Theoretical Computer Science 410 (2009) 2393–2400

Contents lists available at ScienceDirect

Theoretical Computer Science

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

Twin-roots of words and their properties

Lila Kari, Kalpana Mahalingam [1], Shinnosuke Seki *

Department of Computer Science, The University of Western Ontario, London, Ontario, Canada, N6A 5B7

ARTICLE INFO

Keywords:
f-symmetric words
Twin-roots
Morphic and antimorphic involutions
Primitive roots

ABSTRACT

In this paper we generalize the notion of an ι-symmetric word, from an antimorphic involution, to an arbitrary involution ι as follows: a nonempty word w is said to be ι-symmetric if $w = \alpha\beta = \iota(\beta\alpha)$ for some words α, β. We propose the notion of ι-twin-roots (x, y) of an ι-symmetric word w. We prove the existence and uniqueness of the ι-twin-roots of an ι-symmetric word, and show that the left factor α and right factor β of any factorization of w as $w = \alpha\beta = \iota(\beta\alpha)$, can be expressed in terms of the ι-twin-roots of w. In addition, we show that for any involution ι, the catenation of the ι-twin-roots of w equals the primitive root of w. We also provide several characterizations of the ι-twin-rots of a word, for ι being a morphic or antimorphic involution.

1. Introduction

Periodicity, primitivity, overlaps, and repetitions of factors play an important role in combinatorics of words, and have been the subject of extensive studies, [8,12]. Recently, a new interpretation of these notions has emerged, motivated by information encoding in DNA computing.

DNA computing is based on the idea that data can be encoded as biomolecules, [1], e.g., DNA strands, and molecular biology tools can be used to transform this data to perform, e.g., arithmetic and logic operations. DNA (deoxyribonucleic acid) is a linear chain made up of four different types of nucleotides, each consisting of a base (Adenine, Cytosine, Guanine, or Thymine) and a sugar-phosphate unit. The sugar-phosphate units are linked together by covalent bonds to form the backbone of the DNA single strand. Since nucleotides may differ only by their bases, a DNA strand can be viewed as simply a word over the four-letter alphabet {A, C, G, T}. A DNA single strand has an orientation, with one end known as the 5' end, and the other as the 3' end, based on their chemical properties. By convention, a word over the DNA alphabet represents the corresponding DNA single strand in the 5' to 3' orientation, i.e., the word GGTTTTT stands for the DNA single strand 5'-GGTTTTT-3'. A crucial feature of DNA single strands is their Watson–Crick complementarity: A is complementary to T, G is complementary to C, and two complementary DNA single strands with opposite orientation will bind to each other by hydrogen bonds between their individual bases to form a stable DNA double strand with the backbones at the outside and the bound pairs of bases lying at the inside.

Thus, in the context of DNA computing, a word u encodes the same information as its complement $\theta(u)$, where θ denotes the Watson–Crick complementarity function, or its mathematical formalization as an arbitrary antimorphic involution. This special feature of DNA-encoded information led to new interpretations of the concepts of repetitions and periodicity in words, wherein u and $\theta(u)$ were considered to encode the same information. For example, [4] proposed the notion of θ-primitive words for an antimorphic involution θ: a nonempty word w is θ-primitive iff it cannot be written in the form $w = u_1u_2 \dots u_n$ where $u_i \in \{u, \theta(u)\}$, $n \geq 2$. Initial results concerning this special class of primitive words are promising and include, e.g., an extension, [4], of the Fine-and-Wilf's theorem [5].

* Corresponding author. Tel.: +1 519 661 2111; fax: +1 519 661 3515.
E-mail addresses: lila@csd.uwo.ca (L. Kari), kalpana@csd.uwo.ca, kmahalingam@iitm.ac.in (K. Mahalingam), sseki@csd.uwo.ca (S. Seki).

1 Current address: Department of Mathematics, Indian Institute of Technology, Madras 600042, India.

doi:10.1016/j.tcs.2009.02.032

To return to our motivation, the proof of the extended Fine-and-Wilf's theorem [4], as well as that of an extension of the Lyndon–Schützenberger equation $u^i = v^j w^k$ in [10], to cases involving both words and their Watson–Crick complements, pointed out the importance of investigating overlaps between the square u^2 of a word u, and its complement $\theta(u)$, i.e., overlaps of the form $u^2 = v\theta(u)w$ for some words v, w. This is an analogue of the classical situation wherein u^2 overlaps with u, i.e., $u^2 = vuw$, which happens iff $v = p^i$ and $w = p^j$ for some $i, j \geq 1$, where p is the primitive root of u.

A natural question is thus whether there is any kind of 'root' which characterizes overlaps between u^2 and $\theta(u)$ in the same way in which the primitive root characterizes the overlaps between u^2 and u. For an arbitrary involution ι, this paper proposes as a candidate the notion of *ι-twin-roots* of a word. Unlike the primitive root, the ι-twin-roots are defined only for *ι-symmetric* words. A word u is ι-symmetric if $u = \alpha\beta = \iota(\beta\alpha)$ for some words α, β and the connection with the overlap problem is the following: If ι is an involution and u is an ι-symmetric word, then u^2 overlaps with $\iota(u)$, i.e., $u^2 = \alpha\iota(u)\beta$. The implication becomes equivalence if ι is a morphic or antimorphic involution. In this paper, we prove that an ι-symmetric word u has unique ι-twin-roots (x, y) such that xy is the primitive root of u (i.e., $u = (xy)^n$ for some $n \geq 1$). In addition, if $u = \alpha\beta = \iota(\beta\alpha)$, then $\alpha = (xy)^i x$, $\beta = y(xy)^{n-i-1}$ for some $i \geq 1$ (Proposition 4). Moreover, we provide several characterizations of ι-twin-roots for the case when ι is morphic or antimorphic.

The paper is organized as follows. After basic notations, definitions and examples in Section 2, in Section 3 we investigate relationships between the primitive root and twin-roots of a word. We namely show that for an involution ι, the primitive root of an ι-symmetric word equals the catenation of its ι-twin-roots. Furthermore, for a morphic or antimorphic involution δ, we provide several characteristics of δ-twin-roots of words. In Section 4, we place the set of δ-symmetric words in the Chomsky hierarchy of languages. As an application of these results, in Section 5 we investigate the μ-commutativity between languages, $XY = \mu(Y)X$, for a morphic involution μ.

2. Preliminaries

Let Σ be a finite alphabet. A word over Σ is a finite sequence of symbols in Σ. The empty word is denoted by λ. By Σ^*, we denote the set of all words over Σ, and $\Sigma^+ = \Sigma^* \setminus \{\lambda\}$. For a word $w \in \Sigma^*$, the set of its prefixes, infixes, and suffixes are defined as follows: $\text{Pref}(w) = \{u \in \Sigma^+ \mid \exists v \in \Sigma^*, uv = w\}$, $\text{Inf}(w) = \{u \in \Sigma^+ \mid \exists v, v' \in \Sigma^*, vuv' = w\}$, and $\text{Suff}(w) = \{u \in \Sigma^+ \mid \exists v \in \Sigma^*, vu = w\}$. For other notions in the formal language theory, we refer the reader to [11,12].

