (z_2 \hat{\times} z_3)).$$

In fact, we will apply the identity e_9 only by replacing a subterm of the form $(t_1 \hat{+} t_2) \hat{\times} t_3$ by $(t_1 \hat{\times} t_3) \hat{+} (t_2 \hat{\times} t_3)$.

First we prove the following auxiliary result.

Lemma 6.4. There is an effective procedure for constructing, given $s \in \text{ST}(X)$ and $t \in \text{PT}(X)$, a polynomial term $t' \in \text{PT}(X)$ with $s \hat{\times} t =_{E_{\text{rd}}} t'$ and $\text{size}(t') \leq 2^{\text{size}(s)} \cdot \text{size}(t)$ in $O(2^{\text{size}(s)})$ steps, using at most $\text{size}(s)$ applications of right-distributivity.

Proof. We proceed by induction on $\text{size}(s)$. If $s \in X$, the result is trivial, as $t' = s \hat{\times} t$ is already a polynomial term.

Let us first assume that s is a sum term, so $s = s_1 \hat{+} s_2$. Then $s \hat{\times} t =_{E_{\text{rd}}} (s_1 \hat{\times} t) \hat{+} (s_2 \hat{\times} t)$. By induction hypothesis, we can construct polynomial terms $t'_i \in \text{PT}(X)$ with $s_i \hat{\times} t =_{E_{\text{rd}}} t'_i$ and $\text{size}(t'_i) \leq 2^{\text{size}(s_i)} \cdot \text{size}(t)$ in $O(2^{\text{size}(s_i)})$ steps, using at most $\text{size}(s_i)$ applications of right-distributivity, for $i = 1, 2$. Put $t' = t'_1 \hat{+} t'_2$. Then $t' \in \text{PT}(X)$, and we have $\text{size}(t') = \text{size}(t'_1) + \text{size}(t'_2) + 1 \leq (2^{\text{size}(s_1)} + 2^{\text{size}(s_2)}) \cdot \text{size}(t) + 1 \leq 2^{\text{size}(s)} \cdot \text{size}(t)$. Clearly, we needed at most $O(2^{\text{size}(s)})$ steps, and our construction involved at most $1 + \text{size}(s_1) + \text{size}(s_2) = \text{size}(s)$ applications of right-distributivity.

Second, assume that s is a product term, say $s = s_1 \hat{\times} s_2$. By our induction hypothesis, we can construct a polynomial term $t'' \in \text{PT}(X)$ with $s_2 \hat{\times} t =_{E_{\text{rd}}} t''$ and $\text{size}(t'') \leq 2^{\text{size}(s_2)} \cdot \text{size}(t)$ in $O(2^{\text{size}(s_2)})$ steps, using at most $\text{size}(s_2)$ applications of right-distributivity. Then, again by our induction hypothesis, we can construct a polynomial term $t' \in \text{PT}(X)$ with $s_1 \hat{\times} t'' =_{E_{\text{rd}}} t'$ and $\text{size}(t') \leq 2^{\text{size}(s_1)} \cdot \text{size}(t'') \leq 2^{\text{size}(s_1)} \cdot 2^{\text{size}(s_2)} \cdot \text{size}(t) \leq 2^{\text{size}(s)} \cdot \text{size}(t)$ in $O(2^{\text{size}(s_1)})$ steps, using at most $\text{size}(s_1)$ applications of right-distributivity. Then we have $t' =_{E_{\text{rd}}} s_1 \hat{\times} t'' =_{E_{\text{rd}}} s_1 \hat{\times} (s_2 \hat{\times} t) =_{\text{AC}} (s_1 \hat{\times} s_2) \hat{\times} t = s \hat{\times} t$, and we have obtained t' in at most $O(2^{\text{size}(s)})$ steps, using at most $\text{size}(s)$ applications of right-distributivity. $\square$

Now we can show:

Theorem 6.5. *There are effective procedures for constructing, given $t \in \text{T}(X)$, terms*

- (a) $t_1 \in \text{ST}(X)$ with $t =_E t_1$ and $\text{size}(t_1) \leq \text{size}(t)$ using at most $O(\text{size}(t))$ steps,
- (b) $t_2 \in \text{PT}(X)$ with $t =_{E_{\text{rd}}} t_2$ and $\text{size}(t_2) \leq 2^{\text{size}(t)}$ in $O(2^{\text{size}(t)})$ steps using at most $\text{size}(t)$ applications of right-distributivity, and
- (c) $t_3 \in \text{PT}_{\text{id}}(X)$ with $t =_{E_{\text{id}, \text{rd}}} t_3$ and $\text{size}(t_3) \leq 2^{\text{size}(t)}$ in $O(2^{\text{size}(t)})$ steps using at most $\text{size}(t)$ applications of right-distributivity.

Proof. (a) For constructing t_1 , we can proceed as described at the beginning of the proof of Theorem 5.5. This needs at most $O(\text{size}(t))$ steps.

(b) Using (a), first we construct the simple term t_1 with $t =_E t_1$. Then we also have $t =_{E_{\text{rd}}} t_1$. Hence we may assume without loss of generality that $t \in \text{ST}(X)$.

Then we proceed by induction on the size of t . If $t \in X \cup \{\hat{0}, \hat{1}\}$, the result is trivial. Therefore we can assume that t is a sum term or a product term.

First, assume that t is a sum term, say, $t = t_1 \hat{+} t_2$. By induction hypothesis, we can construct polynomial terms $t'_i \in \text{PT}(X)$ with $t_i =_{E_{\text{rd}}} t'_i$ and $\text{size}(t'_i) \leq 2^{\text{size}(t_i)}$ in $O(2^{\text{size}(t_i)})$ steps, using at most $\text{size}(t_i)$ applications of right-distributivity, for $i = 1, 2$. Then with $t' = t'_1 \hat{+} t'_2 \in \text{PT}(X)$ we obtain the result.

Second, assume that t is a product term, say, $t = t_1 \hat{\times} t_2$. By our induction hypothesis, we can construct a polynomial term $t'' \in \text{PT}(X)$ with $t_2 =_{E_{\text{rd}}} t''$ and $\text{size}(t'') \leq 2^{\text{size}(t_2)}$ in $O(2^{\text{size}(t_2)})$ steps, using at most $\text{size}(t_2)$ applications of right-distributivity. Then, by Lemma 6.4 (note that $t_1 \in \text{ST}(X)$), we can construct a polynomial term $t' \in \text{PT}(X)$ with $t_1 \hat{\times} t'' =_{E_{\text{rd}}} t'$ and $\text{size}(t') \leq 2^{\text{size}(t_1)} \cdot \text{size}(t'') \leq 2^{\text{size}(t_1)} \cdot 2^{\text{size}(t_2)} \leq 2^{\text{size}(t)}$ in $O(2^{\text{size}(t_1)})$ steps, using at most $\text{size}(t_1)$ applications of right-distributivity. In total, our construction of t' used at most $O(2^{\text{size}(t)})$ steps with at most $\text{size}(t)$ applications of right-distributivity, and $t =_{E_{\text{rd}}} t_1 \hat{\times} t'' =_{E_{\text{rd}}} t'$.

(c) Similarly as in (b), we may assume without loss of generality that $t \in \text{ST}(X)$. First, as in (b), we construct the polynomial term t_2 from t . Then we apply Lemma 6.2 to obtain in time $O(\text{size}(t_2))$ an id-reduced term t_3 with $t_2 =_{\text{AC}_{\text{id}}} t_3$ and $\text{size}(t_3) \leq \text{size}(t_2)$. Then t_3 is an id-reduced polynomial term. $\square$

Observe that the above proof immediately gives rise to an inductive algorithm for computing a polynomial term $t' \in \text{PT}(X)$ which is $=_{E_{\text{rd}}}$ -equivalent to a given term $t \in \text{ST}(X)$, as follows, by iterating (1) and (2):

(1) If t is a sum term with sum-product decomposition $t = t_1 \hat{+} \dots \hat{+} t_n$, apply the algorithm to each term t_i separately and take the sum of the resulting polynomial terms.

(2) If t is a product term with product-sum decomposition $t = t_1 \hat{\times} \dots \hat{\times} t_n$, first find a polynomial term $t'_n \in \text{PT}(X)$ with $t_n =_{E_{\text{rd}}} t'_n$. Then follow the proof of Lemma 6.4 to find, successively, polynomial terms $t'_{n-1}, \dots, t'_1 \in \text{PT}(X)$ with $t'_i =_{E_{\text{rd}}} t_i \hat{\times} t'_{i+1}$, for $i = n-1, \dots, 1$. Here, replace each possibly arising term of the form $\hat{1} \hat{\times} s$ by s . Then we have $t =_{E_{\text{rd}}} t'_1$.

