ASSOCIATIVE STRING FUNCTIONS

ERKKO LEHTONEN, JEAN-LUC MARICHAL, AND BRUNO TEHEUX

Abstract. We introduce the concept of associativity for string functions, where a string function is a unary operation on the set of strings over a given alphabet. We discuss this new property and describe certain classes of associative string functions. We also characterize the recently introduced preassociative functions as compositions of associative string functions with injective unary maps. Finally, we provide descriptions of the classes of associative and preassociative functions which depend only on the length of the input.

1. Introduction

Throughout this paper, X denotes a nonempty set, called the *alphabet,* and its elements are called *letters*. The symbol X^* stands for the free monoid $\bigcup_{n\geqslant 0} X^n$ generated by X, and its elements are called *strings*. Thus, we assume that X^* is endowed with the concatenation operation for which the empty string ε is the neutral element. We denote the elements of X^* by bold roman letters $\mathbf{x}$, $\mathbf{y}$, $\mathbf{z}$. If we want to stress that such an element is a letter of X, we use non-bold italic letters x, y, z, … For every string $\mathbf{x}$ and every integer $n \geqslant 0$, the power $\mathbf{x}^n$ stands for the string obtained by concatenating n copies of $\mathbf{x}$. In particular, we have $\mathbf{x}^0 = \varepsilon$. The notation $\mathbf{x}^*$ stands for the set of all powers of $\mathbf{x}$. The *length* of a string $\mathbf{x}$ is denoted by $|\mathbf{x}|$. In particular, we have $|\varepsilon| = 0$.

The classical concept of associativity for binary operations can be easily generalized to string-defined operations (or $*$-ary operations, *pronounced "star-ary"*), i.e., functions $F\colon \bigcup_{n\geqslant 1} X^n \to X$ which are extended to X^* by setting $F(\varepsilon) = \varepsilon$. A $*$-ary operation $F\colon X^* \to X$ is said to be *associative* [2, p. 24] if

$$F(\mathbf{x}\mathbf{y}\mathbf{z}) = F(\mathbf{x}F(\mathbf{y})\mathbf{z}), \qquad \mathbf{x},\mathbf{y},\mathbf{z} \in X^*. \tag{1}$$

A *string function* over the alphabet X is a mapping $F\colon X^* \to X^*$. Interestingly, formally applying identity (1) to string functions enables us to immediately extend the definition of associativity of $*$-ary operations to string functions.

Data processing can be seen as the computation of string functions. Many common-place data processing tasks correspond to associative string functions, e.g., sorting data in alphabetical order, transforming a string of letters into upper case. In this context, associativity may be a desirable property because it allows to work locally on small pieces of data at a time.

By definition every $*$-ary operation $F\colon X^* \to X$ satisfies the condition

$$F(\mathbf{x}) = \varepsilon \quad \Longleftrightarrow \quad \mathbf{x} = \varepsilon. \tag{2}$$

Date: March 27, 2014.

2010 *Mathematics Subject Classification.* 20M05, 20M32, 39B72, 68R99.

Key words and phrases. Associativity, preassociativity, string functions, functional equation, axiomatizations.

For string functions $F\colon X^* \to X^*$, this condition may or may not hold. For instance it holds when F corresponds to sorting the letters of every string in alphabetical order and does not hold when F consists in removing from every string all occurrences of a given letter.

In Section 2 of this paper we investigate the associativity property for string functions. In particular, we provide different equivalent definitions of this property. We also investigate the subclass of associative functions $F\colon X^* \to X^*$ satisfying the condition $|F(\mathbf{x})| \leqslant m$ for every $\mathbf{x} \in X^*$, where m is a fixed nonnegative integer (when $m = 1$ this subclass includes the associative $*$-ary operations). In Section 3 we investigate the class of preassociative functions, which was recently introduced in [3]. In particular we characterize these functions as compositions of associative string functions with injective unary maps. Finally, in Section 4 we provide descriptions of the classes of associative and preassociative functions which depend only on the length of the input.

The following notation will be used in this paper. We let $\mathbb{N}$ denote the set of nonnegative integers. For every $n \in \mathbb{N}$ and for every function $F\colon X^* \to Y$, we denote by F_n the *n-ary part of F*, i.e., the restriction $F|_{X^n}$ of F to the set X^n. The domain and range of any function f are denoted by $\mathrm{dom}(f)$ and $\mathrm{ran}(f)$, respectively. The identity function on any nonempty set is denoted by id.

2. Associative functions

As mentioned in the introduction, we extend the definition of associativity of $*$-ary operations to string functions.

Definition 2.1. We say that a function $F\colon X^* \to X^*$ is *string-associative* if it satisfies Eq. (1). We say that it is *associative* if it satisfies both Eqs. (1) and (2).

Clearly, the identity function on X^* is associative. The following two examples provide nontrivial instances of string-associative and associative functions.

Example 2.2 (Letter removing)**.** Let $a \in X$ be fixed. Let the map $F_a\colon X^* \to X^*$ be defined inductively by $F_a(z) = z$ if $z \neq a$, $F_a(a) = \varepsilon$, and $F_a(\mathbf{x}z) = F_a(\mathbf{x})F_a(z)$. Let also the map $G_a\colon X^* \to X^*$ be defined by $G_a(\mathbf{x}) = a$, if $\mathbf{x} \in a^*$, and $G_a(\mathbf{x}) = F_a(\mathbf{x})$, if $\mathbf{x} \notin a^*$. Then both F_a and G_a are string-associative but not associative. Moreover, $F_a(\varepsilon) = \varepsilon$ and $G_a(\varepsilon) \neq \varepsilon$.

Example 2.3 (Duplicate removing)**.** Define the function $\mathrm{ofo}\colon X^* \to X^*$ by the following procedure. Given a string $\mathbf{x} \in X^*$, delete all repeated occurrences of elements, keeping only the first occurrence of each element; the resulting string is $\mathrm{ofo}(\mathbf{x})$. In other words, the function ofo outputs the letters of its input in the *order of first occurrence* (hence the acronym ofo). For example,

$$\mathrm{ofo}(\mathit{indivisibilities}) = \mathit{indvsblte}\,,$$
$$\mathrm{ofo}(\mathit{uncopyrightable}) = \mathit{uncopyrightable}\,.$$

It is easy to verify that the function ofo is associative.

Fact 2.4. *Any string-associative function $F\colon X^* \to X^*$ is idempotent w.r.t. composition, i.e., we have $F \circ F = F$ (take $\mathbf{xz} = \varepsilon$ in Eq. (1)).*

As the examples given above illustrate, it is natural for a string-associative function $F\colon X^* \to X^*$ to satisfy $F(\varepsilon) = \varepsilon$. Indeed, if $F(\varepsilon) = \mathbf{a}$ for some $\mathbf{a} \in X^* \setminus \{\varepsilon\}$, then by string-associativity we obtain $F(\mathbf{xz}) = F(\mathbf{xa}^*\mathbf{z})$ for every $\mathbf{x},\mathbf{z}\in X^*$, which shows that $F(\varepsilon)$ in a sense behaves like the empty string ε.

The following result, which also holds for $*$-ary operations (replacing string-associativity with associativity, see [1]), gives equivalent definitions of string-associativity under the condition $F(\varepsilon)=\varepsilon$.

Proposition 2.5. *Let $F\colon X^*\to X^*$ be a function such that $F(\varepsilon)=\varepsilon$. The following conditions are equivalent.*

(i) *F is string-associative.*
(ii) *For any $\mathbf{x},\mathbf{y},\mathbf{z},\mathbf{x}',\mathbf{y}',\mathbf{z}'\in X^*$ such that $\mathbf{xyz}=\mathbf{x}'\mathbf{y}'\mathbf{z}'$ we have $F(\mathbf{x}F(\mathbf{y})\mathbf{z}) = F(\mathbf{x}'F(\mathbf{y}')\mathbf{z}')$.*
(iii) *For any $\mathbf{x},\mathbf{y},\mathbf{z}\in X^*$ we have $F(F(\mathbf{xy})\mathbf{z}) = F(\mathbf{x}F(\mathbf{yz}))$.*
(iv) *For any $\mathbf{x},\mathbf{y}\in X^*$ we have $F(\mathbf{xy}) = F(F(\mathbf{x})F(\mathbf{y}))$.*

Proof. (i) $\implies$ (ii) $\implies$ (iii). Trivial.