A word $u \in \Sigma^+$ is said to be *primitive* if $u = v^i$ implies $i = 1$. By Q we denote the set of all primitive words. For any nonempty word $u \in \Sigma^+$, there is a unique primitive word $p \in Q$, which is called the *primitive root* of u, such that $u = p^n$ for some $n \geq 1$. The primitive root of u is denoted by $\sqrt{u}$.

An *involution* is a mapping f such that f^2 is the identity. A *morphism* (resp. *antimorphism*) f over an alphabet Σ is a mapping such that $f(uv) = f(u)f(v)$ ($f(uv) = f(v)f(u)$) for all words $u, v \in \Sigma^*$. We denote by f, ι, μ, θ, and δ, an arbitrary mapping, an involution, a morphic involution, an antimorphic involution and a d-morphic involution (an involution that is either morphic or antimorphic), respectively. Note that an involution is not always length-preserving but a d-morphic involution is.

A palindrome is a word which is equal to its mirror image. The concept of palindromes was generalized to θ-palindromes, [7,9], where θ is an arbitrary antimorphic involution: a word w is called a *θ-palindrome* if $w = \theta(w)$.

This definition can be generalized as follows: For an arbitrary mapping f on Σ^*, a word $w \in \Sigma^*$ is called a *f-palindrome* if $w = f(w)$. We denote by P_f the set of all f-palindromes over Σ^*. The name f-palindrome serves as a reminder of the fact that, in the particular case when f is the mirror-image function, i.e., the identity function on Σ extended to an antimorphism of Σ^*, an f-palindrome is an ordinary palindrome. An additional reason for this choice of term was the fact that, in biology, the term "palindrome" is routinely used to describe DNA strings u with the property that $\theta(u) = u$, where θ is the Watson–Crick complementarity function. In the case when f is an arbitrary function on Σ^*, what we here call an f-palindrome is simply a fixed point for the function f.

Lemma 1. *Let $u \in \Sigma^+$ and δ be a d-morphic involution. Then $u \in \text{P}_\delta$ if and only if $\sqrt{u} \in \text{P}_\delta$.*

Proof. Note that $\delta(\sqrt{u}^n) = \delta(\sqrt{u})^n$ for a d-morphic involution δ. If $u \in \text{P}_\delta$, then we have $\sqrt{u}^n = \delta(\sqrt{u}^n)$. This means that $\sqrt{u}^n = \delta(\sqrt{u})^n$. Since δ is length-preserving, $\sqrt{u} = \delta(\sqrt{u})$. The opposite direction can be proved in a similar way. □

The θ-symmetric property of a word was introduced in [9] for antimorphic involutions θ. In [9], a word is said to be θ-symmetric if it can be written as a product of two θ-palindromes. We extend this notion to the f-symmetric property, where f is an arbitrary mapping. For a mapping f, a nonempty word $w \in \Sigma^+$ is *f-symmetric* if $w = \alpha\beta = f(\beta\alpha)$ for some $\alpha \in \Sigma^+$ and $\beta \in \Sigma^*$. Our definition is a generalization of the definition in [9]. Indeed, when f is an antimorphic involution, $w = \alpha\beta = f(\beta\alpha) = f(\alpha)f(\beta)$ implies $\alpha, \beta \in \text{P}_f$. For an f-symmetric word w, we call a pair (α, β) such that $w = \alpha\beta = f(\beta\alpha)$ an *f-symmetric factorization* of w. Given an f-symmetric factorization (α, β) of a word, α is called its left factor and β is called its right factor. We denote by S_f the set of all f-symmetric words over Σ^*. We have the following observation on the inclusion relation between P_f and S_f.

Proposition 2. *For a mapping f on Σ^*, $\text{P}_f \subseteq \text{S}_f$.*

3. Twin-roots and primitive roots

Given an involution ι, in this section we define the notion of ι-twin-roots of an ι-symmetric word u with respect to ι. We prove that any ι-symmetric word u has unique ι-twin roots. We show that the right and left factors of any ι-symmetric factorization of u as $u = \alpha\beta = \iota(\beta\alpha)$ can all be expressed in terms of the twin-roots of u with respect to ι. Moreover, we show that the catenation of the twin-roots of an ι-symmetric word u with respect to ι equals the primitive root of u. We also provide several other properties of twin-roots, for the particular case of d-morphic involutions.

We begin by recalling a theorem from [6] on language equation of the type $Xu = vX$, whose corollary will be used for finding the "twin-roots" of an ι-symmetric word.

Corollary 3 ([6]). *Let $u, v, w \in \Sigma^+$. If $uw = wv$, then there uniquely exist two words $x, y \in \Sigma^*$ with $xy \in Q$ such that $u = (xy)^i$, $v = (yx)^i$, and $w = (xy)^j x$ for some $i \geq 1$ and $j \geq 0$.*

Proposition 4. *Let ι be an involution on Σ^* and u be an ι-symmetric word. Then there uniquely exist two words $x, y \in \Sigma^*$ such that $u = (xy)^i$ for some $i \geq 1$ with $xy \in Q$, and if $u = \alpha\beta = \iota(\beta\alpha)$ for some $\alpha, \beta \in \Sigma^*$, then there exists $k \geq 0$ such that $\alpha = (xy)^{i-k-1}x$ and $\beta = y(xy)^k$.*

Proof. Given that u is ι-symmetric and (α, β) is an ι-symmetric factorization of u. It is easy to see that $\beta u = \iota(u)\beta$ holds. Then from Corollary 3, there exist two words $x, y \in \Sigma^*$ such that $xy \in Q$, $u = (xy)^i$, $\iota(u) = (yx)^i$, and $\beta = y(xy)^k$ for some $k \geq 0$. Since $u = \alpha\beta = (xy)^i$, we have $\alpha = (xy)^{i-k-1}x$. Now we have to prove that such (x, y) does not depend on the choice of (α, β). Suppose there were an ι-symmetric factorization (α', β') of u for which $x'y' \in Q$, $u = (x'y')^i$, $\iota(u) = (y'x')^i$, $\alpha' = (x'y')^{i-j-1}x'$, and $\beta' = y'(x'y')^j$ for some $0 \leq j < i$ and $x', y' \in \Sigma^*$ such that $(x, y) \neq (x', y')$. Then we have $xy = x'y'$ and $yx = y'x'$, which contradicts the primitivity of xy. □

The preceding result shows that, if u is ι-symmetric, then its left factor and right factor can be written in terms of a unique pair (x, y). We call (x, y) the *twin-roots of u with respect to ι*, or shortly *ι-twin-roots* of u. We denote the ι-twin-roots of u by $\sqrt[\iota]{u}$. Note that $x \neq y$ and we can assume that x cannot be empty whereas y can. Proposition 4 has the following two consequences.

Corollary 5. *Let ι be an involution on Σ^* and u be an ι-symmetric word. Then the number of ι-symmetric factorizations of u is n for some $n \geq 1$ if and only if $u = (\sqrt{u})^n$.*

Corollary 6. *Let ι be an involution on Σ^* and u be an ι-symmetric word such that $\sqrt[\iota]{u} = (x, y)$. Then the primitive root of u is xy.*

Corollary 6 is the first result that relates the notion of the primitive root of an ι-symmetric word to ι-twin-roots. For the particular case of a d-morphic involution δ, the primitive root and the δ-twin-roots are related more strongly. Firstly, we make a connection between the two elements of δ-twin-roots.