This algorithm will employ at most $\text{size}(t)$ applications of right-distributivity.

As a consequence, we obtain algorithms for deciding the equivalence of terms modulo our congruences, as indicated by Theorem 5.4. For deciding the AC-equivalence of simple terms, we have already obtained in Lemma 6.1 a linear time algorithm.

Corollary 6.6. It is decidable, given $s, t \in \text{T}(X)$ and $n = \max\{\text{size}(s), \text{size}(t)\}$, in linear time $O(n)$ whether $s =_E t$, and in exponential time $O(2^n)$ whether $s =_{E_{\text{rd}}} t$ and whether $s =_{E_{\text{id}, \text{rd}}} t$.

Proof. For the first claim, given $s, t \in \text{T}(X)$, use Theorem 6.5 to construct $s', t' \in \text{ST}(X)$ with $s =_E s'$ and $t =_E t'$ in $O(n)$ steps. By Theorem 5.4(a) it follows that $s =_E t$ if and only if $s' =_E t'$ if and only if $s' =_{\text{AC}} t'$. The latter AC-equivalences can be decided in $O(n)$ steps by using Lemma 6.1.

For the second claim, we proceed analogously. By Theorem 6.5, we construct $s', t' \in \text{PT}(X)$, each of size at most 2^n , with $s =_{E_{\text{rd}}} s'$ and $t =_{E_{\text{rd}}} t'$ in $O(2^n)$ steps. By Theorem 5.4(b) we have $s =_{E_{\text{rd}}} t$ if and only if $s' =_{E_{\text{rd}}} t'$ if and only if $s' =_{\text{AC}} t'$. The latter AC-equivalences can be decided by Lemma 6.1 with a number of steps linear in the sizes of s' and t' .

The proof of the third claim can be obtained from the proof of the second one by replacing $=_{E_{rd}}$ and Theorem 5.4(b) by $=_{E_{id,rd}}$ and Theorem 5.4(c), respectively. $\square$

Unfortunately, as is well-known from the theory of terms and polynomials over $\mathbb{N}$, the above decision algorithm needs exponentially many steps (in the size of the given terms). This also applies here, using only right-distributivity. The above algorithm rests on the construction of a polynomial equivalent to a given term. Now, let $t_1 = \hat{1} \hat{+} \hat{1}$ and inductively, $t_{n+1} = (\hat{1} \hat{+} \hat{1}) \hat{\times} t_n$ for each $n \geq 1$. With our algorithm, we can transform t_n into a sum term with 2^n summands of $\hat{1}$. Since t_n has size $3 + 4 \times (n - 1)$, this algorithm employs $O(2^n)$ many steps.

Next, we wish to further investigate effective procedures for constructing polynomial terms as in Theorem 6.5.

Given $t \in T(X)$, perform the following algorithm for constructing a polynomial term $t' \in PT(X)$ with $t =_{E_{rd}} t'$.

- (1) Eliminate additions of $\hat{0}$ and multiplications with $\hat{0}$ or $\hat{1}$, as in the proof of Theorem 5.5.
- (2) Replace a subterm of the form $(t_1 \hat{\times} t_2) \hat{\times} t_3$ by $t_1 \hat{\times} (t_2 \hat{\times} t_3)$.
- (3) Replace a subterm of the form $(t_1 \hat{+} t_2) \hat{\times} t_3$ by $(t_1 \hat{\times} t_3) \hat{+} (t_2 \hat{\times} t_3)$.
- (4) Iterate (1), (2) and (3) as far as possible.

We will see that this process terminates (cf. Lemma 6.10). It transforms the term t into a simple term t' which has no subterms of the form $(t_1 \hat{\times} t_2) \hat{\times} t_3$ or $(t_1 \hat{+} t_2) \hat{\times} t_3$. By Lemma 6.7 shown below, then $t' \in PT(X)$. Since these reductions imply $=_{E_{rd}}$ -congruency, we obtain $t =_{E_{rd}} t'$ as claimed.

Lemma 6.7. Let $t \in ST(X)$. If t has neither subterms of the form $(t_1 \hat{\times} t_2) \hat{\times} t_3$ nor subterms of the form $(t_1 \hat{+} t_2) \hat{\times} t_3$, then $t \in PT(X)$.

Proof. We proceed by induction on the size of t . For this, let $t \in ST(X)$ which satisfies the condition of the lemma.

If $t \in \{\hat{0}, \hat{1}\}$, then the statement is clear by Definition 4.7(1).

Let $t = u_1 \hat{+} u_2$. Then both u_1 and u_2 are in $ST(X)$ and they satisfy the condition of the lemma. Hence, by induction hypothesis, $u_1, u_2 \in PT(X)$ and thus, by Definition 4.7(2), $t \in PT(X)$.

Lastly, let $t = u_1 \hat{\times} u_2$. Since t satisfies the condition of the lemma, u_1 is neither a sum term nor a product term, i.e., $u_1 \in X$. Moreover, by induction hypothesis, $u_2 \in PT(X)$. Then by Definition 4.7(3), $t \in PT(X)$. $\square$

Next, we wish to show that in the above algorithm the replacements of (1), (2) and (3) can be done in any order and will terminate. Moreover, then we will obtain a *unique* polynomial term, which can therefore be considered as the normal form of the term t , as will shown below in Theorem 6.13.

For this, we recall some concepts from abstract reduction systems [BN98, Sec. 2] and term rewriting [BN98, Sec. 4-6.], see also [Klo92].

Let A be a set and $\rightarrow$ a binary relation on A . An element $a \in A$ is a *normal form* (with respect to $\rightarrow$) if there does not exist $b \in A$ such that $a \rightarrow b$. For every $a, b \in A$, if $a \rightarrow^* b$ and b is a normal form, then b is a *normal form of a* (with respect to $\rightarrow$). We say that $\rightarrow$ is *terminating* if there does not exist a family $(a_n \mid n \in \mathbb{N})$ of elements of A such that $a_n \rightarrow a_{n+1}$ for each

$n \in \mathbb{N}$. Moreover, $\rightarrow$ is *confluent* if, for every $a, b_1, b_2 \in A$ with $a \rightarrow^* b_1$ and $a \rightarrow_R^* b_2$, there exists $c \in A$ such that $b_1 \rightarrow^* c$ and $b_2 \rightarrow^* c$.

Now let Σ be an arbitrary signature. We define the *set of positions* of terms by a mapping pos from $T_\Sigma(Z)$ to the collection of finite subsets of $\mathbb{N}_+^*$ such that

- (i) for each $t \in (\Sigma^{(0)} \cup Z)$ let $\text{pos}(t) = \{\varepsilon\}$ and
- (ii) for every $t = \sigma(t_1, \dots, t_k)$ with $k \in \mathbb{N}_+$, $\sigma \in \Sigma^{(k)}$, and $t_1, \dots, t_k \in T_\Sigma(Z)$, let $\text{pos}(t) = \{\varepsilon\} \cup \{iv \mid i \in [k], v \in \text{pos}(t_i)\}$.

Then, let $t, u \in T_\Sigma(Z)$ and $w \in \text{pos}(t)$. We define the *subterm of t at w* , denoted by $t|_w$ and the *replacement of the subterm of t at w by u* , denoted by $t[u]_w$, by structural induction as follows:

- (i) if $t \in (\Sigma^{(0)} \cup Z)$, then $t|_\varepsilon = t$, and $t[u]_\varepsilon = u$,
- (ii) for every $t = \sigma(t_1, \dots, t_k)$ with $k \in \mathbb{N}_+$, $\sigma \in \Sigma^{(k)}$, and $t_1, \dots, t_k \in T_\Sigma(Z)$, we let $t|_\varepsilon = t$ and $t[u]_\varepsilon = u$, and for every $i \in [k]$ and $w' \in \text{pos}(t_i)$, we define

$$t|_{iw'} = t_i|_{w'} \quad \text{and} \quad t[u]_{iw'} = \sigma(t_1, \dots, t_{i-1}, t_i[u]_{w'}, t_{i+1}, \dots, t_k).$$

By a *substitution* we mean a mapping $\varphi : Z \rightarrow T_\Sigma(Z)$. Such a mapping φ extends uniquely to a Σ -algebra homomorphism from $T_\Sigma(Z)$ to itself. We denote this extension also by φ . The name substitution is due to the fact that for each $t \in T_\Sigma(Z)$, the term $\varphi(t)$ is obtained by substituting $\varphi(z)$ for z in t , for each $z \in Z$.