(iii) $\implies$ (iv). Taking $\mathbf{yz}=\varepsilon$ shows that F satisfies $F\circ F=F$. Taking $\mathbf{x}=\varepsilon$ and then $\mathbf{z}=\varepsilon$, we obtain $F(\mathbf{x}F(\mathbf{y})) = F(F(\mathbf{x})\mathbf{y}) = F(F(\mathbf{xy})) = F(\mathbf{xy})$ and therefore $F(F(\mathbf{x})F(\mathbf{y})) = F(\mathbf{xy})$.

(iv) $\implies$ (i). F clearly satisfies $F\circ F=F$ (take $\mathbf{y}=\varepsilon$). Repeated applications of (iv) then give

$$\begin{aligned}F(\mathbf{x}F(\mathbf{y})\mathbf{z}) &= F(F(\mathbf{x}F(\mathbf{y}))F(\mathbf{z})) = F(F(F(\mathbf{x})F(F(\mathbf{y})))F(\mathbf{z}))\\ &= F(F(F(\mathbf{x})F(\mathbf{y}))F(\mathbf{z})) = F(F(\mathbf{xy})F(\mathbf{z})) = F(\mathbf{xyz}),\end{aligned}$$

which completes the proof. □

The following proposition shows that the definition of string-associativity remains unchanged if the length of the string $\mathbf{xz}$ is bounded above by one.

Proposition 2.6. *A function $F\colon X^*\to X^*$ is string-associative if and only if $F(\mathbf{xyz}) = F(\mathbf{x}F(\mathbf{y})\mathbf{z})$ for any $\mathbf{x},\mathbf{y},\mathbf{z}\in X^*$ such that $|\mathbf{xz}|\leqslant 1$.*

Proof. Necessity is obvious. For sufficiency, assume that $F(\mathbf{xyz}) = F(\mathbf{x}F(\mathbf{y})\mathbf{z})$ for any $\mathbf{x},\mathbf{y},\mathbf{z}\in X^*$ such that $|\mathbf{xz}|\leqslant 1$. We prove by induction on $|\mathbf{xz}|$ that $F(\mathbf{xyz}) = F(\mathbf{x}F(\mathbf{y})\mathbf{z})$ holds for all $\mathbf{x},\mathbf{y},\mathbf{z}\in X^*$. The basis of the induction is clear from our assumption. Assume that the claim holds if $|\mathbf{xz}|=k$ for some $k\geqslant 1$. Let $\mathbf{x},\mathbf{y},\mathbf{z}\in X^*$ be such that $|\mathbf{xz}|=k+1$. If $|\mathbf{x}|\geqslant 1$, then $\mathbf{x}=a\mathbf{x}'$ for some $a\in X$, $\mathbf{x}'\in X^*$, with $|\mathbf{x}'|=|\mathbf{x}|-1$, and we have

$$F(\mathbf{x}F(\mathbf{y})\mathbf{z}) = F(aF(\mathbf{x}'F(\mathbf{y})\mathbf{z})) = F(aF(\mathbf{x}'\mathbf{yz})) = F(\mathbf{xyz}),$$

where the first and the third equalities hold by our assumption, and the second equality holds by the induction hypothesis since $|\mathbf{x}'\mathbf{z}| = |\mathbf{xz}|-1 = k$. A similar argument shows that $F(\mathbf{x}F(\mathbf{y})\mathbf{z}) = F(\mathbf{xyz})$ if $|\mathbf{z}|\geqslant 1$. This completes the proof, because at least one of $\mathbf{x}$ and $\mathbf{z}$ is nonempty. □

It is noteworthy that any string-associative function $F\colon X^*\to X^*$ satisfies the following equation

$$F(x_1\cdots x_n) \;=\; F(F(x_1\cdots x_{n-1})x_n)\,,\qquad n\geqslant 1, \tag{3}$$

or equivalently,

$$F(x_1\cdots x_n) \;=\; F(F(\cdots F(F(x_1)x_2)\cdots)x_n)\,,\qquad n\geqslant 1. \tag{4}$$

It is well known that associative $*$-ary operations satisfy Eq. (3) and therefore are completely determined by their unary and binary parts (see, e.g., [3]). The following proposition gives an extension of this observation to string functions.

Definition 2.7. Let D be a nonempty set and let $m \in \mathbb{N}$. We say that a map $F\colon D \to X^*$ is *m-bounded* if $|F(\mathbf{x})| \leqslant m$ for every $\mathbf{x} \in D$.

For instance, a function $F\colon X^* \to X^*$ is a $*$-ary operation if and only if it is 1-bounded and satisfies Eq. (2).

Proposition 2.8. *Let $F\colon X^* \to X^*$ be a string-associative function and let $m \in \mathbb{N}$.*

(a) *F is m-bounded if and only if $F_0, \dots, F_{m+1}$ are m-bounded.*
(b) *If F is m-bounded, then F is uniquely determined by its parts of arity at most $m+1$, i.e., if $G\colon X^* \to X^*$ is a string-associative m-bounded function such that $G_i = F_i$ for $i = 0, \dots, m+1$, then $F = G$.*

Proof. (a) Necessity is trivial. For sufficiency, assume that $F_0, \dots, F_{m+1}$ are m-bounded. We show by induction on k that F_k is m-bounded. Assume that F_k is m-bounded for some $k \geqslant m+1$. Let $\mathbf{x} \in X^{k+1}$. By string-associativity we have $F_{k+1}(x_1 \cdots x_{k+1}) = F(F_k(x_1 \cdots x_k) x_{k+1})$. Since F_k is m-bounded we have $|F(F_k(x_1 \cdots x_k) x_{k+1})| \leqslant m$ and hence F_{k+1} is m-bounded.

(b) Let $F\colon X^* \to X^*$ and $G\colon X^* \to X^*$ be string-associative m-bounded functions such that $G_i = F_i$ for $i = 0, \dots, m+1$. We show by induction on k that $F_k = G_k$ for all $k \in \mathbb{N}$. Assume that $F_k = G_k$ for some $k \geqslant m+1$. Let $\mathbf{x} \in X^{k+1}$. We then have

$$\begin{aligned} G_{k+1}(x_1 \cdots x_{k+1}) = G(G_k(x_1 \cdots x_k) x_{k+1}) &= G(F_k(x_1 \cdots x_k) x_{k+1}) \\ &= F(F_k(x_1 \cdots x_k) x_{k+1}) = F_{k+1}(x_1 \cdots x_{k+1}), \end{aligned}$$

where the first equality holds by string-associativity of G, the second equality holds by the inductive hypothesis, the third equality holds since F is m-bounded and by the inductive hypothesis, and the last equality holds by string-associativity of F. We conclude that $F = G$. $\square$

Setting $m = 1$ in Proposition 2.8(a) leads immediately to the following corollary.

Corollary 2.9. *An associative function $F\colon X^* \to X^*$ is a $*$-ary operation if and only if $\mathrm{ran}(F_1) \subseteq X$ and $\mathrm{ran}(F_2) \subseteq X$.*

The following result gives necessary and sufficient conditions for an m-bounded function $F\colon X^* \to X^*$ to be string-associative. This result was established in [3, Proposition 3.3] in the special case of $*$-ary operations.