Lemma 7. *Let δ be a d-morphic involution on Σ^*, and u be a δ-symmetric word with δ-twin-roots (x, y). Then $xy = \delta(yx)$.*

Proof. Let $u = (xy)^i = \alpha\beta = \delta(\beta\alpha)$ for some $i \geq 1$ and $\alpha, \beta \in \Sigma^*$. Due to Proposition 4, $\alpha = (xy)^k x$ and $\beta = y(xy)^{i-k-1}$ for some $0 \leq k < i$. Substituting these into $(xy)^i = \delta(\beta\alpha)$ results in $(xy)^i = \delta((yx)^i)$. Since δ is either morphic or antimorphic, we have $xy = \delta(yx)$. □

Proposition 8. *Let δ be a d-morphic involution on Σ^*, and u, v be δ-symmetric words. Then $\sqrt{u} = \sqrt{v}$ if and only if $\sqrt[\delta]{u} = \sqrt[\delta]{v}$.*

Proof. (If) For $\sqrt[\delta]{u} = \sqrt[\delta]{v} = (x, y)$, Corollary 6 implies $\sqrt{u} = \sqrt{v} = xy$. **(Only if)** Let $\sqrt[\delta]{u} = (x, y)$ and $\sqrt[\delta]{v} = (x', y')$. Corollary 6 implies $\sqrt{u} = xy$ and $\sqrt{v} = x'y'$. Let $p = \sqrt{u} = \sqrt{v}$ and we have $p = xy = x'y'$. From Lemma 7, both (x, y) and (x', y') are δ-symmetric factorizations of p. If $(x, y) \neq (x', y')$, due to Corollary 5, $p = (\sqrt{p})^n$ for some $n \geq 2$, a contradiction. □

Proposition 9. *Let δ be a d-morphic involution on Σ^*, and u be a δ-symmetric word such that $\sqrt[\delta]{u} = (x, y)$.*

(1) *If δ is antimorphic, then both x and y are δ-palindromes,*
(2) *If δ is morphic, then either* (i) *x is a δ-palindrome and $y = \lambda$, or* (ii) *x is not a δ-palindrome and $y = \delta(x)$.*

Proof. Due to Lemma 7, we have $xy = \delta(yx)$. If δ is antimorphic, then this means that $xy = \delta(x)\delta(y)$, and hence $x = \delta(x)$ and $y = \delta(y)$. If δ is morphic, then $xy = \delta(y)\delta(x)$. If $y = \lambda$, then we have $x = \delta(x)$. Otherwise, we have three cases depending on the lengths of x and y. If they have the same length, then $y = \delta(x)$. The primitivity of xy forces x not to be a δ-palindrome. If $|x| < |y|$, then $y = y_1y_2$ for some $y_1, y_2 \in \Sigma^+$ such that $\delta(y) = xy_1$ and $y_2 = \delta(x)$. Then $xy = x\delta(x)\delta(y_1) = \delta(y_1)x\delta(x)$, which is a contradiction with $xy \in Q$. The case when $|y| < |x|$ can be proved by symmetry. □

Next we consider the δ-twin-roots of a δ-palindrome; indeed δ-palindromes are δ-symmetric (Proposition 2), and hence have δ-twin-roots. The δ-twin-roots of δ-palindromes have the following property.

Lemma 10. *Let δ be a d-morphic involution and u be a δ-symmetric word such that $\sqrt[\delta]{u} = (x, y)$ for some $x \in \Sigma^+$ and $y \in \Sigma^*$. Then u is a δ-palindrome if and only if x is a δ-palindrome and $y = \lambda$.*

Proof. **(If)** Since $y = \lambda$, $u = x^i$ for some $i \geq 1$. Then $\delta(u) = \delta(x^i) = \delta(x)^i = x^i$, and hence $u \in P_\delta$. **(Only if)** First we consider the case when δ is antimorphic. From Proposition 9, $x, y \in P_\delta$. Suppose $y \neq \lambda$. Since $u \in P_\delta$, Lemma 1 implies $\sqrt{u} \in P_\delta$, and hence $xy = \delta(xy) = \delta(y)\delta(x) = yx$. This means that nonempty words x and y commute, a contradiction with $xy \in Q$. Next we consider the case of δ being morphic. Since u is a δ-palindrome, any letter a from u has the palindrome property, i.e., $\delta(a) = a$. Then all prefixes of u satisfy the palindrome property so that $x = \delta(x)$. Proposition 9 implies either $y = \lambda$ or $y = \delta(x)$, but the latter, with $\sqrt{u} = xy$, leads to $\sqrt{u} = x^2$, a contradiction. □

Note that the notion of ι-symmetry and ι-twin-roots of a word are dependent on the involution ι under consideration. Thus, for example, a word u may be ι_1-symmetric and not ι_2-symmetric, and its twin-roots might be different depending on the involution considered. The following two examples show that there exist words u and morphic involutions μ_1 and μ_2 such that the μ_1-twin-roots of u are different from μ_2-twin-roots of u, and the same situation can be found for the antimorphic case.

Example 11. Let $u = \mathtt{ATTAATTA}$, μ_1 be the identity on Σ extended to a morphism, and μ_2 be the morphic involution such that $\mu_2(\mathtt{A}) = \mathtt{T}$ and $\mu_2(\mathtt{T}) = \mathtt{A}$. Then u is both μ_1-symmetric and μ_2-symmetric. Indeed, $u = \mathtt{ATTA} \cdot \mathtt{ATTA} = \mu_1(\mathtt{ATTA})\mu_1(\mathtt{ATTA})$, and $u = \mathtt{AT} \cdot \mathtt{TAATTA} = \mu_2(\mathtt{TAATTA})\mu_2(\mathtt{AT})$. The μ_1-symmetric property of u implies that $\sqrt[\mu_1]{u} = (\mathtt{ATTA}, \lambda)$, and the μ_2-symmetric property of u implies $\sqrt[\mu_2]{u} = (\mathtt{AT}, \mathtt{TA})$. We can easily check that $\sqrt{u} = \mathtt{ATTA} \cdot \lambda = \mathtt{AT} \cdot \mathtt{TA}$.

Example 12. Let $u = \mathtt{TAAATTTAAATT}$, mi be the identity on Σ extended to an antimorphism, namely the well-known mirror-image mapping, and θ be the antimorphic involution such that $\theta(\mathtt{A}) = \mathtt{T}$ and $\theta(\mathtt{T}) = \mathtt{A}$. We can split u into two palindromes TAAAT and TTAAATT so that u is mi-symmetric. By the same token, u is a product of two θ-palindromes TAAATTTA and AATT, and hence θ-symmetric. We have that $\sqrt[mi]{u} = (\mathtt{TAAAT}, \mathtt{T})$ and $\sqrt[\theta]{u} = (\mathtt{TA}, \mathtt{AATT})$. Note that $\sqrt{u} = \mathtt{TAAAT} \cdot \mathtt{T} = \mathtt{TA} \cdot \mathtt{AATT}$ holds.