A *term rewriting system* over Σ is a set R of Σ -identities over Z (cf. Section 2) such that for each $(\ell, r) \in R$, all variables of r occur in ℓ . We call the identities in R *rules* and we write a rule (ℓ, r) in the form $\ell \rightarrow r$. The reduction relation induced by R on $T_\Sigma(Z)$ (the adaptation of the corresponding concept in Section 2 for $E = R$ and $A = T_\Sigma(Z)$) is the binary relation $\Rightarrow_R$ on $T_\Sigma(Z)$ defined as follows: for every $t_1, t_2 \in T_\Sigma(Z)$, we let $t_1 \Rightarrow_R t_2$ if there exist a position $w \in \text{pos}(t_1)$, a rule $\ell \rightarrow r$ in R , a substitution $\varphi : Z \rightarrow T_\Sigma(Z)$ such that $t_1|_w = \varphi(\ell)$ and $t_2 = t_1[\varphi(r)]_w$.

A term rewriting system R is *terminating* (respectively, *confluent*) if the relation $\Rightarrow_R$ is terminating (respectively, confluent).

Theorem 6.8. [BN98, Lm. 2.18] *Let R be a term rewriting system which is terminating and confluent. Then each element of $T_\Sigma(Z)$ has a unique normal form.* $\square$

Now we consider again how to construct, for a given term $t \in T(X)$, a polynomial term $t' \in \text{PT}(X)$ with $t =_{E_{\text{rd}}} t'$.

For this, we use a term rewriting system over the signature $\Sigma_{\text{sb}} \cup X$, where we consider the elements of X as nullary symbols. We write $T(X, Z)$ for $T_{\Sigma_{\text{sb}} \cup X}(Z)$, hence $T(X) \subset T(X, Z)$.

We consider the following term rewriting system

$$\begin{aligned} \mathcal{R} = \{ & \rho_1 : \hat{0} \hat{+} z \rightarrow z, \quad \rho_2 : z \hat{+} \hat{0} \rightarrow z, \\ & \rho_3 : \hat{1} \hat{\times} z \rightarrow z, \quad \rho_4 : z \hat{\times} \hat{1} \rightarrow z \quad \rho_5 : \hat{0} \hat{\times} z \rightarrow \hat{0}, \quad \rho_6 : z \hat{\times} \hat{0} \rightarrow \hat{0}, \\ & \rho_7 : (z_1 \hat{\times} z_2) \hat{\times} z_3 \rightarrow z_1 \hat{\times} (z_2 \hat{\times} z_3) \\ & \rho_8 : (z_1 \hat{+} z_2) \hat{\times} z_3 \rightarrow (z_1 \hat{\times} z_3) \hat{+} (z_2 \hat{\times} z_3) \} . \end{aligned}$$

Clearly, for every $s, t \in T(X)$, the relation $s \Rightarrow_{\mathcal{R}}^* t$ implies that $s =_{E_{\text{rd}}} t$. We will use this fact without further reference. We will show that $\mathcal{R}$ is terminating and confluent.

We begin with the proof of termination. For the proof we employ the method based on reduction order and monotone polynomial interpretation, see e.g. Sections 5.2 and 5.3 of [BN98]. Since we do not need the full power of that method, we do not recall all concepts and results in their general form.

Our aim is to define a mapping $|\cdot| : T(X, Z) \rightarrow \mathbb{N} \setminus \{0, 1\}$ such that, for every $s, t \in T(X, Z)$, if $s \Rightarrow_{\mathcal{R}} t$, then $|s| > |t|$. Then, for every $s, t \in T(X, Z)$, if $s \Rightarrow_{\mathcal{R}}^+ t$, then $|s| > |t|$, hence there does not exist an infinite sequence $s_1 \Rightarrow_{\mathcal{R}} s_2 \Rightarrow_{\mathcal{R}} \dots$ of reductions. Hence $\mathcal{R}$ is terminating.

We define $|\cdot|$ by induction as follows: for every $y \in X \cup Z \cup \{\hat{0}, \hat{1}\}$, we let $|y| = 2$, and for terms $t_1, t_2 \in T(X)$, we let $|t_1 \hat{+} t_2| = |t_1| + |t_2|$ and $|t_1 \hat{\times} t_2| = |t_1|^2 |t_2|$.

Next we show two properties of the mapping $|\cdot|$. In the proof we will use the fact that $|t| > 1$ for each $t \in T(X)$ without any reference.

Lemma 6.9.

- (a) For every rule $\ell \rightarrow r$ of $\mathcal{R}$ and substitution $\varphi : Z \rightarrow T(X, Z)$, we have $|\varphi(\ell)| > |\varphi(r)|$.
- (b) For every $s, t, u \in T(X, Z)$, if $|s| > |t|$, then $|u \hat{+} s| > |u \hat{+} t|$, $|s \hat{+} u| > |t \hat{+} u|$, $|u \hat{\times} s| > |u \hat{\times} t|$, and $|s \hat{\times} u| > |t \hat{\times} u|$.

Proof. The proof for rules $\rho_1 - \rho_6$ is omitted. For rules ρ_7 and ρ_8 , let $\varphi : Z \rightarrow T(X, Z)$ be a substitution with $\varphi(z_i) = t_i$ for each $i \in \{1, 2, 3\}$. Then

$$|\varphi((z_1 \hat{\times} z_2) \hat{\times} z_3)| = |(t_1 \hat{\times} t_2) \hat{\times} t_3| = |t_1|^4 |t_2|^2 |t_3| > |t_1|^2 |t_2|^2 |t_3| = |t_1 \hat{\times} (t_2 \hat{\times} t_3)| = |\varphi(z_1 \hat{\times} (z_2 \hat{\times} z_3))|,$$

and

$$\begin{aligned} |\varphi((z_1 \hat{+} z_2) \hat{\times} z_3)| &= |(t_1 \hat{+} t_2) \hat{\times} t_3| = |t_1 \hat{+} t_2|^2 |t_3| = (|t_1| + |t_2|)^2 |t_3| > \\ &|t_1|^2 |t_3| + |t_2|^2 |t_3| = |(t_1 \hat{\times} t_3) \hat{+} (t_2 \hat{\times} t_3)| = |\varphi((z_1 \hat{\times} z_3) \hat{+} (z_2 \hat{\times} z_3))|, \end{aligned}$$

which proves, respectively, that (a) holds for rules ρ_7 and ρ_8 .

The proof of (b) is obvious by the definition of $|\cdot|$. □

Lemma 6.10. The term rewriting system $\mathcal{R}$ is terminating.

Proof. By Lemma 6.9, it follows that for every $s, t \in T(X, Z)$, if $s \Rightarrow_{\mathcal{R}} t$, then $|s| > |t|$. Hence $\mathcal{R}$ is terminating. □

Now we turn to the proof of confluency. For this, we recall the concept of a critical pair, cf. [BN98, Def. 6.2.1]. Let again Σ be an arbitrary signature. For the definition of the critical pair, we need the following concepts.

Let $t_1, t_2 \in T_{\Sigma}(Z)$. A substitution $\varphi : Z \rightarrow T_{\Sigma}(Z)$ is a *unifier* of t_1 and t_2 if $\varphi(t_1) = \varphi(t_2)$. A unifier φ of t_1 and t_2 is a *most general unifier* of t_1 and t_2 (for short: mgu) if, for each unifier ψ of t_1 and t_2 there exists a substitution $\theta : Z \rightarrow T_{\Sigma}(Z)$ such that $\psi = \theta \circ \varphi$.

Let $\ell_1 \rightarrow r_1$ and $\ell_2 \rightarrow r_2$ be two rules of some term rewrite system R whose variables have been renamed such that ℓ_1 and ℓ_2 have no common variables. If there exists a $w \in \text{pos}(\ell_1)$ such that $\ell_1(w) \notin Z$, and there exists a most general unifier $\varphi : Z \rightarrow T_{\Sigma}(Z)$ of $\ell_1|_w$ and ℓ_2 , then we say that the two rules *overlap*. In this case these objects determine the *critical pair* $\langle \varphi(r_1), \varphi(\ell_1)[\varphi(r_2)]_w \rangle$ of R .

Proposition 6.11. (cf. [BN98, Cor. 6.2.5]) A terminating term rewriting system R is confluent iff for each $\langle t_1, t_2 \rangle$ of its critical pairs there exists a $t \in T_\Sigma(Z)$ such that $t_1 \Rightarrow_R^* t$ and $t_2 \Rightarrow_R^* t$. $\square$

Now we return to our particular term rewriting system $\mathcal{R}$ and show the following result.