Proposition 2.10. *Let $m \in \mathbb{N}$. An m-bounded function $F\colon X^* \to X^*$ is string-associative if and only if the following conditions are satisfied.*

(a) *$F \circ F_k = F_k$ for $k = 0, \dots, m+1$.*
(b) *$F(F(x\mathbf{y})z) = F(xF(\mathbf{y}z))$ for all $x \in X$, $\mathbf{y} \in X^*$, and $z \in X$ such that $|x\mathbf{y}z| \leqslant m+2$.*
(c) *Condition (3) or condition (4) holds.*

Proof. Conditions (a)–(c) clearly follow from string-associativity. We prove that conditions (a)–(c) are sufficient. By conditions (b)–(c) and Proposition 2.6, it is enough to show that $F \circ F = F$ and that $F(x\mathbf{y}z) = F(F(x\mathbf{y})z) = F(xF(\mathbf{y}z))$ for all $x\mathbf{y}z \in X^*$ such that $|x\mathbf{y}z| > m+2$. For the second assertion, we proceed by induction on $k = |x\mathbf{y}z|$. Assume that the condition holds for some $k \geqslant m+2$ and let $u \in X$. We then have

$$F(x\mathbf{y}zu) = F(F(x\mathbf{y}z)u) = F(F(xF(\mathbf{y}z))u) = F(xF(F(\mathbf{y}z)u)) = F(xF(\mathbf{y}zu)),$$

where the first equality is obtained by condition (c) and the other equalities by the induction hypothesis and the fact that F is m-bounded.

It remains to prove that $F \circ F = F$, or equivalently, $F \circ F_k = F_k$ for every $k \in \mathbb{N}$. According to condition (a), we may assume that $k \geqslant m+2$. Setting $\mathbf{x} = \mathbf{y}z$ such that $|\mathbf{x}| \geqslant m+2$, we have

$$F(\mathbf{x}) = F(\mathbf{y}z) = F(F(\mathbf{y})z) = F(F(F(\mathbf{y})z)) = F(F(\mathbf{y}z)) = F(F(\mathbf{x})),$$

where the second and the fourth equality are obtained by condition (c) and the third by condition (a) and the fact that F is m-bounded. □

The following important result immediately follows from Proposition 2.10. It gives necessary and sufficient conditions on $F_0, \ldots, F_{m+1}$ for an m-bounded function $F\colon X^* \to X^*$ to be string-associative.

Theorem 2.11. *Let $m \in \mathbb{N}$. For $k = 0, \ldots, m+1$, let $F_k\colon X^k \to X^*$ be an m-bounded function. Then there exists a string-associative m-bounded function $G\colon X^* \to X^*$ such that $G_k = F_k$ for $k = 0, \ldots, m+1$ if and only if conditions (a)–(b) of Proposition 2.10 hold. Such a function is then uniquely determined by the condition $G(\mathbf{y}z) = G(G(\mathbf{y})z)$ for every $\mathbf{y} \in X^*$ and every $z \in X$.*

Remark 1. Let $F\colon X^* \to X^*$ be a string-associative m-bounded function and let $k \in \{0, \ldots, m\}$. From Proposition 2.10 it follows that if we replace F_j with the identity function on X^j for $j = 0, \ldots, k$, then the resulting function is still string-associative and m-bounded.

It is clear that the identity function on X^* is an associative function that is not m-bounded for any $m \in \mathbb{N}$. The following examples provide other instances of associative functions that are not m-bounded.

Example 2.12. Let $|$ be a fixed letter of the alphabet X, and define the string function $F\colon X^* \to X^*$ by the following procedure: given an input string, insert the letter $|$ between any two consecutive letters neither one of which is $|$. For example,

$$F(a) = a, \quad F(ab) = F(a|b) = a|b, \quad F(||) = ||, \quad F(||ab|||cd) = ||a|b|||c|d.$$

It is an easy exercise to verify that the function F is associative. It is also clear that F is not m-bounded for any $m \in \mathbb{N}$.

Example 2.13. Let $m \in \mathbb{N}$ and let $c \in X$. Assume that $F\colon X^* \to X^*$ is a string-associative function that satisfies $|F_k(\mathbf{x})| = k$ for $k = 0, \ldots, m$. The function $G\colon X^* \to X^*$ defined by $G_0 = F_0, \ldots, G_m = F_m$, and $G_k = c^k$ for every $k \geqslant m+1$, is associative.

Remark 2. It is an open problem whether Example 2.13 would remain true if we replaced the equality $|F_k(\mathbf{x})| = k$ with the inequality $|F_k(\mathbf{x})| \leqslant k$.

We end this section by investigating the string-associative functions which are injective. Actually, as the following result shows, string-associative functions are never injective (except the identity function) and hence cannot be used as coding functions.

Proposition 2.14. *If $F: X^* \to X^*$ is injective and satisfies $F = F \circ F$, then it is equal to the identity. In particular, any string-associative injective function $F: X^* \to X^*$ is equal to the identity.*

Proof. Applying F^{-1} to both sides of $F = F \circ F$ immediately shows that F is the identity function. The second statement follows immediately by Fact 2.4. □

Remark 3. Proposition 2.14 can be refined as follows. Suppose $F: X^* \to X^*$ satisfies $F = F \circ F$ and suppose that $\operatorname{ran}(F_k) \subseteq X^k$ and F_k is injective for some $k \in \mathbb{N}$, then $F_k = \mathrm{id}|_{X^k}$.

Proposition 2.14 raises the question of measuring how far a string-associative function different from the identity is from being injective. The following proposition shows that such a function is in a sense highly non-injective.

Definition 2.15. Let $\preceq$ be the quasiorder (i.e., reflexive and transitive binary relation) defined on the set of string functions by setting $F \preceq G$ if $\ker(G) \subseteq \ker(F)$, that is,

$$G(\mathbf{x}) = G(\mathbf{y}) \quad \Longrightarrow \quad F(\mathbf{x}) = F(\mathbf{y}), \qquad \mathbf{x}, \mathbf{y} \in X^*.$$

We denote by $\prec$ the irreflexive part of $\preceq$.

Proposition 2.16. *Let $F: X^* \to X^*$ be a string-associative function different from the identity. Then there is an infinite sequence of string-associative functions $(F^m: X^* \to X^*)_{m \geqslant 1}$ such that $F \preceq F^1 \prec F^2 \prec \cdots \prec \mathrm{id}$.*

Proof. First, we note that there exists $(\mathbf{x}_0, \mathbf{x}_1) \in \ker(F)$ such that $\mathbf{x}_0 \neq \mathbf{x}_1$ and $\varepsilon \notin \{\mathbf{x}_0, \mathbf{x}_1\}$. Indeed, since F is not injective there exists $(\mathbf{y}_0, \mathbf{y}_1) \in \ker(F)$ such that $\mathbf{y}_0 \neq \mathbf{y}_1$. If $\mathbf{y}_0 = \varepsilon$, it follows that for every $\mathbf{x} \in X^*$, we have $F(\mathbf{x}) = F(\mathbf{x}\varepsilon) = F(\mathbf{x}F(\varepsilon)) = F(\mathbf{x}F(\mathbf{y}_1)) = F(\mathbf{x}\mathbf{y}_1)$. Therefore, we can choose $(\mathbf{x}_0, \mathbf{x}_1) = (\mathbf{x}, \mathbf{x}\mathbf{y}_1)$, where $\mathbf{x} \neq \varepsilon$.

For any integer $m \geqslant 0$, denote by θ_m the equivalence relation defined as follows: we say that two strings are θ_m-equivalent if one can be obtained from the other by substituting some occurrences of $\mathbf{x}_0^{2^m}$ with $\mathbf{x}_1^{2^m}$ and some occurrences of $\mathbf{x}_1^{2^m}$ with $\mathbf{x}_0^{2^m}$. It follows that $\theta_{m+1} \subset \theta_m$ for every $m \geqslant 0$ and by definition $\theta_0 \subseteq \ker(F)$.

For every integer $m \geqslant 1$ we denote by π_m the quotient map $\pi_m: X^* \to X^*/\theta_m$ and we let $g_m: X^*/\theta_m \to X^*$ be a map satisfying $g_m(\mathbf{x}/\theta_m) \in \mathbf{x}/\theta_m$. Let us prove that the sequence $(F^m: X^* \to X^*)_{m \geqslant 1}$ defined as $F^m = g_m \circ \pi_m$ satisfies the conditions of the statement. Since by definition we have $\ker(F^m) = \theta_m$ for all $m \geqslant 1$, it remains the prove that the functions F^m are string-associative.