The last example shows that it is possible to find a word u, and morphic and antimorphic involutions μ and θ, such that the μ-twin-roots of u and the θ-twin-roots of u are distinct.

Example 13. Let $u = \mathtt{AACGTTGC}$. μ and θ be morphic and antimorphic involutions, respectively, which map A to T, C to G, and vice versa. Then $u = \mu(\mathtt{TTGC})\mu(\mathtt{AACG}) = \theta(\mathtt{AACGTT})\theta(\mathtt{GC})$ so that u is both μ-symmetric and θ-symmetric. We have that $\sqrt[\mu]{u} = (\mathtt{AACG}, \mathtt{TTGC})$ and $\sqrt[\theta]{u} = (\mathtt{AACGTT}, \mathtt{GC})$. Moreover $\sqrt{u} = \mathtt{AACG} \cdot \mathtt{TTGC} = \mathtt{AACGTT} \cdot \mathtt{GC}$.

4. The set of symmetric words in the Chomsky hierarchy

In this section we consider the classification of the language S_μ of the μ-symmetric words with respect to a morphic involution μ, and S_θ of the θ-symmetric words with respect to an antimorphic involution θ, in the Chomsky hierarchy, [2,11]. For a morphic involution μ, we show that P_μ, the set of all μ-palindromes, is regular (Proposition 14). Unless empty, the set $S_\mu \setminus P_\mu$ of all μ-symmetric but non-μ-palindromic words, is not context-free (Proposition 16) but is context-sensitive (Proposition 19). As a corollary of these results we show that, unless empty, the set S_μ of all μ-symmetric words is context-sensitive (Corollary 20), but not context-free (Corollary 17). In contrast, for an antimorphic involution θ, the set of all θ-symmetric words turns out to be context-free (Proposition 21).

Proposition 14. *Let μ be a morphic involution on Σ^*. Then P_μ is regular.*

Proof. For $\Sigma_p = \{a \in \Sigma \mid a = \mu(a)\}$, $P_\mu = \Sigma_p^*$, which is regular. □

Next we consider $S_\mu \setminus P_\mu$. If $c = \mu(c)$ holds for all letters $c \in \Sigma$, then $\Sigma^* = P_\mu$, that is, $S_\mu \setminus P_\mu$ is empty. Therefore, we assume the existence of a character $c \in \Sigma$ satisfying $c \neq \mu(c)$. Under this assumption, we show that $S_\mu \setminus P_\mu$ is not context-free but context-sensitive.

Lemma 15. *Let μ be a morphic involution on Σ^*. If there is $c \in \Sigma$ such that $c \neq \mu(c)$, then $S_\mu \setminus P_\mu$ is infinite.*

Proof. This is clear from the fact that $(c\mu(c))^k \in S_\mu \setminus P_\mu$ for all $k \geq 1$. □

Proposition 16. *Let μ be a morphic involution on Σ^*. If Σ contains a character $c \in \Sigma$ satisfying $c \neq \mu(c)$, then $S_\mu \setminus P_\mu$ is not context-free.*

Proof. Lemma 15 implies that $S_\mu \setminus P_\mu$ is not finite. Suppose $S_\mu \setminus P_\mu$ were context-free. Then there is an integer n given to us by the pumping lemma. Let us choose $z = a^n\mu(a)^n a^n \mu(a)^n$ for some $a \in \Sigma$ satisfying $a \neq \mu(a)$. We may write $z = uvwxy$ subject to the usual constraints (1) $|vwx| \leq n$, (2) $vx \neq \lambda$, and (3) for all $i \geq 0$, $z_i = uv^iwx^iy \in S_\mu \setminus P_\mu$.

Note that for any $w \in S_\mu \setminus P_\mu$ and any $a \in \Sigma$ satisfying $a \neq \mu(a)$, the number of occurrences of a in w should be equal to that of $\mu(a)$ in w. Therefore, if vx contained different numbers of a's and $\mu(a)$'s, $z_0 = uwy$ would not be a member of $S_\mu \setminus P_\mu$. Suppose vwx straddles the first block of a's and the first block of $\mu(a)$'s of z, and vx consists of k a's and k $\mu(a)$'s for some $k > 0$. Note that $2k < n$ because $|vx| \leq |vwx| \leq n$. Then $z_0 = a^{n-k}\mu(a)^{n-k}a^n\mu(a)^n$, and $z_0 \in S_\mu \setminus P_\mu$ means that there exist $\gamma \notin P_\mu$ and an integer $m \geq 1$ such that $z_0 = (\gamma\mu(\gamma))^m$. Thus, $\mu(\gamma) \in \Sigma^*\mu(a)$, i.e., $\gamma \in \Sigma^* a$. This implies that the last block of $\mu(a)$ of z_0 is a suffix of the last $\mu(\gamma)$ of z_0, and hence $|\gamma| = |\mu(\gamma)| \geq n$. As a result, $a^{n-k}\mu(a)^k \in \mathrm{Pref}(\gamma)$, i.e., $\mu(a)^{n-k}a^k \in \mathrm{Pref}(\mu(\gamma))$. Since $a \neq \mu(a)$, we have $\mu(\gamma) = \mu(a)^{n-k}a^k\beta\mu(a)^n$ for some $\beta \in \Sigma^*$.

This implies $|\mu(\gamma)| \geq 2n$. On the other hand, $|z_0| = 4n-2k$, and hence $|\mu(\gamma)| \leq 2n-k$. Now we reached the contradiction. Even if we suppose that vwx straddles the second block of a's and the second block of $\mu(a)$'s of z, we would reach the same contradiction. Finally, suppose that vwx were a substring of the first block of $\mu(a)$'s and the second block of a's of z. Then $z_0 = a^n\mu(a)^{n-k}a^{n-k}\mu(a)^n = (\gamma\mu(\gamma))^m$ for some $m \geq 1$. As proved above, $\mu(a)^n \in \mathrm{Suff}(\mu(\gamma))$, and this is equivalent to $a^n \in \mathrm{Suff}(\gamma)$. Since z_0 contains the n consecutive a's only as the prefix a^n, we have $\gamma = a^n$, i.e., $\mu(\gamma) = \mu(a)^n$. However, the prefix a^n is followed by at most $n-k$ occurrences of $\mu(a)$ and $k \geq 1$. This is a contradiction. Consequently, $\mathrm{S}_\mu \setminus \mathrm{P}_\mu$ is not context-free. □

The proof of Proposition 16 suggests that for an alphabet Σ containing a character c satisfying $c \neq \mu(c)$, S_μ is not context-free either.