Lemma 6.12. The term rewriting system $\mathcal{R}$ is confluent.

Proof. By Lemma 6.10, it suffices to show that all critical pairs of $\mathcal{R}$ are joinable in the sense of Proposition 6.11.

In the following table we show some critical pairs of $\mathcal{R}$. In the first column we show the rules ρ_i and ρ_j which we consider for a critical pair, where $i, j \in \{1, \dots, 8\}$. By ℓ_i and r_i we denote the left-hand side and the right-hand side of the rule ρ_i , respectively. We assume that the variables z_1, z_2 , and z_3 in ρ_j are renamed y_1, y_2 , and y_3 , respectively (cf. the definition of critical pair). In the second, third, and fourth column we show the position w at which $\ell_i|_w$ and ℓ_j overlap, the most general unifier, and the critical pair, respectively.

rules ρ_i and renamed ρ_j	overlap	mgu φ	critical pair $\langle \varphi(r_i), \varphi(\ell_i)[\varphi(r_j)]_w \rangle$
ρ_7, ρ_7	$\ell_7 _1, \ell_7$	$z_1 \mapsto y_1 \hat{\times} y_2$ $z_2 \mapsto y_3$	$\langle (y_1 \hat{\times} y_2) \hat{\times} (y_3 \hat{\times} z_3), ((y_1 \hat{\times} y_2) \hat{\times} y_3) \hat{\times} z_3 \rangle$
ρ_7, ρ_8	$\ell_7 _1, \ell_8$	$z_1 \mapsto y_1 \hat{+} y_2$ $z_2 \mapsto y_3$	$\langle (y_1 \hat{+} y_2) \hat{\times} (y_3 \hat{\times} z_3), ((y_1 \hat{\times} y_3) \hat{+} (y_2 \hat{\times} y_3)) \hat{\times} z_3 \rangle$

It is easy to check that for each $\langle t_1, t_2 \rangle$ of the above critical pairs there exists a $t \in T(X, Z)$ such that $t_1 \Rightarrow_{\mathcal{R}}^* t$ and $t_2 \Rightarrow_{\mathcal{R}}^* t$. For instance, let us consider the critical pair for ρ_7, ρ_8 . Then

$$(y_1 \hat{+} y_2) \hat{\times} (y_3 \hat{\times} z_3) \Rightarrow_{\mathcal{R}} y_1 \hat{\times} (y_3 \hat{\times} z_3) \hat{+} y_2 \hat{\times} (y_3 \hat{\times} z_3) \Rightarrow_{\mathcal{R}}^2 (y_1 \hat{\times} y_3) \hat{\times} z_3 \hat{+} (y_2 \hat{\times} y_3) \hat{\times} z_3$$

by using rules ρ_8 and ρ_7 twice, and

$$((y_1 \hat{\times} y_3) \hat{+} (y_2 \hat{\times} y_3)) \hat{\times} z_3 \Rightarrow_{\mathcal{R}} (y_1 \hat{\times} y_3) \hat{\times} z_3 \hat{+} (y_2 \hat{\times} y_3) \hat{\times} z_3$$

by using rule ρ_8 .

The proof for the other critical pairs is left to the reader. $\square$

As an immediate consequence, we obtain the following normal form result for representing arbitrary terms by polynomial terms.

Theorem 6.13. For each term $t \in T(X)$, there is a unique polynomial term $t' \in \text{PT}(X)$ in normal form with respect to $\Rightarrow_{\mathcal{R}}$ such that $t \Rightarrow_{\mathcal{R}}^* t'$, in particular $t =_{E_{\text{rd}}} t'$.

Proof. Let $t \in T(X)$. By Lemmas 6.10 and 6.12, and Theorem 6.8, there is a unique term $t' \in T(X)$ in normal form with respect to $\Rightarrow_{\mathcal{R}}$. Due to the shape of the rules in $\mathcal{R}$, $t' \in \text{ST}(X)$ and t' has neither subterms of the form $(t_1 \hat{\times} t_2) \hat{\times} t_3$ nor subterms of the form $(t_1 \hat{+} t_2) \hat{\times} t_3$. Then $t' \in \text{PT}(X)$ by Lemma 6.7. $\square$

We note that different reduction strategies by $\mathcal{R}$ may involve different numbers of applications of the right-distributivity rule ρ_7 . As example, we use the term given after Corollary 6.6.

Example 6.14. Let $t_1 = \hat{1} \hat{+} \hat{1}$ and inductively, $t_n = (\hat{1} \hat{+} \hat{1}) \hat{\times} t_{n-1}$ for each $n \geq 2$. Fix some $n \geq 2$. Then t_n is a product of n factors of $\hat{1} \hat{+} \hat{1}$.

In our first strategy, we apply right-distributivity always to the left-most factor. We claim that then for t_n we will use $2^{n-1} - 1$ applications of right-distributivity to obtain the equivalent polynomial term. We have:

$$t_n \Rightarrow_{\mathcal{R}} (\hat{1} \hat{\times} t_{n-1}) \hat{+} (\hat{1} \hat{\times} t_{n-1}) \Rightarrow_{\mathcal{R}}^2 t_{n-1} \hat{+} t_{n-1} .$$

By induction, for t_{n-1} our method employs $2^{n-2} - 1$ applications of right-distributivity to obtain the equivalent polynomial term. Substituting these for both t_{n-1} , we obtain a polynomial term equivalent to t_n (a sum term with 2^n summands of $\hat{1}$).

In total then we have $1 + 2(2^{n-2} - 1) = 2^{n-1} - 1$ applications of right-distributivity, as claimed. Since t_n has size $3 + 4 \times (n - 1)$, this is exponential in the size of t_n .

In our second strategy, we follow the algorithm described after the proof of Theorem 6.5. First, note that the final factor $(\hat{1} \hat{+} \hat{1})$ is already a polynomial term. Now we can apply right-distributivity to the next factor on the left and rule ρ_3 , and we obtain

$$t_n \Rightarrow_{\mathcal{R}}^* t_{n-2} \hat{\times} ((\hat{1} \hat{+} \hat{1}) \hat{\times} (\hat{1} \hat{+} \hat{1})) \Rightarrow_{\mathcal{R}}^3 t_{n-2} \hat{\times} ((\hat{1} \hat{+} \hat{1}) \hat{+} (\hat{1} \hat{+} \hat{1}))$$

In contrast to the previous sum term, here we have obtained again a product term, now with $n - 1$ factors. By an induction hypothesis, this employs $n - 2$ further applications of right-distributivity (just apply right-distributivity successively from the right to the left).

In total, we need $n - 1$ applications of right-distributivity to find the (same) equivalent polynomial term. This number is bounded by the size of t_n . $\square$

Next we wish to derive a result like Theorem 6.13 for the idempotent case, i.e., for a construction of an id-reduced polynomial term as in Theorem 5.5. For this, in order to simplify, e.g., a term like $s \hat{+} (t \hat{+} s)$ to $s \hat{+} t$, our term rewriting rules will need to include rules for associativity and commutativity. However, as is well-known, an inclusion of both implications taken from the identities e_1, e_2 leads to a term rewriting systems which is (obviously) not terminating. Therefore, as is standard in the literature, we will employ R/E rewriting, where R is a term rewriting system and E is a set of identities, see e.g. [JK84] and [BP85]. The relation $\Rightarrow_{R/E}$, called *R-rewriting modulo E*, is defined by $\Rightarrow_{R/E} = \Leftrightarrow_E^* \circ \Rightarrow_R \circ \Leftrightarrow_E^*$. We say that R is *E-terminating* if the relation $\Rightarrow_{R/E}$ is terminating.

Let

$$\rho_9 : z \hat{+} z \rightarrow z \text{ and } \mathcal{R}_{\text{id}} = \mathcal{R} \cup \{\rho_9\}.$$

Clearly, the term rewriting systems $\mathcal{R}$ and $\mathcal{R}_{\text{id}}$ are not AC-terminating, as can be seen by considering $\rho_7 \in \mathcal{R}$ and $e_4 \in \text{AC}$. Therefore, subsequently we consider the set $\text{AC}_+ = \{e_1, e_2\}$. Also, let $\text{AC}_{+, \text{id}} = \{e_1, e_2, e_{11}\}$.

Lemma 6.15. The term rewriting system $\mathcal{R}_{\text{id}}$ is AC_+ -terminating on $\text{T}(X)$.