Let $m \geqslant 1$ and let $\mathbf{x}, \mathbf{y}, \mathbf{z} \in X^*$. Since $F^m(\mathbf{y}) = (g_m \circ \pi_m)(\mathbf{y})$ we obtain that $\mathbf{y}$ and $F^m(\mathbf{y})$ are θ_m-equivalent. It follows easily from the definition of θ_m that the strings $\mathbf{xyz}$ and $\mathbf{x}F^m(\mathbf{y})\mathbf{z}$ are θ_m-equivalent, that is, $F^m(\mathbf{xyz}) = F^m(\mathbf{x}F^m(\mathbf{y})\mathbf{z})$. □

3. Preassociative functions

Let Y be a nonempty set. Recall that a function $F: X^* \to Y$ is said to be *preassociative* [3] if

$$F(\mathbf{y}) = F(\mathbf{y}') \quad \Longrightarrow \quad F(\mathbf{xyz}) = F(\mathbf{x}\mathbf{y}'\mathbf{z}), \qquad \mathbf{x}, \mathbf{y}, \mathbf{y}', \mathbf{z} \in X^* \tag{5}$$

and

$$F(\mathbf{x}) = F(\varepsilon) \quad \Longleftrightarrow \quad \mathbf{x} = \varepsilon. \tag{6}$$

Definition 3.1. We say that a function $F\colon X^* \to Y$ is *string-preassociative* if it satisfies Eq. (5).

Example 3.2. The function $F\colon X^* \to \mathbb{N}$ defined by $F(\mathbf{x}) = |\mathbf{x}|$ (number of letters in $\mathbf{x}$) is preassociative. For every $a \in X$, the function $F\colon X^* \to \mathbb{N}$ defined by $F(\mathbf{x}) = |F_a(\mathbf{x})|$ (number of letters in $\mathbf{x}$ distinct from a), where F_a is defined in Example 2.2, is string-preassociative but not preassociative. For every $a \in X$, the function $F\colon X^* \to \mathbb{N}$ defined by $F(\mathbf{x}) = |G_a(\mathbf{x})|$, where G_a is defined in Example 2.2, is not string-preassociative. Indeed, for every $b \in X \setminus \{a\}$, we have $F(ba^*) = F(a^*) = 1$ but $F(b^2a^*) = 2 \neq 1 = F(ba^*)$. The function $F\colon X^* \to \mathbb{N}$ defined by $F(\mathbf{x}) = |\mathrm{ofo}(\mathbf{x})|$ (number of distinct letters in $\mathbf{x}$), where ofo is defined in Example 2.3, is not string-preassociative. Indeed, for distinct $a, b \in X$, we have $F(a) = F(b) = 1$ but $F(aa) = 1 \neq 2 = F(ab)$. Finally, for every $a \in X$, the functions F_a and G_a are string-preassociative but not preassociative. The function ofo is preassociative.

Remark 4. Example 3.2 motivates the following open question. Find necessary and sufficient conditions on a string-associative function $F\colon X^* \to X^*$ for the function $\mathbf{x} \mapsto |F(\mathbf{x})|$ to be string-preassociative.

The following two results are straightforward adaptations of Propositions 4.3 and 4.5 in [3].

Proposition 3.3. *Let $F\colon X^* \to Y$ be a string-preassociative (resp. preassociative) function and let $g\colon Y \to Y'$ be a function. If $g|_{\mathrm{ran}(F)}$ is injective, then the function $H\colon X^* \to Y'$ defined as $H = g \circ F$ is string-preassociative (resp. preassociative).*

Proposition 3.4. *Let $F\colon X^* \to X^*$ be a function. The following conditions hold.*

(a) *F is string-associative if and only if it is string-preassociative and satisfies $F = F \circ F$.*
(b) *If F is associative, then it is preassociative.*
(c) *If F is preassociative and satisfies $F = F \circ F$ and $F(\varepsilon) = \varepsilon$, then it is associative.*

We now define a new concept which will prove to be closely related to m-bounded string functions (see Proposition 3.6).

Definition 3.5. Let $m \in \mathbb{N}$. We say that a map $F\colon X^* \to Y$ has an *m-determined range* if $\mathrm{ran}(F) = \bigcup_{k=0}^{m} \mathrm{ran}(F_k)$.

We immediately observe that the property of having an m-determined range is preserved under left composition with unary maps: if $F\colon X^* \to Y$ has an m-determined range, then so has $g \circ F$ for any map $g\colon Y \to Y'$, where Y' is an nonempty set.

Proposition 3.6. *Let $m \in \mathbb{N}$. Any map $F\colon X^* \to Y$ satisfying $F = F \circ H$, where $H\colon X^* \to X^*$ is m-bounded, has an m-determined range.*

Proof. Let $F\colon X^* \to Y$ be a function satisfying $F = F \circ H$, where $H\colon X^* \to X^*$ is m-bounded, and let $\mathbf{x} \in X^*$. Since H is m-bounded, there exists $k \in \{0, \ldots, m\}$ such that $F(\mathbf{x}) = (F \circ H)(\mathbf{x}) = (F_k \circ H)(\mathbf{x})$. Therefore, we have $\mathrm{ran}(F) \subseteq \bigcup_{k=0}^{m} \mathrm{ran}(F_k)$. Since the other inclusion is obvious, F has an m-determined range. □

We now give a characterization of the string-preassociative (resp. preassociative) functions $F\colon X^* \to Y$ as compositions of the form $F = f \circ H$, where $H\colon X^* \to X^*$ is string-associative (resp. associative) and $f\colon \mathrm{ran}(H) \to Y$ is injective. This result answers a question raised in [3] and is stated in Theorem 3.9 below.

First recall that a function g is a *quasi-inverse* [4, Sect. 2.1] of a function f if

$$f \circ g|_{\mathrm{ran}(f)} = \mathrm{id}|_{\mathrm{ran}(f)} \qquad \text{and} \qquad \mathrm{ran}(g|_{\mathrm{ran}(f)}) = \mathrm{ran}(g).$$

The set of quasi-inverses of a function f is denoted by $Q(f)$. Under the assumption of the Axiom of Choice (AC), the set $Q(f)$ is nonempty for any function f. In fact, the Axiom of Choice is just another form of the statement "every function has a quasi-inverse". Note also that the relation of being quasi-inverse is symmetric: if $g \in Q(f)$ then $f \in Q(g)$; moreover, we have $\mathrm{ran}(g) \subseteq \mathrm{dom}(f)$ and $\mathrm{ran}(f) \subseteq \mathrm{dom}(g)$ and the functions $f|_{\mathrm{ran}(g)}$ and $g|_{\mathrm{ran}(f)}$ are injective.

The following two lemmas are extensions of Proposition 2.2 and Lemma 4.8 in [3].

Lemma 3.7. *Assume AC and let $F\colon X^* \to Y$ be a function. For any $g \in Q(F)$, define the function $H\colon X^* \to X^*$ by $H = g \circ F$. Then the following conditions hold.*

(a) *We have $F = F \circ H$, $H = H \circ H$, and the map $F|_{\mathrm{ran}(H)}$ is injective.*
(b) *F satisfies condition* (6) *if and only if H satisfies condition* (2).

Moreover, if F has an m-determined range for some $m \in \mathbb{N}$, then g can always be chosen so that $\mathrm{ran}(g) \subseteq \bigcup_{k=0}^{m} X^k$ and therefore H is m-bounded. Conversely, if H is m-bounded for some $m \in \mathbb{N}$, then F has an m-determined range.

Proof. By definition of H we have $F \circ H = F \circ g \circ F = F$, $H \circ H = g \circ F \circ g \circ F = g \circ F = H$, and the map $F|_{\mathrm{ran}(g)} = F|_{\mathrm{ran}(H)}$ is injective. If F satisfies condition (6), then from the identity $F(H(\varepsilon)) = F(\varepsilon)$ we immediately derive $H(\varepsilon) = \varepsilon$. Moreover, if $H(\mathbf{x}) = \varepsilon$, then we have $F(\mathbf{x}) = F(H(\mathbf{x})) = F(\varepsilon)$ and therefore $\mathbf{x} = \varepsilon$, which shows that H satisfies condition (2). If H satisfies condition (2), then from the identity $F(\mathbf{x}) = F(\varepsilon)$ we obtain $H(\mathbf{x}) = (g \circ F)(\mathbf{x}) = (g \circ F)(\varepsilon) = H(\varepsilon) = \varepsilon$ and therefore $\mathbf{x} = \varepsilon$, which shows that F satisfies condition (6).