Corollary 17. *Let μ be a morphic involution on Σ^*. If Σ contains a character $c \in \Sigma$ satisfying $c \neq \mu(c)$, then S_μ is not context-free.*

Next we prove that $\mathrm{S}_\mu \setminus \mathrm{P}_\mu$ is context-sensitive. We will construct a type-0 grammar and prove that the grammar is indeed a context-sensitive grammar. For this purpose, the workspace theorem is employed, which requires a few terminologies: Let $G = (N, T, S, P)$ be a grammar and consider a derivation D according to G like $D : S = w_0 \Rightarrow w_1 \Rightarrow \cdots \Rightarrow w_n = w$. The workspace of w by D is defined as $WS_G(w, D) = \max\{|w_i| \mid 0 \leq i \leq n\}$. The workspace of w is defined as $WS_G(w) = \min\{WS_G(w, D) \mid D \text{ is a derivation of } w\}$.

Theorem 18 (*Workspace Theorem [11]*). *Let G be a type-0 grammar. If there is a nonnegative integer k such that $WS_G(w) \leq k|w|$ for all nonempty words $w \in L(G)$, then $L(G)$ is context-sensitive.*

Proposition 19. *Let μ be a morphic involution on Σ^*. If Σ contains a character $c \in \Sigma$ satisfying $c \neq \mu(c)$, then $\mathrm{S}_\mu \setminus \mathrm{P}_\mu$ is context-sensitive.*

Proof. We provide a type-0 grammar which generates a language equivalent to $\mathrm{S}_\mu \setminus \mathrm{P}_\mu$. Let $G = (N, \Sigma, P, S)$, where $N = \{S, \hat{Z}, \overleftarrow{Z}, \hat{X}_i, \hat{X}_m, Y, \overleftarrow{L}, \#\} \cup \bigcup_{a\in\Sigma}\{\overrightarrow{X_a}, \overrightarrow{C_a}\}$, the set of nonterminal symbols, and P is the set of production rules given below. First off, this grammar creates $\alpha\mu(\alpha)$ for $\alpha \in \Sigma^*$ that contains a character $c \in \Sigma$ satisfying $c \neq \mu(c)$. The 1–7th rules of the following list of P achieve this task. Secondly, 5th and 10–18th rules copy $\alpha\mu(\alpha)$ at arbitrary times so that the resulting word is $(\alpha\mu(\alpha))^i$ for some $i \geq 0$.

1.	S	$\rightarrow$	$\#\hat{Z}a\hat{X}_i\overrightarrow{X_a}Y\#$	$\forall a \in \Sigma$,
2.	S	$\rightarrow$	$\#\hat{Z}b\hat{X}_m\overrightarrow{X_b}Y\#$	$\forall b \in \Sigma$ such that $b \neq \mu(b)$,
3.	$\overrightarrow{X_a}c$	$\rightarrow$	$c\overrightarrow{X_a}$	$\forall a, c \in \Sigma$,
4.	$\overrightarrow{X_a}Y$	$\rightarrow$	$\overleftarrow{L}\mu(a)Y$	$\forall a \in \Sigma$,
5.	$c\overleftarrow{L}$	$\rightarrow$	$\overleftarrow{L}c$	$\forall c \in \Sigma$,
6.	$\hat{X}_i\overleftarrow{L}$	$\rightarrow$	$a\hat{X}_i\overrightarrow{X_a}$	$\forall a \in \Sigma$,
7.	$\hat{X}_i\overleftarrow{L}$	$\rightarrow$	$b\hat{X}_m\overrightarrow{X_b}$	$\forall b \in \Sigma$ such that $b \neq \mu(b)$,
8.	$\hat{X}_m\overleftarrow{L}$	$\rightarrow$	$a\hat{X}_m\overrightarrow{X_a}$	$\forall a \in \Sigma$,
9.	$\hat{X}_m\overleftarrow{L}$	$\rightarrow$	$\overleftarrow{L}$	
10.	$\hat{Z}a\overleftarrow{L}$	$\rightarrow$	$a\hat{Z}\overrightarrow{C_a}$	$\forall a \in \Sigma$,
11.	$\overrightarrow{C_a}c$	$\rightarrow$	$c\overrightarrow{C_a}$	$\forall a, c \in \Sigma$,
12.	$\overrightarrow{C_a}Y$	$\rightarrow$	$Y\overrightarrow{C_a}$	$\forall a \in \Sigma$,
13.	$\overrightarrow{C_a}\#$	$\rightarrow$	$\overleftarrow{L}a\#$	$\forall a \in \Sigma$,
14.	$Y\overleftarrow{L}$	$\rightarrow$	$\overleftarrow{L}Y$,	
15.	$\hat{Z}Y\overleftarrow{L}$	$\rightarrow$	$\overleftarrow{Z}\,\overleftarrow{L}Y$	
16.	$\hat{Z}Y\overleftarrow{L}$	$\rightarrow$	λ	
17.	$c\overleftarrow{Z}$	$\rightarrow$	$\overleftarrow{Z}c$	$\forall c \in \Sigma$,
18.	$\#\overleftarrow{Z}$	$\rightarrow$	$\#\hat{Z}$,	
19.	$\#$	$\rightarrow$	λ.	

This grammar works in the following manner. After the 1st or 6th rule generates a terminal symbol $a \in \Sigma$, the 3rd and 4th rules deliver information of the symbol to Y and generate $\mu(a)$ just before Y, and by the 5th rule, the header $\overleftarrow{L}$ go back to $\hat{X}_i$. This process is repeated until a character $b \in \Sigma$ satisfying $b \neq \mu(b)$ is generated, which is followed by changing $\hat{X}_i$ to $\hat{X}_m$ and generating $\mu(b)$ just before Y. Now the grammar may continue the a-$\theta(a)$ generating process or shift to a copy phase (9th rule $\hat{X}_m\overleftarrow{L} \rightarrow \overleftarrow{L}$). From now on, whenever the a-$\mu(a)$ process ends, the grammar can do this choice. Just after using the 9th rule $\hat{X}_m\overleftarrow{L} \rightarrow \overleftarrow{L}$, the sentential form of this derivation is $\hat{Z}\alpha\overleftarrow{L}\mu(\alpha)Y$ for some $\alpha \in \Sigma^+$ which contains at least one character $b \in \Sigma$ satisfying $b \neq \mu(b)$. The 5th and 10–18th rules copy $\alpha\mu(\alpha)$ at the end of sentential form. Just after coping $\alpha\mu(\alpha)$, the sentential form $\alpha\mu(\alpha)\hat{Z}Y\overleftarrow{L}(\alpha\mu(\alpha))^m$ appears so that if the 15th rule is applied, then another

$\alpha\mu(\alpha)$ is copied; otherwise the derivation terminates. Therefore, a word w derived by this grammar G can be represented as $(\alpha\mu(\alpha))^n$ for some $n \geq 1$, and hence $w \in \mathrm{S}_\mu$. In addition, G generates only non-θ-palindromic word so that $w \in \mathrm{S}_\mu \setminus \mathrm{P}_\mu$. Thus, $L(G) \subseteq \mathrm{S}_\mu \setminus \mathrm{P}_\mu$. Conversely, if $w \in \mathrm{S}_\mu \setminus \mathrm{P}_\mu$, then it has the μ-twin-roots $\sqrt[\mu]{w} = (x, y)$ and $w = (xy)^n$ for some $n \geq 1$. Since $y = \mu(x)$, w can be generated by G. Therefore, $\mathrm{S}_\mu \setminus \mathrm{P}_\mu \subseteq L(G)$. Consequently, $L(G) = \mathrm{S}_\mu \setminus \mathrm{P}_\mu$. Furthermore, this grammar satisfies the workspace theorem (Theorem 18). Any sentential form to derive a word cannot be longer than $|w| + c$ for some constant $c \geq 0$. Therefore, $L(G)$ is context-sensitive. □

Corollary 20. *Let μ be a morphic involution on Σ^*. If Σ contains a character $c \in \Sigma$ satisfying $c \neq \mu(c)$, then S_μ is context-sensitive.*

Finally we show that the set of all θ-symmetric words for an antimorphic involution θ is context-free.