Proof. Let $s, t \in \text{T}(X)$ such that $s \Rightarrow_{\mathcal{R}_{\text{id}}/\text{AC}_+} t$. There exist $s', t' \in \text{T}(X)$ with $s =_{\text{AC}_+} s' \Rightarrow_{\mathcal{R}_{\text{id}}} t' =_{\text{AC}_+} t$. Then $|s| = |s'| > |t'| = |t|$. Hence, $\mathcal{R}_{\text{id}}/\text{AC}_+$ is terminating. $\square$

Next, we derive a confluence type result for the relation $\Rightarrow^*_{\mathcal{R}_{\text{id}}/\text{AC}_+}$.

Lemma 6.16. Let $s, t, u \in \text{ST}(X)$ be such that $u \Rightarrow^*_{\mathcal{R}_{\text{id}}/\text{AC}_+} s$ and $u \Rightarrow^*_{\mathcal{R}_{\text{id}}/\text{AC}_+} t$. Then there are $s'', t'' \in \text{PT}_{\text{id}}(X)$ in $\mathcal{R}$ -normal form such that $s \Rightarrow^*_{\mathcal{R}_{\text{id}}/\text{AC}_+} s''$ and $t \Rightarrow^*_{\mathcal{R}_{\text{id}}/\text{AC}_+} t''$, and $s'' =_{\text{AC}_+} t''$.

Proof. By Theorem 6.13, we find polynomial terms $s', t' \in \text{PT}(X)$ in $\mathcal{R}$ -normal form such that $s \Rightarrow^*_{\mathcal{R}} s'$ and $t \Rightarrow^*_{\mathcal{R}} t'$. Now, by using AC_+ we can re-order the summands of sum-product decompositions of s' and t' and of their subterms so that identical summands are next to each other. Then we can apply rule ρ_9 to delete multiple summands. Here, it may happen that we reduce a sum of the form $(\hat{1} \dot{+} \dots \dot{+} \hat{1})$ to $\hat{1}$.

In case the sum $(\hat{1} \dot{+} \dots \dot{+} \hat{1})$ occurred as a factor in a product-sum decomposition of s' resp. t' or their subterms, it must have occurred as the last factor of this product, since otherwise we could have applied right-distributivity (rule ρ_8), but s' and t' are in $\mathcal{R}$ -normal form. In this case we delete the factor $\hat{1}$ in these products by applying rule ρ_4 . Hence we obtain $s'', t'' \in \text{PT}_{\text{id}}(X)$ such that $s' \Rightarrow^*_{\mathcal{R}_{\text{id}}/\text{AC}_+} s''$ and $t' \Rightarrow^*_{\mathcal{R}_{\text{id}}/\text{AC}_+} t''$. These applications of rule ρ_9 and possibly rule ρ_4 do not change the structure of the parenthesizing, so we cannot apply rules ρ_7 or ρ_8 . Hence s'' and t'' are in $\mathcal{R}$ -normal form.

Then, we have $s'' =_{\text{AC}_{\text{id}}} s' =_{E_{\text{rd}}} s =_{E_{\text{id}, \text{rd}}} u =_{E_{\text{id}, \text{rd}}} t =_{E_{\text{rd}}} t' =_{\text{AC}_{\text{id}}} t''$, so $s'' =_{E_{\text{id}, \text{rd}}} t''$. By Theorem 5.4(c), we obtain $s'' =_{\text{AC}} t''$. Since s'' and t'' are in $\mathcal{R}$ -normal form, we obtain $s'' =_{\text{AC}_+} t''$. $\square$

As an immediate consequence, we obtain the following normal form result for representing arbitrary terms by id-reduced polynomial terms.

Theorem 6.17. For each term $t \in \text{T}(X)$, there is an AC_+ -unique id-reduced polynomial term $t' \in \text{PT}_{\text{id}}(X)$ in $\mathcal{R}_{\text{id}}/\text{AC}_+$ -normal form such that $t \Rightarrow^*_{\mathcal{R}_{\text{id}}/\text{AC}_+} t'$, in particular $t =_{E_{\text{id}, \text{rd}}} t'$.

Proof. Immediate by Lemmas 6.15 and 6.16. $\square$

7 An application in weighted automata theory

As noted in Section 1, weighted (tree) automata assign to each input (i.e., a word or a term over a ranked alphabet) a value from some given weight structure. A weighted (tree) automaton is called *finite-valued*, if the set of all values assigned is finite. From the beginning of the theory of weighted automata, it has been an essential question to find conditions for determining whether weighted automata over particular weight structures are finite-valued. It is easy to see that if the weight structure is a strong bimonoid $\mathbf{B}$ which is locally finite (i.e., each finitely generated strong subbimonoid is finite), then each weighted (tree) automaton over $\mathbf{B}$ is finite-valued (cf., e.g., [FV22]). For more detailed investigations, cf. e.g. [DSV10], [DFKV22], and [FV22]. Among others, the notion of "weakly locally finite" strong bimonoid was introduced (precise definition is given below). It was shown that each weighted automaton over a weakly locally finite strong bimonoid is finite-valued [DSV10, Lm. 18]. However, the situation changes for weighted tree automata. In fact, by Theorem [DFTV24, Thm. 5.1], for each ranked alphabet which contains at least one binary symbol and for each finitely generated strong bimonoid, we can construct a weighted tree automaton over that ranked alphabet which takes on all elements of the given

strong bimonoid as values. Hence, if the strong bimonoid is finitely generated and infinite, then this weighted tree automaton is infinite-valued even if the strong bimonoid is weakly locally finite. Therefore, it is important to know if there are strong bimonoids which are weakly locally finite but not locally finite. The question was answered positively in [DFTV24, Thm. 3.5], where a right-distributive and weakly locally finite but not locally finite strong bimonoid was constructed.

The main goal of this section is to sharpen this result as follows: we will construct an idempotent right-distributive strong bimonoid which is weakly locally finite but not locally finite.

We start with giving the relevant definitions. Let Σ be a signature and $\mathbf{A} = (A, \theta)$ be a Σ -algebra. For $A' \subseteq A$, we denote by $\langle A' \rangle_{\theta(\Sigma)}$ the smallest subset of A which contains A' and is closed under the operations in $\theta(\Sigma)$. The Σ -algebra $\mathbf{A} = (A, \theta)$ is *locally finite* if, for each finite subset $A' \subseteq A$, the set $\langle A' \rangle_{\theta(\Sigma)}$ is finite.

Let $\mathbf{B} = (B, \oplus, \otimes, 0, 1)$ be a strong bimonoid and $A \subseteq B$. The *weak closure of A (with respect to $\mathbf{B}$)*, denoted by $\text{wcl}(A)$, is the smallest subset $C \subseteq B$ such that $A \cup \{0, 1\} \subseteq C$ and, for every $b, b' \in C$ and $a \in A$, we have $b \oplus b' \in C$ and $b \otimes a \in C$.

We call the strong bimonoid $\mathbf{B}$

- *additively locally finite* if $(B, \oplus, 0)$ is locally finite,
- *multiplicatively locally finite* if $(B, \otimes, 1)$ is locally finite,
- *bi-locally finite* if it is additively and multiplicatively locally finite, and
- *weakly locally finite* if, for each finite subset $A \subseteq B$, the weak closure of A is finite.

The following implications between the above properties of strong bimonoids immediately follow from the corresponding definitions:

$$\text{locally finite} \Rightarrow \text{weakly locally finite} \Rightarrow \text{bi-locally finite}.$$

We will also use the following result.

Lemma 7.1. [DSV10, Rem. 17] Let $\mathbf{B}$ be a right distributive strong bimonoid. Then $\mathbf{B}$ is bi-locally finite if and only if $\mathbf{B}$ is weakly locally finite.

We just note in passing that without the assumption of right-distributivity, there are examples of strong bimonoids which are bi-locally finite but not weakly locally finite, see [DV12, Ex. 2.1(2)] and [DSV10, Ex. 25] (cf. [FV22, Ex. 2.6.10(2),(9)]).

In the rest of this section we will prove the following result (for the proof cf. Theorem 7.8).

Theorem 7.2. *There exists an idempotent right-distributive strong bimonoid $\mathbf{M}$ which is weakly locally finite but not locally finite.*

The underlying idea is indicated by the following lemma.

Lemma 7.3. Let $\mathbf{B} = (B, +, \times, 0, 1)$ be an idempotent right-distributive strong bimonoid, and let $d \in B$. Let $\sim$ be a congruence relation on $\mathbf{B}$ such that for all $a, b, c \in B \setminus \{0, 1\}$, we have $a \times (b \times c) \sim d \times (d \times c)$. Then $\mathbf{B}/\sim$ is an idempotent right-distributive weakly locally finite strong bimonoid.