Now, if F has an m-determined range for some $m \in \mathbb{N}$, then there always exists $g \in Q(F)$ such that $\mathrm{ran}(g) \subseteq \bigcup_{k=0}^{m} X^k$; indeed, if $y \in \mathrm{ran}(F_k)$ for some $k \leqslant m$, then we can take $g(y) \in F_k^{-1}\{y\} \subseteq X^k$. Therefore $H = g \circ F$ is m-bounded. Conversely, if H is m-bounded for some $m \in \mathbb{N}$, then F has an m-determined range by Proposition 3.6. □

Lemma 3.8. *Assume AC and let $F\colon X^* \to Y$ be a function. The following assertions are equivalent.*

(i) *F is string-preassociative (resp. preassociative).*
(ii) *For every $g \in Q(F)$, the function $H\colon X^* \to X^*$ defined by $H = g \circ F$ is string-associative (resp. associative).*
(iii) *There is $g \in Q(F)$ such that the function $H\colon X^* \to X^*$ defined by $H = g \circ F$ is string-associative (resp. associative).*

For any $m \in \mathbb{N}$, the same equivalence holds if we add the condition that F has an m-determined range in assertion (i) and the conditions $\mathrm{ran}(g) \subseteq \bigcup_{k=0}^{m} X^k$ and H is m-bounded in assertions (ii) and (iii).

Proof. (i) $\implies$ (ii). Let $g \in Q(F)$ and $H = g \circ F$. We know by Lemma 3.7 that $H = H \circ H$. Since $g|_{\mathrm{ran}(F)}$ is injective, we have that H is string-preassociative (resp. preassociative) by Proposition 3.3. It follows from Proposition 3.4 that H

is string-associative (resp. string-associative and even associative since it satisfies condition (2) by Lemma 3.7(b)).

(ii) $\implies$ (iii). Trivial.

(iii) $\implies$ (i). By Proposition 3.4, H is string-preassociative (resp. preassociative). Since $g|_{\mathrm{ran}(F)}$ is an injective function from $\mathrm{ran}(F)$ onto $\mathrm{ran}(g) = \mathrm{ran}(H)$, we have $F = (g|_{\mathrm{ran}(F)})^{-1} \circ H$ and the function $(g|_{\mathrm{ran}(F)})^{-1}$ is injective from $\mathrm{ran}(H)$ onto $\mathrm{ran}(F)$. It follows from Proposition 3.3 that F is string-preassociative (resp. preassociative).

The last part of the result follows from Lemma 3.7. □

Theorem 3.9. *Assume AC and let $F\colon X^* \to Y$ be a function. The following conditions are equivalent.*

(i) *F is string-preassociative (resp. preassociative).*
(ii) *There exists a string-associative (resp. associative) function $H\colon X^* \to X^*$ and an injective function $f\colon \mathrm{ran}(H) \to Y$ such that $F = f \circ H$.*

Moreover, we have the following.

(a) *If condition (ii) holds, then we have $f = F|_{\mathrm{ran}(H)}$, $f^{-1} \in Q(F)$, and we may choose $H = g \circ F$ for any $g \in Q(F)$.*
(b) *For any $m \in \mathbb{N}$, the equivalence between (i) and (ii) still holds if we add the condition that F has an m-determined range in assertion (i) and the condition that H is m-bounded in assertion (ii). In this case the condition $\mathrm{ran}(g) \subseteq \bigcup_{k=0}^{m} X^k$ must be added in statement (a).*

Proof. (i) $\implies$ (ii). Let $H\colon X^* \to X^*$ be defined by $H = g \circ F$, where $g \in Q(F)$. By Lemma 3.7 we have $F = f \circ H$, where $f = F|_{\mathrm{ran}(H)}$ is injective. By Lemma 3.8, H is string-associative (resp. associative).

(ii) $\implies$ (i). By Proposition 3.4 we have that H is string-preassociative (resp. preassociative). Then also F is string-preassociative (resp. preassociative) by Proposition 3.3.

(a) If condition (ii) holds, then $F \circ H = f \circ H \circ H = f \circ H$ and hence $F|_{\mathrm{ran}(H)} = f|_{\mathrm{ran}(H)} = f$. Moreover, since f is injective we have $H = f^{-1} \circ F$ and hence $F \circ f^{-1} \circ F = F \circ H = f \circ H \circ H = f \circ H = F$, which shows that $f^{-1} \in Q(F)$.

(b) Follows from Proposition 3.6 and Lemmas 3.7 and 3.8. □

Example 3.10. As already observed in [3] and Example 3.2, the function $F\colon X^* \to \mathbb{N}$ defined by $F(\mathbf{x}) = |\mathbf{x}|$ is preassociative. The function $g\colon \mathbb{N} \to X^*$ defined by $g(n) = a^n$ for some fixed $a \in X$ is a quasi-inverse of F. The function $H = g \circ F$, from X^* to X^*, is then defined by $H(\mathbf{x}) = a^{|\mathbf{x}|}$ and the function $f = F|_{\mathrm{ran}(H)}$, from $\mathrm{ran}(H)$ to $\mathbb{N}$, is defined by $f(a^n) = n$. In accordance with Theorem 3.9, we have $F = f \circ H$, where f is injective and H is associative.

Remark 5. (a) The restriction of Theorem 3.9 to functions $F\colon X^* \to Y$ having a 1-determined range and satisfying condition (6) was obtained in [3, Theorem 4.9]. Here we have extended this factorization result to any string-preassociative or preassociative function.

(b) It is noteworthy that, by making an appropriate choice of $g \in Q(F)$ in Lemma 3.7, Lemma 3.8, and Theorem 3.9, the function $H|_{F^{-1}(\mathrm{ran}(F_k))}$ can always be made k-bounded for every $k \in \mathbb{N}$. Indeed, for every function

$F: X^* \to X^*$, define the map $\ell: \mathrm{ran}(F) \to \mathbb{N}$ by
$$\ell(y) = \min\{j \in \mathbb{N} : X^j \cap F^{-1}\{y\} \neq \varnothing\}.$$
We say that a quasi-inverse g of F is *length-optimized* if $g(y) \in X^{\ell(y)}$ for every $y \in \mathrm{ran}(F)$. Under AC we have $\varnothing \neq Q_\ell(F) \subseteq Q(F)$, where $Q_\ell(F)$ denotes the set of length-optimized quasi-inverses of F. Now, under the assumptions of Lemma 3.7, if $g \in Q_\ell(F)$, then for every $k \in \mathbb{N}$ the function $H|_{F^{-1}(\mathrm{ran}(F_k))}$ is k-bounded. Indeed, if $\mathbf{x} \in F^{-1}(\mathrm{ran}(F_k))$, then $k \in \{j \in \mathbb{N} : X^j \cap F^{-1}\{F(\mathbf{x})\} \neq \varnothing\}$ and therefore $|H(\mathbf{x})| = |g(F(\mathbf{x}))| = \ell(F(\mathbf{x})) \leqslant k$.

Combining Proposition 2.8 and Theorem 3.9, we immediately derive the following corollary.

Corollary 3.11. *Assume AC and let $m \in \mathbb{N}$. Any string-preassociative function $F: X^* \to Y$ having an m-determined range is completely determined by its parts of arity at most $m+1$, i.e., if $G: X^* \to Y$ is a string-preassociative function having an m-determined range and such that $G_i = F_i$, for $i = 0, \ldots, m+1$, then $F = G$.*

Remark 6. If $F: X^* \to Y$ is string-preassociative and has an m-determined range for some $m \in \mathbb{N}$, then by combining Eq. (3) with Theorem 3.9 we see that F can be computed recursively from $F_0, \ldots, F_{m+1}$ by
$$F_n(x_1 \cdots x_n) = F((g \circ F_{n-1})(x_1 \cdots x_{n-1})\, x_n), \qquad n \geqslant m+2,$$
where $g \in Q(F)$ satisfies $\mathrm{ran}(g) \subseteq \bigcup_{k=0}^m X^k$.