Proposition 21. *For an antimorphic involution θ, S_θ is context-free.*

Proof. It is known that P_θ is context-free and the family of context-free languages is closed under catenation. Since $\mathrm{S}_\theta = \mathrm{P}_\theta \cdot \mathrm{P}_\theta$, S_θ is context-free. □

5. On the pseudo-commutativity of languages

We conclude this paper with an application of the results obtained in Section 3 to the μ-commutativity of languages for a morphic involution μ. For two languages $X, Y \subseteq \Sigma^*$, X is said to *μ-commute with Y* if $XY = \mu(Y)X$ holds.

Example 22. Let $\Sigma = \{a, b\}$ and μ be a morphic involution such that $\mu(a) = b$ and $\mu(b) = a$. For $X = \{ab(baab)^i \mid i \geq 0\}$ and $Y = \{(baab)^j \mid j \geq 1\}$, $XY = \mu(Y)X$ holds.

In this section we investigate languages X which μ-commute with a set Y of μ-symmetric words. When analyzing such pseudo-commutativity equations, the first step is to investigate equations wherein the set of the shortest words in X μ-commutes with the set of the shortest words of Y. (In [3], the author used this strategy to find a solution to the classical commutativity of formal power series, result known as Cohn's theorem.) For $n \geq 0$, by X_n we denote the set of all words in X of length n, i.e., $X_n = \{w \in X \mid |w| = n\}$. Let m and n be the lengths of the shortest words in X and Y, respectively. Then $XY = \mu(Y)X$ implies $X_mY_n = \mu(Y_n)X_m$. The main contribution of this section is to use results from Section 3 to prove that X cannot contain any word shorter than the shortest left factor of all μ-twin-roots of words in Y_n (Proposition 28). Its proof requires several results, e.g., Lemmata 25–27.

Lemma 23 ([12]). *Let $u, v \in \Sigma^+$ and $X \subseteq \Sigma^*$. If X is not empty and $Xu = vX$ holds, then $|X_n| \leq 1$ for all $n \in \mathbb{N}_0$.*

Lemma 24. *Let $u, v \in \Sigma^+$ and $X \subseteq \Sigma^*$. If X is not empty and $uX = \mu(X)v$ holds, then $|X_n| \leq 1$ for all $n \in \mathbb{N}_0$.*

Let $X \subseteq \Sigma^*$, $Y \subseteq \mathrm{S}_\mu \setminus \mathrm{P}_\mu$ such that $XY = \mu(Y)X$, and n be the length of the shortest words in Y. For $n \geq 1$, let $Y_{n,\ell} = \{y \in Y_n \mid \sqrt[\mu]{y} = (x, \mu(x)), |x| = \ell\}$. Informally speaking, $Y_{n,\ell}$ is a set of words in Y of length n having the μ-twin-roots whose left factor is of length ℓ.

Lemma 25. *Let $Y \subseteq \mathrm{S}_\mu \setminus \mathrm{P}_\mu$, $y_1, y_2 \in Y_{n,\ell}$ for some $n, \ell \geq 1$, and $u, w \in \Sigma^*$. If $uy_1 = \mu(y_2)w$ and $|u|, |w| \leq \ell$, then $u = w$.*

Proof. Since $|y_1| = |y_2| = n$, we have $|u| = |w|$. Let $y_1 = (x_1\mu(x_1))^{n/2\ell}$ and $y_2 = (x_2\mu(x_2))^{n/2\ell}$, where $\sqrt[\mu]{y_1} = (x_1, \mu(x_1))$ and $\sqrt[\mu]{y_2} = (x_2, \mu(x_2))$ for some $x_1, x_2 \in \Sigma^+$. Now we have $u(x_1\mu(x_1))^{n/2\ell} = \mu(x_2\mu(x_2))^{n/2\ell}w$. This equation, with $|u| \leq \ell$, implies that $ux_1\mu(x_1) = \mu(x_2\mu(x_2))w$. Then we have $\mu(x_2) = u\alpha$ for some $\alpha \in \Sigma^*$, and $ux_1\mu(x_1) = u\alpha\mu(u)\mu(\alpha)w$. This means $x_1 = \alpha\mu(u)$ and $\mu(x_1) = \mu(\alpha)w$, which conclude $u = w$. □

Lemma 26. *Let $X \subseteq \Sigma^*$, and $Y \subseteq \mathrm{S}_\mu \setminus \mathrm{P}_\mu$ such that $XY = \mu(Y)X$. For integers $m, n \geq 1$ such that $X_mY_n = \mu(Y_n)X_m$ and $m \leq \min\{\ell \mid Y_{n,\ell} \neq \emptyset\}$, we have $X_mY_{n,\ell} = \mu(Y_{n,\ell})X_m$ for all $\ell \geq 1$.*

Proof. Let $y_1 \in Y_n$ such that $y_1 = (x_1\mu(x_1))^i$ for some $i \geq 1$, where $\sqrt[\mu]{y_1} = (x_1, \mu(x_1))$. Since $X_mY_n = \mu(Y_n)X_m$ holds, there exist $u, v \in X_m$ and $y_2 \in Y_n$ satisfying $uy_1 = \mu(y_2)v$. When $y_2 = (x_2\mu(x_2))^j$ for some $j \geq 1$, where $\sqrt[\mu]{y_2} = (x_2, \mu(x_2))$, we will show that $i = j$.