Proof. We write $\mathbf{B}/\sim = (B/\sim, \oplus, \otimes, 0, 1)$. Clearly, $\mathbf{B}/\sim$ is an idempotent, hence additively locally finite, right-distributive strong bimonoid. We show that it is also multiplicatively locally

finite as follows. If F is a finite subset of $\mathbf{B}/\sim$, then the multiplicative submonoid $\langle F \rangle_{\{\otimes\}}$ of $\mathbf{B}/\sim$ generated by F contains $F \cup \{1\}$, all binary products of elements of F and, possibly, $[d]_{\sim} \otimes ([d]_{\sim} \otimes [d]_{\sim})$. Thus $\langle F \rangle_{\{\otimes\}}$ is finite.

Hence, $\mathbf{B}/\sim$ is bi-locally finite. Since $\mathbf{B}/\sim$ is right-distributive, by Lemma 7.1, it is weakly locally finite. $\square$

The problem is to construct a strong bimonoid $\mathbf{B}$ and a congruence $\sim$ satisfying the conditions of Lemma 7.3, but so that the strong bimonoid $\mathbf{B}/\sim$ is not locally finite.

For this, we will exploit the idempotent right-distributive strong bimonoid $\mathbf{B}_{\text{id,rd}}[X]$. Clearly, $\mathbf{B}_{\text{id,rd}}[X]$ is not multiplicatively locally finite, since for each $x \in X$, the multiplicative submonoid generated by $\{[x]_{\text{AC}}\}$ is infinite. Hence our goal is to choose a suitable congruence $\sim$ on $\mathbf{B}_{\text{id,rd}}[X]$ so that the strong bimonoid $\mathbf{M}(X) = \mathbf{B}_{\text{id,rd}}[X]/\sim$ satisfies the conditions of Lemma 7.3, without being locally finite.

We will need the notion of subpolynomial. Intuitively, an id-reduced polynomial p is a subpolynomial of an id-reduced polynomial q , if q can be obtained from p and arbitrary id-reduced polynomials resp. monomials by the constructions described in Observation 4.21. The exact definition is the following.

Definition 7.4. Let $p, q \in \mathbf{B}_{\text{id,rd}}[X]$. We say that p is a *subpolynomial* of q , if whenever U is a subset of $\mathbf{B}_{\text{id,rd}}[X]$ satisfying that

- $p \in U$,
- if $r \in U$, $r' \in \mathbf{B}_{\text{id,rd}}[X]$ and m is a monomial, then $r +_{\text{id}} r' \in U$ and $m \times r \in U$, and
- if $m \in U$ is a monomial and $r \in \mathbf{B}_{\text{id,rd}}[X]$, then $m \times r \in U$,

then $q \in U$. $\square$

Equivalently, we have $p = [s]_{\text{AC}}$ and $q = [t]_{\text{AC}}$ for some $s, t \in \text{PT}_{\text{id}}(X)$ such that s is a subterm of t .

We define the collection of large polynomials in $\mathbf{B}_{\text{id,rd}}[X]$ as follows. Intuitively, all products $p \times_{\text{rd}} (q \times_{\text{rd}} r)$ of id-reduced polynomials $p, q, r \in \mathbf{B}_{\text{id,rd}}[X] \setminus \{0, 1\}$ are large, and any id-reduced polynomial obtained from a large polynomial by adding or multiplying it with any further id-reduced polynomials should also be large. As formal definition we take the following.

Definition 7.5. A polynomial $q \in \mathbf{B}_{\text{id,rd}}[X] \setminus \{0, 1\}$ is *large*, if q has a subpolynomial p of the form

$$p = [x]_{\text{AC}} \times (([y_1]_{\text{AC}} \times p') + \dots + ([y_n]_{\text{AC}} \times p')),$$

where $n \geq 1$, $x, y_1 \in X$, $y_i \in X \cup \{\hat{1}\}$ for each $i \in [n]$, the elements $y_1, \dots, y_n$ are pairwise different, and $p' \in \mathbf{B}_{\text{id,rd}}[X] \setminus \{0, 1\}$. $\square$

Subsequently, we will use the following implication several times: If $q \in \mathbf{B}_{\text{id,rd}}[X]$ is large, $r \in \mathbf{B}_{\text{id,rd}}[X]$ and m is a monomial, then $q +_{\text{id}} r = r +_{\text{id}} q$ and $m \times q$ are also large. This is immediate, since each subpolynomial of q is also a subpolynomial of $q +_{\text{id}} r$ and of $m \times q$.

Lemma 7.6. Let $p, q, r \in \mathbf{B}_{\text{id,rd}}[X] \setminus \{0, 1\}$. Then $p \times_{\text{rd}} (q \times_{\text{rd}} r)$ is large.

Proof. We put $u = p \times_{\text{rd}} (q \times_{\text{rd}} r)$. We proceed by induction on $\text{size}(p) + \text{size}(q)$. First, assume that $p = [x]_{\text{AC}}$ with $x \in X$. Then $u = p \times (q \times_{\text{rd}} r)$.

If also $q \in X/AC$, say $q = [y]_{AC}$ with $y \in X$, then $u = [x]_{AC} \times ([y]_{AC} \times r)$ has the required form showing that u is large.

Now, let q be a sum polynomial. Write $q = q_1 + \dots + q_n$ where $n \geq 2$ and each q_i is a product polynomial or an element of $X/AC \cup \{1\}$, and the elements $q_1, \dots, q_n$ are pairwise different. Recall that by Corollary 4.17(b), the elements $q_1 \times_{rd} r, \dots, q_n \times_{rd} r$ are pairwise different. Then $u = p \times (q_1 \times_{rd} r + \dots + q_n \times_{rd} r)$.

First assume that $q_i \in X/AC \cup \{1\}$ for each $i \in [n]$. Since q is id-reduced, we have $q_i = 1$ for at most one $i \in [n]$. Since $n \geq 2$, we may assume that $q_1 \in X/AC$. Then $u = p \times (q_1 \times r + \dots + q_n \times r)$, showing that u has the form described in Definition 7.5.

Second, assume that there exists $i \in [n]$ such that q_i is a product polynomial. Then $q_i = m_i \times q'_i$ for a monomial m_i and a polynomial $q'_i \neq 1$. Since $\text{size}(m_i) + \text{size}(q'_i) < \text{size}(q) < \text{size}(p) + \text{size}(q)$, by our induction hypothesis the product $q_i \times_{rd} r = m_i \times_{rd} (q'_i \times_{rd} r)$ is large. Then, as noted above, $q_1 \times_{rd} r + \dots + q_n \times_{rd} r$ is also large, hence also u .

Next, let q be a product polynomial. Write $q = m \times q'$ with a monomial m and a polynomial q' . Then $u = p \times (m \times (q' \times_{rd} r))$. Since $\text{size}(m) + \text{size}(q') < \text{size}(q) < \text{size}(p) + \text{size}(q)$, by our induction hypothesis the product $m \times (q' \times_{rd} r) = m \times_{rd} (q' \times_{rd} r)$ is large. Again, as noted above, then also u is large.

Secondly, assume that p is a sum polynomial. Write $p = p_1 + \dots + p_n$ where $n \geq 2$, and each p_i is a product polynomial or an element of $X/AC \cup \{1\}$, and the elements $p_1, \dots, p_n$ are pairwise different. Since $n \geq 2$, there is $j \in [n]$ with $p_j \neq 1$. We have $u = p_1 \times_{rd} (q \times_{rd} r) + \dots + p_n \times_{rd} (q \times_{rd} r)$. Since $\text{size}(p_j) + \text{size}(q) < \text{size}(p) + \text{size}(q)$, by our induction hypothesis the product $p_j \times_{rd} (q \times_{rd} r)$ is large, consequently also u .

Finally, let p be a product polynomial. Write $p = m \times p'$ with a monomial m and a polynomial p' . Then $u = m \times (p' \times_{rd} (q \times_{rd} r))$. Since $\text{size}(p') + \text{size}(q) < \text{size}(p) + \text{size}(q)$, by the induction hypothesis the product $p' \times_{rd} (q \times_{rd} r)$ is large, consequently again also u . $\square$

Next we show that the collection of large polynomials is closed under the addition of and multiplication with arbitrary id-reduced polynomials.

Lemma 7.7. Let $p, q \in \mathbb{B}_{id,rd}[X] \setminus \{0, 1\}$. If p is large, then $p +_{id} q$, $p \times_{rd} q$ and $q \times_{rd} p$ are also large.