We now provide necessary and sufficient conditions on the parts $F_0, \ldots, F_{m+1}$ for a function $F: X^* \to Y$ to be string-preassociative and have an m-determined range. The result is stated in Theorem 3.13 below and follows from the next proposition.

Proposition 3.12. *Assume AC and let $m \in \mathbb{N}$. A function $F: X^* \to Y$ is string-preassociative and has an m-determined range if and only if $\mathrm{ran}(F_{m+1}) \subseteq \bigcup_{k=0}^m \mathrm{ran}(F_k)$ and there exists $g \in Q(F)$, with $\mathrm{ran}(g) \subseteq \bigcup_{k=0}^m X^k$, such that*

(a) *$F(H(x\mathbf{y})z) = F(xH(\mathbf{y}z))$ for all $x \in X$, $\mathbf{y} \in X^*$, and $z \in X$ such that $|x\mathbf{y}z| \leqslant m+2$.*

(b) *$F(\mathbf{y}z) = F(H(\mathbf{y})z)$ for all $\mathbf{y} \in X^*$ and all $z \in X$,*

where $H = g \circ F$.

Proof. (Necessity) Let $F: X^* \to Y$ be string-preassociative and have an m-determined range. Then clearly $\mathrm{ran}(F_{m+1}) \subseteq \mathrm{ran}(F) = \bigcup_{k=0}^m \mathrm{ran}(F_k)$. Let $g \in Q(F)$ such that $\mathrm{ran}(g) \subseteq \bigcup_{k=0}^m X^k$ and let $H = g \circ F$. By Lemma 3.8, H is string-associative and m-bounded, and therefore conditions (a)–(b) hold by Proposition 2.10.

(Sufficiency) Let $F: X^* \to Y$ be a function satisfying $\mathrm{ran}(F_{m+1}) \subseteq \bigcup_{k=0}^m \mathrm{ran}(F_k)$ and conditions (a)–(b) for some $g \in Q(F)$ such that $\mathrm{ran}(g) \subseteq \bigcup_{k=0}^m X^k$. Since $H = g \circ F$ is m-bounded, by condition (b) we must have $\mathrm{ran}(F_n) \subseteq \mathrm{ran}(F_{m+1}) \subseteq \bigcup_{k=0}^m \mathrm{ran}(F_k)$ for every $n \geqslant 1$ and hence F has an m-determined range.

Let us show that F is string-preassociative. By Lemma 3.8, it suffices to show that $H = g \circ F$ is string-associative. By Proposition 2.10 it suffices to show that $H \circ H_k = H_k$ or equivalently $g \circ F \circ g \circ F_k = g \circ F_k$ for $k = 0, \ldots, m+1$. This identity clearly holds by definition of g. □

Theorem 3.13. *Assume AC and let $m \in \mathbb{N}$. For $k = 0, \ldots, m+1$, let $F_k: X^k \to Y$ be functions. Then there exists a string-preassociative function $G: X^* \to Y$ having* *an m-determined range and such that $G_k = F_k$ for $k = 0, \ldots, m+1$ if and only if $\mathrm{ran}(F_{m+1}) \subseteq \bigcup_{k=0}^{m} \mathrm{ran}(F_k)$ and there exists $g \in Q(F)$, with $\mathrm{ran}(g) \subseteq \bigcup_{k=0}^{m} X^k$, such that condition (a) of Proposition 3.12 holds, where $H = g \circ F$. Such a function G is then uniquely determined by $G(\mathbf{y}z) = G((g \circ G)(\mathbf{y})\, z)$ for every $\mathbf{y}z \in X^*$.*

We end this section by giving equivalent conditions for a function $F: X^* \to Y$ to have an m-determined range. This result generalizes Proposition 2.4 in [3].

Proposition 3.14. *Assume AC, let $F: X^* \to Y$ be a function, and let $m \in \mathbb{N}$. The following assertions are equivalent.*

(i) *F has an m-determined range.*
(ii) *There exists an m-bounded function $H: X^* \to X^*$ such that $F = F \circ H$.*
(iii) *There exists an m-bounded function $H: X^* \to X^*$, with $H_k = \mathrm{id}|_{X^k}$ for $k = 0, \ldots, m$, and a function $f: X^* \to Y$ such that $F = f \circ H$. In this case, $f_k = F_k$ for $k = 0, \ldots, m$.*
(iv) *There exist functions $H: X^* \to X^*$ and $f: X^* \to Y$ such that $F = f \circ H$ and there exists a partition $\{A_0, \ldots, A_m\}$ of X^* such that $\mathrm{ran}(H|_{A_k}) \subseteq X^k$ and $H|_{A_k} = H_k \circ H|_{A_k}$ for $k = 0, \ldots, m$. In this case, $F|_{A_k} = F_k \circ H|_{A_k}$ for $k = 0, \ldots, m$.*
(v) *There exists a function $H: X^* \to X^*$ having an m-determined range and a function $f: X^* \to Y$ such that $F = f \circ H$.*

Proof. (i) $\Longrightarrow$ (ii) Follows from Lemma 3.7.

(ii) $\Longrightarrow$ (iii) Modifying H_k into $\mathrm{id}|_{X^k}$ for $k = 0, \ldots, m$ and taking $f = F$, we obtain $F = f \circ H$. We then have $F_k = f \circ H_k = f_k$ for $k = 0, \ldots, m$.

(iii) $\Longrightarrow$ (iv) The first part is trivial. We can take, e.g., $A_k = H^{-1}(X^k)$. Also, we have $F_k \circ H|_{A_k} = f \circ H_k \circ H|_{A_k} = f \circ H|_{A_k} = F|_{A_k}$ for $k = 0, \ldots, m$.

(iv) $\Longrightarrow$ (v) If $y \in \mathrm{ran}(H)$, then there exists $k \in \{0, \ldots, m\}$ such that $y \in \mathrm{ran}(H|_{A_k}) \subseteq \mathrm{ran}(H_k)$. Hence H has an m-determined range.

(v) $\Longrightarrow$ (i) Follows from the fact that the property of having an m-determined range is preserved under left composition with unary maps. □

Corollary 3.15. *Let $m \in \mathbb{N}$ and let $F: X^* \to Y$ have an m-determined range. If $F_0, \ldots, F_m$ are injective, then there exists a unique m-bounded function $H: X^* \to X^*$ such that $F = F \circ H$.*

Proof. By Proposition 3.14 there exists an m-bounded function $H: X^* \to X^*$ such that $F = F \circ H$. Also, there exists a partition $\{A_0, \ldots, A_m\}$ of X^* such that $F|_{A_k} = F_k \circ H|_{A_k}$, or equivalently, $H|_{A_k} = F_k^{-1} \circ F|_{A_k}$ for $k = 0, \ldots, m$. Hence H is uniquely determined. □

4. Functions depending only on the length of the input

We now consider the special class of string functions that depend only on the length of the input. Our aim is to characterize (string-) associativity and (string-) preassociativity within this class.

Definition 4.1. We say that a function $F: X^* \to X^*$ is *weakly length-based* if for every $\mathbf{x}, \mathbf{y} \in X^*$ we have $|F(\mathbf{x})| = |F(\mathbf{y})|$ whenever $|\mathbf{x}| = |\mathbf{y}|$. We say that F is *length-based* if for every $\mathbf{x}, \mathbf{y} \in X^*$ we have $F(\mathbf{x}) = F(\mathbf{y})$ whenever $|\mathbf{x}| = |\mathbf{y}|$.

Note that F is length-based if and only if there exists a map $\phi: \mathbb{N} \to X^*$ such that $F = \phi \circ |\cdot|$, i.e., $F(\mathbf{x}) = \phi(|\mathbf{x}|)$ for all $\mathbf{x} \in X^*$.