Suppose $i \neq j$. We only have to consider the case where i and j are relatively prime. The symmetry makes it possible to assume $i < j$, and we consider three cases: (1) $i = 1$ and j is even; (2) $i = 1$ and j is odd; and (3) $i, j \geq 2$. Firstly, we consider the case (1), where we have $ux_1\mu(x_1) = (\mu(x_2)x_2)^jv$. Since $|u| \leq |x_1|, |x_2|$, we can let $ux_1 = (\mu(x_2)x_2)^{j/2}\alpha$ and $\alpha\mu(x_1) = (\mu(x_2)x_2)^{j/2}v$ for some $\alpha \in \Sigma^*$. Note that $|\alpha| = |u| = |v|$ because $|x_1\mu(x_1)| = |(\mu(x_2)x_2)^j|$. Since $|u| \leq |x_2|$, let $\mu(x_2) = u\beta$ for some $\beta \in \Sigma^*$. Then the former of preceding equations implies $x_1 = \beta x_2(\mu(x_2)x_2)^{j/2-1}\alpha$. Substituting these into the latter equation gives $\alpha\mu(\beta)\mu(x_2)(x_2\mu(x_2))^{j/2-1}\mu(\alpha) = u\beta x_2(\mu(x_2)x_2)^{j/2-1}v$. This provides us with $x_2 = \mu(x_2)$, which contradicts $x_2 \notin \mathrm{P}_\mu$. Case (2) is that $i = 1$ and j is odd. In a similar way as the preceding case, let $ux_1 = (\mu(x_2)x_2)^{(j-1)/2}\mu(x_2)\alpha$ and $\alpha\mu(x_1) = x_2(\mu(x_2)x_2)^{(j-1)/2}v$ for some $\alpha \in \Sigma^*$. Since $|u| \leq |x_2|$, the first equation implies that $\mu(x_2) = u\beta$ for some $\beta \in \Sigma^*$. Then substituting this into the second equation results in $\alpha = \mu(u)$. By the same token, we have $\alpha = \mu(v)$, and hence $u = v$. Therefore, $ux_1\mu(x_1) = (\mu(x_2)x_2)^ju = u\beta\mu(u)\mu(\beta)(u\beta\mu(u)\mu(\beta))^{j-1}u = u(\beta\mu(u)\mu(\beta)u)^j$. Thus, $x_1\mu(x_1) = (\beta\mu(u)\mu(\beta)u)^j$, which contradicts the primitivity of $x_1\mu(x_1)$ because the assumption that j is odd and $i < j$ implies $j \geq 3$.

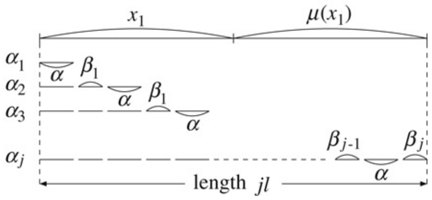

Fig. 1. It is not always the case that $|\alpha_1| < |\alpha_2| < \cdots < |\alpha_j|$. However, we can say that for any k_1, k_2, if $k_1 \neq k_2$, then $|\alpha_{k_1}| \neq |\alpha_{k_2}|$.

What remains now is the case (3) where $i, j \geq 2$ are relatively prime. Since $n = i \cdot |x_1\mu(x_1)| = j \cdot |x_2\mu(x_2)|$, the relative primeness between i and j means that $|x_1\mu(x_1)| = j\ell$ and $|x_2\mu(x_2)| = i\ell$ for some $\ell \geq 1$. For all $1 \leq k \leq j$, $u(x_1\mu(x_1))^{i_k}\alpha_k = \mu(x_2\mu(x_2))^k$ for some $0 \leq i_k \leq i$ and $\alpha_k \in \mathrm{Pref}(x_1\mu(x_1))$. We claim that for some ℓ' satisfying $0 \leq \ell' < \ell$, there exists a 1-to-1 correspondence between $\{|\alpha_1|, \ldots, |\alpha_j|\}$ and $\{0 + \ell', \ell + \ell', 2\ell + \ell', \ldots, (j-1)\ell + \ell'\}$. Indeed, $u(x_1\mu(x_1))^{i_k}\alpha_k = \mu(x_2\mu(x_2))^k$ implies $|u| + i_k j\ell + |\alpha_k| = k|x_2\mu(x_2)|$. Then, $|\alpha_k| = k|x_2\mu(x_2)| - i_k j\ell - |u| = (ik - i_k j)\ell - |u|$. Thus, $|\alpha_k| = -|u| \pmod{\ell}$. We can easily check that if there exist $1 \leq k_1, k_2 \leq j$ satisfying $ik_1 - i_{k_1}j = ik_2 - i_{k_2}j$, then $k_1 = k_2 \pmod{j}$ because i and j are relatively prime. As a result, $\cup_{k=1}^{k=j}\{ik - i_k j \pmod{j}\} = \{0, 1, \ldots, j-1\}$. By letting $\ell' = -|u| \pmod{\ell}$, the existence of the 1-to-1 correspondence has been proved.

Since $\ell' < \ell$ and $i\ell = |x_2\mu(x_2)|$, let $\mu(x_2\mu(x_2)) = \beta w \alpha$ for some $\beta, w, \alpha \in \Sigma^*$ such that $|\beta| = \ell - \ell'$, $|w| = (i-1)\ell$, and $|\alpha| = \ell'$. Then $u(x_1\mu(x_1))^{i_k}\alpha_k = \mu(x_2\mu(x_2))^k$ implies that for all k, $\alpha \in \mathrm{Suff}(\alpha_k)$. Recall that for all k, $\alpha_k \in \mathrm{Pref}(x_1\mu(x_1))$. Then, with the 1-to-1 correspondence, we can say that α appears on $x_1\mu(x_1)$ at even intervals. Let $x_1\mu(x_1) = \alpha\beta_1\alpha\beta_2\cdots\alpha\beta_j$ (see Fig. 1), where $|\beta_1| = \cdots = |\beta_j| = |\beta|$. We get $(x_1\mu(x_1))^{i_{k+1}-i_k}\alpha_{k+1} = \alpha_k\mu(x_2\mu(x_2)) = \alpha_k\beta w\alpha$ for any $1 \leq k \leq j-1$ by substituting $\mu(x_2\mu(x_2))^k = u(x_1\mu(x_1))^{i_k}\alpha_k$ into $\mu(x_2\mu(x_2))^{k+1} = u(x_1\mu(x_1))^{i_{k+1}}\alpha_{k+1}$. Note that $i_{k+1} \geq i_k$; otherwise, we would have $(x_1\mu(x_1))^{i_k - i_{k+1}}\alpha_k\mu(x_2\mu(x_2)) = \alpha_{k+1}$, which is a contradiction with the fact that $|x_1\mu(x_1)| \geq |\alpha_{k+1}|$. Since $|\alpha_k\beta| \leq |x_1\mu(x_1)|$, $\alpha_k\beta \in \mathrm{Pref}(x_1\mu(x_1))$. Even if $i_{k+1} - i_k = 0$, $\alpha_k\beta \in \mathrm{Pref}(\alpha_{k+1}) \subseteq \mathrm{Pref}(x_1\mu(x_1))$. Thus, there exists an integer $1 \leq j' \leq j$ such that $\beta_1 = \cdots = \beta_{j'-1} = \beta_{j'+1} = \cdots = \beta_j = \beta$, that is, $x_1\mu(x_1) = (\alpha\beta)^{j'-1}\alpha\beta_{j'}(\alpha\beta)^{j-j'}$. If $j' < j$, then there exist k_1, k_2 such that $\alpha_{k_1} = (\alpha\beta)^{j'-1}\alpha\beta_{j'}\alpha$ and $\alpha_{k_2} = \alpha(\beta\alpha)^k$ for some $k \geq 1$. Clearly, $|\alpha_{k_1}|, |\alpha_{k_2}| \geq \ell$. By the original definitions of α_{k_1} and α_{k_2}, they must share the suffix of length ℓ. Hence, $\beta_{j'} = \beta$. If $j' = j$, then we claim that for all $1 \leq k < j$ and some $w \in \Sigma^{\leq 2\ell}$, $\alpha_k w \in \mathrm{Pref}(x_1\mu(x_1))$ implies $w \in \mathrm{Pref}(\mu(x_2\mu(x_2)))$. Indeed, as above we have $(x_1\mu(x_1))^{i_{k+1}-i_k}\alpha_{k+1} = \alpha_k\mu(x_2\mu(x_2))$. If $i_{k+1} - i_k \geq 1$, then this means that $\alpha_k w \in \mathrm{Pref}(\alpha_k\mu(x_2\mu(x_2)))$, and hence $w \in \mathrm{Pref}(\mu(x_2\mu(x_2)))$; otherwise, $\alpha_{k+1} = \alpha_k\mu(x_2\mu(x_2))$. Since $\alpha_{k+1} \in \mathrm{Pref}(x_1\mu(x_1))$ and $x_2\mu(x_2) \geq 2\ell$, $\alpha_k w \in \mathrm{Pref}(\alpha_{k+1})$, and hence $w \in \mathrm{Pref}(\mu(x_2\mu(x_2)))$. Let $\alpha_{k_1} = (\alpha\beta)^{j-3}\alpha$ and $\alpha_{k_2} = (\alpha\beta)^{j-2}\alpha$. Then $\alpha_{k_1}\beta\alpha\beta\alpha \in \mathrm{Pref}(x_1\mu(x_1))$ implies $\beta\alpha\beta\alpha \in \mathrm{Pref}(\mu(x_2\mu(x_2)))$. By the same token, $\alpha_{k_2}\beta\alpha\beta_j = x_1\mu(x_1)$ implies $\beta\alpha\beta_j \in \mathrm{Pref}(\mu(x_2\mu(x_2)))$. Thus, $\beta_j = \beta$. Consequently, $x_1\mu(x_1) = (\alpha\beta)^j$. Since $j \geq 3$, this contradicts the primitivity of $x_1\mu(x_1)$. □