Proof. Let p be large. The result for $p +_{id} q$ was already noted before.

Now we consider $p \times_{rd} q$. We proceed by case distinction.

First, let p be a monomial. Then $p \times_{rd} q = p \times q$. Each subpolynomial of p is also a subpolynomial of $p \times q$. Hence $p \times q$ is large.

Secondly, let p be a product polynomial. Then $p = m \times p'$ for a monomial m and a polynomial $p' \neq 1$. Then by Lemma 7.6, $p \times_{rd} q = m \times_{rd} (p' \times_{rd} q)$ is large.

Thirdly, assume that p is a sum polynomial. Write $p = p_1 + \dots + p_n$ where $n \geq 2$ and each p_i is a product polynomial or an element of $X/AC \cup \{1\}$, and the elements $p_1, \dots, p_n$ are pairwise different. Clearly, we cannot have $p_i \in X/AC \cup \{1\}$ for each $i \in [n]$, since then p would not be large. Hence there is $i \in [n]$ such that p_i is a product polynomial. Then, as shown above, $p_i \times_{rd} q$ is large by Lemma 7.6. As already seen, then the sum polynomial $p \times_{rd} q = p_1 \times_{rd} q + \dots + p_n \times_{rd} q$ is also large.

Finally, we consider $q \times_{\text{rd}} p$. We proceed again by case distinction.

If q is a monomial, we have $q \times_{\text{rd}} p = q \times p$ and our assumption on p implies the result for $q \times p$.

Also, if q is a product polynomial, by Lemma 7.6, $q \times_{\text{rd}} p$ is large.

It remains to consider the case that q is a sum polynomial. Write $q = q_1 + \dots + q_n$ where $n \geq 2$ and each q_i is a product polynomial or an element of $X/\text{AC} \cup \{1\}$, and the elements $q_1, \dots, q_n$ are pairwise different. Then $q \times_{\text{rd}} p = q_1 \times_{\text{rd}} p + \dots + q_n \times_{\text{rd}} p$. Now if q_1 is a product polynomial, then by Lemma 7.6, $q_1 \times_{\text{rd}} p$ is large. From this we obtain, as before, that the sum given by $q \times_{\text{rd}} p$ is large. But if $q_1 \in X/\text{AC} \cup \{1\}$, then $q_1 \times_{\text{rd}} p = q_1 \times p$, and the assumption on p implies that $q_1 \times p$ is large, consequently again also $q \times_{\text{rd}} p$. $\square$

We note in passing that, as a consequence, a polynomial $\pi \in \mathbb{B}_{\text{id,rd}}[X]$ is large if and only if π contains a product of the form $p \times_{\text{rd}} (q \times_{\text{rd}} r)$, for some $p, q, r \in \mathbb{B}_{\text{id,rd}}[X] \setminus \{0, 1\}$, as a subpolynomial. Here the "if" part is immediate by Lemma 7.6. The converse is also immediate noting that the subpolynomial described in Definition 7.5 can be written as $[x]_{\text{AC}} \times_{\text{rd}} (([y_1]_{\text{AC}} + \dots + [y_n]_{\text{AC}}) \times_{\text{rd}} p')$. This was our goal mentioned before Definition 7.5. However, this characterization will not be used subsequently.

Now we define a binary relation $\sim_L$ on $\mathbb{B}_{\text{id,rd}}[X]$ as follows: for every $q, r \in \mathbb{B}_{\text{id,rd}}[X]$, we let $q \sim_L r$ if and only if $q = r$ or both q and r are large.

Clearly, by Lemma 7.7, if $p, q, r \in \mathbb{B}_{\text{id,rd}}[X]$ and $q \sim_L r$, then also $p +_{\text{id}} q \sim_L p +_{\text{id}} r$, $p \times_{\text{rd}} q \sim_L p \times_{\text{rd}} r$, and $q \times_{\text{rd}} p \sim_L r \times_{\text{rd}} p$. Hence $\sim_L$ is a congruence on $\mathbb{B}_{\text{id,rd}}[X]$.

The quotient algebra of $\mathbb{B}_{\text{id,rd}}[X]$ with respect to $\sim_L$ is

$$\mathbb{B}_{\text{id,rd}}[X]/\sim_L = (\mathbb{B}_{\text{id,rd}}[X]/\sim_L, +_{\text{id}}/\sim_L, \times_{\text{rd}}/\sim_L, [0]_{\sim_L}, [1]_{\sim_L}) .$$

The algebra $\mathbb{B}_{\text{id,rd}}[X]/\sim_L$ is an idempotent, right-distributive strong bimonoid because it is a factor algebra of the strong bimonoid $\mathbb{B}_{\text{id,rd}}[X]$.

In the following we abbreviate $\mathbb{B}_{\text{id,rd}}[X]/\sim_L$ by $\mathbf{M}(X)$, and abbreviate also the components of $\mathbb{B}_{\text{id,rd}}[X]/\sim_L$ by writing $\mathbf{M}(X) = (\mathbf{M}(X), \oplus, \otimes, \mathbf{0}, \mathbf{1})$. Moreover, for each $q \in \mathbb{B}_{\text{id,rd}}[X]$, we abbreviate $[q]_{\sim_L}$ by $[q]_L$.

With the following result, we also obtain Theorem 7.2.

Theorem 7.8. *The strong bimonoid $\mathbf{M}(X) = (\mathbf{M}(X), \oplus, \otimes, \mathbf{0}, \mathbf{1})$ is idempotent, right-distributive, weakly locally finite and not locally finite.*

Proof. We show that $\mathbf{M}(X)$ is weakly locally finite. Choose any $\pi \in \mathbb{B}_{\text{id,rd}}[X] \setminus \{0, 1\}$, and let $p, q, r \in \mathbb{B}_{\text{id,rd}}[X] \setminus \{0, 1\}$. By Lemma 7.6, the products $p \times_{\text{rd}} (q \times_{\text{rd}} r)$ and $\pi \times_{\text{rd}} (\pi \times_{\text{rd}} \pi)$ are both large, hence $p \times_{\text{rd}} (q \times_{\text{rd}} r) \sim_L \pi \times_{\text{rd}} (\pi \times_{\text{rd}} \pi)$. Now Lemma 7.3 shows that $\mathbf{M}(X) = \mathbb{B}_{\text{id,rd}}[X]/\sim_L$ is weakly locally finite, as claimed.

It remains to show that $\mathbf{M}(X)$ is not locally finite. Choose an $x \in X$.

We define, for each $n \in \mathbb{N}$, the polynomials $p_n \in \text{PT}(X)$ inductively by letting

$$p_0 = [x]_{\text{AC}} \text{ and } p_{n+1} = [x]_{\text{AC}} \times (1 + p_n) = [x]_{\text{AC}} \times_{\text{rd}} (1 + p_n).$$

So, e.g., $p_1 = [x]_{\text{AC}} \times (1 + [x]_{\text{AC}})$ and $p_2 = [x]_{\text{AC}} \times (1 + p_1) = [x]_{\text{AC}} \times (1 + ([x]_{\text{AC}} \times (1 + [x]_{\text{AC}})))$. Then $p_n \in \mathbb{B}_{\text{id,rd}}[X]$ for each $n \in \mathbb{N}$.

Moreover, for each $n \in \mathbb{N}$, p_n is a product polynomial and, in particular, we have $1 + p_n = 1 +_{\text{id}} p_n$.

Now we show that, for each $n \in \mathbb{N}$, p_n is not large. Clearly, p_0 and p_1 are not large. Now let $n \geq 1$ such that p_n is not large, but suppose that p_{n+1} is large. Then p_{n+1} has a subpolynomial p of the form described in Definition 7.5. Since $p_{n+1} = 1 + p_n$ is a sum polynomial but p is a product polynomial, we have $p_{n+1} \neq p$. Hence there are polynomials $q_1, q_2 \in \mathbb{B}_{\text{id}, \text{rd}}[X]$ such that p is a subpolynomial of q_1 and $p_{n+1} = q_1 +_{\text{id}} q_2$. By Lemma 4.9(b), we obtain $q_1 = p_n$ and $q_2 = 1$. Hence, p is a subpolynomial of p_n , a contradiction.

Alternatively, we may argue for p_{n+1} and its subpolynomial p as follows. Choose simple terms $s, t \in \text{ST}(X)$ such that $p_{n+1} = [t]_{\text{AC}}$, $p = [s]_{\text{AC}}$ and s is a subterm of t . Then, due to the form of p and the product term s , the labeled graph $\bar{t}$ would contain a vertex labeled with $\boxplus$ whose children are not $\bar{1}$. But considering the construction of p_{n+1} , it is easy to see that in $\bar{t}$, each vertex labeled with $\boxplus$ has precisely two children, one of them being $\bar{1}$.