Example 4.2. Any $*$-ary operation $F\colon X^* \to X$ is weakly length-based. It is easy to see that if ϕ satisfies $|\phi(n)| = n$ for all $n \in \mathbb{N}$, then the function $F\colon X^* \to X^*$ given by $F = \phi \circ |\cdot|$ is associative. For another example, let $\phi\colon \mathbb{N} \to X^*$ be any map satisfying $|\phi(0)| = 0$, $|\phi(1)| = 1$, $|\phi(2k)| = 4$, $|\phi(2k+1)| = 5$, for all integers $k \geqslant 1$. Then $F\colon X^* \to X^*$ given by $F = \phi \circ |\cdot|$ is associative.

Proposition 4.3. *Let $F\colon X^* \to X^*$ be a function.*

(a) *If F is string-associative and weakly length-based, then there is a map $\alpha\colon \mathbb{N} \to \mathbb{N}$ such that $\mathrm{ran}(F_k) \subseteq X^{\alpha(k)}$ for all $k \in \mathbb{N}$ and*

$$\alpha(n+k) \;=\; \alpha(\alpha(n)+k), \qquad \text{for all } n,k \in \mathbb{N}. \tag{7}$$

In this case, F is associative if and only if α satisfies

$$\alpha(n) = 0 \quad \Longleftrightarrow \quad n = 0, \qquad \text{for all } n \in \mathbb{N}. \tag{8}$$

(b) *F is string-associative and length-based if and only if $F = \psi \circ \alpha \circ |\cdot|$ for some $\psi\colon \mathbb{N} \to X^*$ satisfying $|\psi(n)| = n$ for all $n \in \mathbb{N}$ and some $\alpha\colon \mathbb{N} \to \mathbb{N}$ satisfying (7).*

Proof. (a) Since F is weakly length-based, there is a function $\alpha\colon \mathbb{N} \to \mathbb{N}$ such that $\mathrm{ran}(F_k) \subseteq X^{\alpha(k)}$ for all $k \in \mathbb{N}$. By string-associativity, we have $F(\mathbf{xy}) = F(F(\mathbf{x})\mathbf{y})$ for all $\mathbf{x},\mathbf{y} \in X^*$ with $|\mathbf{x}| = n$ and $|\mathbf{y}| = k$. Since $|F(\mathbf{xy})| = \alpha(n+k)$ and $|F(F(\mathbf{x})\mathbf{y})| = \alpha(\alpha(n)+k)$, it follows that $\alpha(n+k) = \alpha(\alpha(n)+k)$ for all $n,k \in \mathbb{N}$.

The last part of the statement follows from the fact that ε is the only zero-length string.

(b) (Necessity) By (a) and since F is length-based, there is a map $\alpha\colon \mathbb{N} \to \mathbb{N}$ satisfying (7) and some $\mathbf{y}_k \in X^{\alpha(k)}$ for every $k \in \mathbb{N}$ such that $F(\mathbf{x}) = \mathbf{y}_k$ for all $k \in \mathbb{N}$ and all $\mathbf{x} \in X^k$.

Together with string-associativity, this implies that if $|F(\mathbf{x})| = |F(\mathbf{y})|$, then

$$F(\mathbf{x}) \;=\; F(F(\mathbf{x})) \;=\; \mathbf{y}_{|F(\mathbf{x})|} \;=\; \mathbf{y}_{|F(\mathbf{y})|} \;=\; F(F(\mathbf{y})) \;=\; F(\mathbf{y}).$$

Therefore, we can decompose F as $F = \psi \circ \alpha \circ |\cdot|$ for some $\psi\colon \mathbb{N} \to X^*$ such that $|\psi(n)| = n$ for all $n \in \mathbb{N}$.

(Sufficiency) The function $F = \psi \circ \alpha \circ |\cdot|$ is clearly length-based. In order to verify string-associativity, let $\mathbf{x},\mathbf{y},\mathbf{z} \in X^*$ with $|\mathbf{x}| = a$, $|\mathbf{y}| = b$, $|\mathbf{z}| = c$. By condition (7) we have

$$F(\mathbf{x}F(\mathbf{y})\mathbf{z}) \;=\; f(\alpha(a+\alpha(b)+c)) \;=\; f(\alpha(a+b+c)) \;=\; F(\mathbf{xyz}).$$

This completes the proof. □

By Proposition 4.3, the problem of characterizing the length-based string-associative functions reduces to the problem of characterizing the functions $\alpha\colon \mathbb{N} \to \mathbb{N}$ satisfying (7). In what follows, we find an explicit description of such functions α (see Proposition 4.7). We first need to establish a few auxiliary results. We begin by reformulating condition (7) in order to simplify the analysis.

Lemma 4.4. *Condition* (7) *is equivalent to*

$$\alpha(\alpha(n)) = \alpha(n) \qquad \text{and} \tag{9}$$

$$\alpha(n) = \alpha(n') \implies \alpha(n+k) = \alpha(n'+k), \qquad \text{for all } n,n',k \in \mathbb{N}. \tag{10}$$

Proof. Condition (9) is a special case of (7) with $k = 0$. Under the assumption that $\alpha(n) = \alpha(n')$, it follows from condition (7) that

$$\alpha(n+k) \;=\; \alpha(\alpha(n)+k) \;=\; \alpha(\alpha(n')+k) \;=\; \alpha(n'+k).$$

Condition (7) follows from (9) and (10) by taking $n' = \alpha(n)$. □

A function $\alpha\colon \mathbb{N} \to \mathbb{N}$ is (n_1, p)-*periodic* if for all $n \geqslant n_1$ it holds that $\alpha(n) = \alpha(n+p)$. It is clear that if α is (n_1, p)-periodic, then it is (n_1', p')-periodic for every $n_1' \geqslant n_1$ and for every multiple p' of p.

The following lemma is folklore. We provide a proof for the sake of self-containedness.

Lemma 4.5. *If the function $\alpha\colon \mathbb{N} \to \mathbb{N}$ is (n_1, p_1)-periodic and (n_2, p_2)-periodic, then α is $(\min(n_1, n_2), \gcd(p_1, p_2))$-periodic.*

Proof. Assume, without loss of generality, that $n_1 \leqslant n_2$. Let $d = \gcd(p_1, p_2)$. We need to show that $\alpha(n) = \alpha(n+d)$ whenever $n \geqslant n_1$.

By Bézout's lemma, there exist integers c_1 and c_2 such that $d = c_1 p_1 + c_2 p_2$. Note that one of c_1 and c_2 is nonnegative and the other is nonpositive. Consider first the case that $c_1 \leqslant 0$ and $c_2 \geqslant 0$. Let $k \in \mathbb{N}$ be a large enough integer such that $(kp_2 + c_1)p_1 \geqslant n_2 - n_1$. Then, for $n \geqslant n_1$, we have

$$\begin{aligned} \alpha(n+d) \;&=\; \alpha(n + c_1 p_1 + c_2 p_2 + k p_1 p_2) \\ &=\; \alpha(n + (kp_2 + c_1)p_1 + c_2 p_2) \;=\; \alpha(n + (kp_2 + c_1)p_1) \;=\; \alpha(n), \end{aligned}$$

where the first equality holds by Bézout's identity and because α is (n_1, p_1)-periodic; the second equality is the result of simple algebraic rearrangement; the third equality holds because $n + (kp_2 + c_1)p_1 \geqslant n_2$ and α is (n_2, p_2)-periodic; and the last equality holds because α is (n_1, p_1)-periodic.

In the case when $c_1 \geqslant 0$ and $c_2 \leqslant 0$ we choose k in such a way that $(kp_1 + c_2)p_2 \geqslant n_2 - n_1$. Then a similar argument shows that if $n \geqslant n_1$ then $\alpha(n+d) = \alpha(n)$ holds also in this case. □

Lemma 4.6. *Assume that $\alpha\colon \mathbb{N} \to \mathbb{N}$ satisfies conditions* (9) *and* (10). *If $\alpha(n) \neq n$, then α is $(n_0, n_0' - n_0)$-periodic, where $n_0 = \min\{n, \alpha(n)\}$ and $n_0' = \max\{n, \alpha(n)\}$.*

Proof. By (9), we have $\alpha(\alpha(n)) = \alpha(n)$; hence $\alpha(n_0) = \alpha(n_0')$. It follows from (10) that for all $k \in \mathbb{N}$,

$$\alpha(n_0 + k + (n_0' - n_0)) \;=\; \alpha(n_0' + k) \;=\; \alpha(n_0 + k).$$ □

We are now in position to describe how the length of the output depends on the length of the input in a length-based string-associative function.

Proposition 4.7. *Let $\alpha\colon \mathbb{N} \to \mathbb{N}$. The following conditions are equivalent.*

(i) *α satisfies conditions* (9) *and* (10).
(ii) *Either α is the identity function on $\mathbb{N}$ or there exist integers $n_1 \geqslant 0$ and $\ell > 0$ such that*
   (a) *$\alpha(n) = n$ whenever $0 \leqslant n < n_1$,*
   (b) *α is (n_1, ℓ)-periodic,*
   (c) *$\alpha(n) \geqslant n$ and $\alpha(n) \equiv n \pmod{\ell}$ whenever $n_1 \leqslant n < n_1 + \ell$.*

In addition, α satisfies condition (8) *if and only if α is the identity function on $\mathbb{N}$ or α satisfies conditions (a)–(c) with $n_1 > 0$.*

Proof. (i) $\implies$ (ii). If α is not the identity function, then the set $D = \{n \in \mathbb{N} : \alpha(n) \neq n\}$ is nonempty. Let $g(D) = \{\alpha(n) : n \in D\}$, let n_1 be the minimum element of $D \cup \alpha(D)$, and let ℓ be the minimum of the set $L = \{|n - \alpha(n)| : n \in D\}$. In view of Lemmas 4.5 and 4.6, α is (n_1, ℓ)-periodic. Moreover, $\alpha(n) = n$ whenever $n < n_1$ and $n_1 > 0$ if $\alpha(0) = 0$.

Let $n \in \{n_1, \ldots, n_1 + \ell - 1\}$. Suppose, on the contrary, that $\alpha(n) < n$. If $\alpha(n) < n_1$ then n_1 would not be the minimum element of $D \cup \alpha(D)$, a contradiction. If $n_1 \leqslant \alpha(n) < n$ then $|n - \alpha(n)| < \ell$, which contradicts the minimality of ℓ in the set L. We conclude that $\alpha(n) \geqslant n$.

Suppose then, on the contrary, that $\alpha(n) \not\equiv n \pmod{\ell}$. Then $\alpha(n) - n = q\ell + r$ for some $q \geqslant 0$ and $0 < r < \ell$. Since α is (n_1, ℓ)-periodic, we have

$$\alpha(n + q\ell) \;=\; \alpha(n) \;=\; n + q\ell + r.$$

By Lemma 4.6, this contradicts again the minimality of ℓ in the set L. We conclude that $\alpha(n) \equiv n \pmod{\ell}$.

Finally, note that if α satisfies condition (8), then necessarily $n_1 > 0$.

(ii) $\implies$ (i). The identity function on $\mathbb{N}$ clearly satisfies conditions (8), (9), and (10). If α satisfies conditions (a)–(c) with $n_1 > 0$, then α also satisfies condition (8). Assume that α is not the identity function.

If $0 \leqslant n \leqslant n_1 - 1$, then $\alpha(n) = n$ by (a); hence $\alpha(\alpha(n)) = \alpha(n)$. If $n \geqslant n_1$, then $n \equiv m \pmod{\ell}$ for some $m \in \{n_1, \ldots, n_1 + \ell - 1\}$. By (b), $\alpha(n) = g(m)$, and by (c), $\alpha(m) \geqslant n_1$ and $\alpha(m) \equiv m \pmod{\ell}$. Consequently, $\alpha(\alpha(n)) = \alpha(\alpha(m)) = \alpha(m) = \alpha(n)$. Thus, α satisfies condition (9).

Assume then that $\alpha(n) = \alpha(n')$. If $\alpha(n) \leqslant n_1 - 1$, then $n = n'$ and $\alpha(n + k) = \alpha(n' + k)$ holds trivially for all $k \in \mathbb{N}$. If $\alpha(n) \geqslant n_1$, then both n and n' are greater than or equal to n_1 and $n \equiv n' \pmod{\ell}$. Consequently, for all $k \in \mathbb{N}$, it holds that $n + k \equiv n' + k \pmod{\ell}$ and $\alpha(n + k) = \alpha(n' + k)$ by (b). □

We now apply Theorem 3.9 to characterize length-based (string-) preassociative functions.

Proposition 4.8. *Assume AC and let $F: X^* \to Y$ be a function. The following conditions are equivalent.*

(i) *F is string-preassociative and length-based.*
(ii) *There exist functions $\mu: \mathbb{N} \to X^*$ and $f: X^* \to Y$ such that $F = f \circ \mu \circ |\cdot|$, where $f|_{\mathrm{ran}(\mu \circ |\cdot|)}$ is injective and the function $\alpha: \mathbb{N} \to \mathbb{N}$ defined by $\alpha(n) = |\mu(n)|$ satisfies condition (ii) of Proposition 4.7.*

Moreover, the equivalence still holds if we replace 'string-preassociative' with 'associative' in (i) and add the condition $\mu(0) = \varepsilon$ in (ii).

Proof. (i) $\implies$ (ii). If F is string-preassociative, then by Theorem 3.9 there is a string-associative function $H: X^* \to X^*$ and a map $f: X^* \to Y$ such that $F = f \circ H$ and $f|_{\mathrm{ran}(H)}$ is injective. If F is length-based, then so is H and, by Propositions 4.3 and 4.7, we have $H = \psi \circ \alpha \circ |\cdot|$ for some function $\alpha: \mathbb{N} \to \mathbb{N}$ satisfying condition (ii) of Proposition 4.7 and some function $\psi: \mathbb{N} \to X^*$ such that $|\psi(n)| = n$ for all $n \in \mathbb{N}$. It suffices to set $\mu = \psi \circ \alpha$ to obtain the desired result.

(ii) $\implies$ (i). The function $F = f \circ \mu \circ |\cdot|$ is clearly length-based. Moreover, according to Propositions 4.3 and 4.7, the function $\mu \circ |\cdot|$ is string-associative. By Theorem 3.9, the function F is string-preassociative.

The last part of the statement is again a consequence of Propositions 4.3 and 4.7. □

Acknowledgments

This work was developed within the FCT Project PEst-OE/MAT/UI0143/2014 of CAUL, FCUL. It is also supported by the internal research project F1R-MTH-PUL-12RDO2 of the University of Luxembourg.

References

[1] M. Couceiro and J.-L. Marichal. Associative polynomial functions over bounded distributive lattices. *Order* 28:1-8, 2011.

[2] J.-L. Marichal. *Aggregation operators for multicriteria decision aid*. PhD thesis, Department of Mathematics, University of Liège, Liège, Belgium, 1998.

[3] J.-L. Marichal and B. Teheux. Associative and preassociative functions. *Semigroup Forum*, in press.

[4] B. Schweizer and A. Sklar. *Probabilistic metric spaces*. North-Holland Series in Probability and Applied Mathematics. North-Holland Publishing Co., New York, 1983. (New edition in: Dover Publications, New York, 2005).

Centro de Álgebra da Universidade de Lisboa, Avenida Professor Gama Pinto 2, 1649-003 Lisboa, Portugal

E-mail address: erkko[at]campus.ul.pt

Mathematics Research Unit, FSTC, University of Luxembourg, 6, rue Coudenhove-Kalergi, L-1359 Luxembourg, Luxembourg

E-mail address: jean-luc.marichal[at]uni.lu

Mathematics Research Unit, FSTC, University of Luxembourg, 6, rue Coudenhove-Kalergi, L-1359 Luxembourg, Luxembourg

E-mail address: bruno.teheux[at]uni.lu