Consequently, for each $n \in \mathbb{N}$, p_n is not large.

Next, let $m \in \mathbb{N}$. We claim that $p_m \neq p_n$ for all $n \in \mathbb{N}$ with $m < n$. We proceed by induction on m . Trivially, $p_0 \neq p_n$ for each $n \in \mathbb{N}_+$. Now let $m, n \in \mathbb{N}$ with $m + 1 < n$. Suppose we had $p_{m+1} = p_n$. Then $n \geq 2$ and $1 + p_m = p_{m+1} = p_n = 1 + p_{n-1}$. Since p_m and p_{n-1} are product polynomials, by Lemma 4.9(b), we obtain $p_m = p_{n-1}$. But since $m < n - 1$, our induction hypothesis implies $p_m \neq p_{n-1}$, a contradiction.

Now for each $n \in \mathbb{N}$, we let $a_n = [p_n]_L \in \mathbf{M}(X)$. Then $a_{n+1} = [[x]_{\text{AC}}]_L \otimes (\mathbb{1} \oplus a_n)$ for each $n \in \mathbb{N}$, so $a_n \in \langle \{\mathbb{1}, a_0\} \rangle_{\{\oplus, \otimes\}}$.

Now if $m, n \in \mathbb{N}$ with $m < n$, both p_m and p_n are not large and $p_m \neq p_n$. Hence, $p_m \not\sim_L p_n$, showing $a_m \neq a_n$.

Thus, $\langle \{\mathbb{1}, a_0\} \rangle_{\{\oplus, \otimes\}}$ is infinite, showing that $\mathbf{M}(X)$ is not locally finite. $\square$

References

- [ACIM12] L. Aceta, M. Cimini, A. Ingolfssdottir, and M. Mousavi. Rule formats for distributivity. *Theoret. Comput. Sci*, 458:1–28, 2012.
- [AHU74] A.V. Aho, J.E. Hopcroft, and J.D. Ullman. *The Design and Analysis of Computer Algorithms*. Addison-Wesley, 1974.
- [AJTT17] T. Akutsu, J. Jansson, A. Takasu, and T. Tamura. On the parameterized complexity of associative and commutative unification. *Theoret. Comput. Sci*, 660:57–74, 2017.
- [BKN87] D. Benanav, D. Kapur, and P. Narendran. Complexity of matching problems. *Journal of Symbolic Computation*, 3:203–216, 1987.
- [BN98] F. Baader and T. Nipkow. *Term Rewriting and All That*. Cambridge University Press, 1998.
- [BP85] L. Bachmair and D. A. Plaisted. Termination orderings for associative-commutative rewriting systems. *J. Symbolic Computation*, 1:329–349, 1985.

- [BS81] S. Burris and H.P. Sankappanavar. *A Course in Universal Algebra*, volume 78 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, first edition, 1981. Corrected version available at <http://www.thoralf.uwaterloo.ca/htdocs/ualg.html>.
- [CDIV10] M. Ćirić, M. Droste, J. Ignjatović, and H. Vogler. Determinization of weighted finite automata over strong bimonoids. *Inform. Sci.*, 180(18):3497–3520, 2010.
- [DFKV22] M. Droste, Z. Fülöp, D. Kószó, and H. Vogler. Finite-image property of weighted tree automata over past-finite monotonic strong bimonoids. *Theoret. Comput. Sci.*, 919:118–143, 2022.
- [DFTV24] M. Droste, Z. Fülöp, A. Tepavčević, and H. Vogler. The generating power of weighted tree automata with initial algebra semantics. submitted for publication, see also: arXiv 2405.20753, 2024.
- [Dic05] L. E. Dickson. On finite algebras. *Nachr. Ges. Wiss. Göttingen*, pages 358–393, 1905.
- [DSV10] M. Droste, T. Stüber, and H. Vogler. Weighted finite automata over strong bimonoids. *Inform. Sci.*, 180(1):156–166, 2010.
- [DV10] M. Droste and H. Vogler. Kleene and Büchi theorems for weighted automata and multi-valued logics over arbitrary bounded lattices. In Y. Gao, H. Lu, S. Seki, and S. Yu, editors, *Developments in Language Theory (DLT 2020)*, volume 6224 of *Lecture Notes in Computer Science*, pages 160–172. Springer, 2010.
- [DV12] M. Droste and H. Vogler. Weighted automata and multi-valued logics over arbitrary bounded lattices. *Theoret. Comput. Sci.*, 418:14–36, 2012.
- [EEK⁺13] S. Erbatur, S. Escobar, D. Kapur, Z. Liu, C. Lynch, C. Meadows, J. Meseguer, P. Narendran, S. Santiago, and R. Sasse. Asymmetric unification: A new unification paradigm for cryptographic protocol analysis. In M. P. Bonacina, editor, *24th International Conference on Automated Deduction (CADE 2013)*, volume 7898 of *Lecture Notes in Computer Science*, pages 231–248. Springer, Berlin, Heidelberg, 2013.
- [FV22] Z. Fülöp and H. Vogler. *Weighted Tree Automata – May it be a little more?* arXiv:2212.05529 [cs.FL], 2022.
- [FV24] Z. Fülöp and H. Vogler. *Weighted Tree Automata – May it be a little more?* second edition, arXiv:2212.05529v2, 2024.
- [GL86] I. Gnaeding and P. Lescanne. Proving termination of associative commutative rewriting systems by rewriting. In Jörg H. Siekman, editor, *8th International Conference on Automated Deduction*, volume 230 of *Lecture Notes in Computer Science*, pages 52–61. Springer, 1986.
- [Gol99] J.S. Golan. *Semirings and their Applications*. Kluwer Academic Publishers, Dordrecht, 1999.
- [GR04] N. Galatos and J.G. Raftery. Adding involution to residuated structures. *Studia Logica*, 77:181–207, 2004.

- [Grä68] G. Grätzer. *Universal Algebra*. D. van Nostrand Comp., 1968.
- [HW93] U. Hebisch and H.J. Weinert. *Semirings - Algebraic Theory and Applications in Computer Science*. World Scientific, 1993.
- [JK84] J.-P. Jouannaud and H. Kirchner. Completion of a set of rules modulo a set of equations. In *POPL '84: Proceedings of the 11th ACM SIGACT-SIGPLAN symposium on Principles of programming languages*, pages 83–92, New York, NY, United States, 1984. ACM.
- [Klo92] J. W. Klop. Term rewriting systems. In S. Abramsky, Dov M. Gabbay, and T. S. E. Maibaum, editors, *Handbook of Logic in Computer Science, Vol. 2*, Oxford Science Publications, chapter 1. Oxford University Press, 1992.
- [Kri05] K.V. Krishna. *Near-Semirings: Theory and Applications*. PhD thesis, IIT Delhi, New Delhi, India, 2005.
- [MMN15] A.M. Marshall, C. Meadows, and P. Narendran. On unification modulo one-sided distributivity: Algorithms, variants and asymmetry. *Logical Methods in Computer Science*, 11(2:11):1–39, 2015.
- [Moh97] M. Mohri. Finite-state transducers in language and speech processing. *Computational Linguistics*, 23(2):269–311, 1997.
- [Pil77] G. Pilz. *Near-rings: The Theory and Its Applications*. North Holland, Amsterdam, 1977.
- [Sch97] Ch. Schwartz. Nonlinear operators. II. *J. Math. Physics*, 38(7):3841–3862, 1997.
- [TA87] E. Tidén and S. Arnold. Unification problems with one-sided distributivity. *J. of Symbolic Computation*, 3:183–202, 1987.
- [vHvR67] W.G. van Hoorn and B. van Rootselaar. Fundamental notions in the theory of seminearrings. *Compositio Mathematica*, 18:65–78, 1967.
- [VW24] N. Veltri and Cheng-Syuan Wan. Semi-substructural logics with additives. *Elect. Proc. Theoret. Comp. Sci.*, 402:63–80, 2024.
- [Wec92] W. Wechler. *Universal Algebra for Computer Scientists*, volume 25 of *EATCS Monographs on Theoretical Computer Science*. Springer-Verlag, Heidelberg/Berlin, first edition, 1992.
- [Zas36] H. Zassenhaus. Über endliche Fastkörper. *Abh. Math. Sem. Univ. Hamburg*, 11:187–220, 1936.