Lemma 27. *Let $X \subseteq \Sigma^*$, and $Y \subseteq \mathrm{S}_\mu \setminus \mathrm{P}_\mu$ such that $XY = \mu(Y)X$. If there exist $m, n \geq 1$ such that $X_mY_n = \mu(Y_n)X_m$, and $m \leq \min\{\ell \mid Y_{n,\ell} \neq \emptyset\}$, then $|Y_{n,\ell}| \leq 1$ holds for all $\ell \geq 1$.*

Proof. Lemma 26 implies that $X_mY_{n,\ell} = \mu(Y_{n,\ell})X_m$ for all $\ell \geq 1$. Let us consider this equation for some ℓ such that $Y_{n,\ell} \neq \emptyset$. Then for $y_1 \in Y_{n,\ell}$, there must exist $u, w \in X_m$ and $y_2 \in Y_{n,\ell}$ satisfying $uy_1 = \mu(y_2)w$. Lemma 25 enables us to say $u = w$ because $m \leq \ell$. Thus, $X_mY_{n,\ell} = \mu(Y_{n,\ell})X_m$ is equivalent to $\forall u \in X_m$, $uY_{n,\ell} = \mu(Y_{n,\ell})u$. For the latter equation, Lemma 24 and the assumption $|Y_{n,\ell}| \geq 1$ make it possible to conclude $|Y_{n,\ell}| = 1$. □

Having proved the required lemmata, now we will prove the main results.

Proposition 28. *Let $X \subseteq \Sigma^*$, and $Y \subseteq \mathrm{S}_\mu \setminus \mathrm{P}_\mu$ such that $XY = \mu(Y)X$. Let n be the length of the shortest words in Y. Then X does not contain any nonempty word which is strictly shorter than the shortest left factor of μ-twin-roots of an element of Y_n.*

Proof. If there were such an element of X, the shortest words of X are shorter than any left factor of μ-twin-roots of words in Y. Let u be one of the shortest nonempty words in X, and let $|u| = m$ for some $m \geq 1$. Then $XY = \mu(Y)X$ implies $X_mY_n = \mu(Y_n)X_m$. Moreover, Lemma 26 implies that $X_mY_n = \mu(Y_n)X_m$ if and only if $X_mY_{n,\ell} = \mu(Y_{n,\ell})X_m$ for all $\ell \geq 1$. Then, Lemma 27 implies $|Y_{n,\ell}| \leq 1$ for all $\ell \geq 1$. Let us consider the minimum ℓ satisfying $|Y_{n,\ell}| = 1$. Such an ℓ certainly exists because $Y_n \neq \emptyset$. Let $Y_{n,\ell} = \{y\}$, where $y = (x\mu(x))^i$ for some $i \geq 1$ and $\sqrt[\mu]{y} = (x, \mu(x))$. Then, $uy = \mu(y)u$ means $u(x\mu(x))^i = \mu((x\mu(x))^i)u$. Moreover, the condition $|u| < |x|$ results in $ux\mu(x) = \mu(x)xu$. Letting $\mu(x) = u\alpha$ for some $\alpha \in \Sigma^+$, we have $ux\mu(x) = u\alpha\mu(u)\mu(\alpha)u$, which means $x\mu(x) = \alpha \cdot \mu(u)\mu(\alpha)u = \mu(u)\mu(\alpha)u \cdot \alpha$. Since $\alpha, u \in \Sigma^+$, this is a contradiction with the primitivity of $x\mu(x)$. □

Corollary 29. *Let $X \subseteq \Sigma^*$, and $Y \in \mathrm{S}_\mu \setminus \mathrm{P}_\mu$ such that $XY = \mu(Y)X$, and m, n be the lengths of the shortest words in X and in Y, respectively. If $m = \min\{\ell \mid Y_{n,\ell} \neq \emptyset\}$, then both X_m and Y_n are singletons.*

Proof. It is obvious that $X_mY_n = \mu(Y_n)X_m$ holds. Lemma 26 implies that $X_mY_{n,\ell} = \mu(Y_{n,\ell})X_m$ for all $\ell \geq 1$. Moreover Lemma 27 implies that for all ℓ, $|Y_{n,\ell}| \leq 1$. If there exists $\ell' > m$ such that $|Y_{n,\ell'}| = 1$, then $X_mY_{n,\ell'} = \mu(Y_{n,\ell'})X_m$ must hold. This contradicts Proposition 28, where X_m and $Y_{n,\ell'}$ correspond to X and Y in the proposition, respectively. Now we know that Y_n is singleton. Then Lemma 23 means that X_m is singleton. □

Proposition 30. *Let $X \subseteq \Sigma^*$ and $Y \subseteq \mathrm{S}_\mu \setminus \mathrm{P}_\mu$ such that $XY = \mu(Y)X$. Let m and n be the lengths of the shortest words in X and Y, respectively. If $m = \min\{\ell \mid Y_{n,\ell} \neq \emptyset\}$, then a language which commutes with Y cannot contain any nonempty word which is strictly shorter than any primitive root of a word in Y_n.*

Proof. Corollary 29 implies that Y_n is a singleton. Let $Y_n = \{w\}$, and let $w = (x\mu(x))^i$ for some $i \geq 1$, where $\sqrt[\mu]{w} = (x, \mu(x))$. Then from Corollary 6, we have $\sqrt{w} = x\mu(x)$. Let Z be a language which commutes with Y. Suppose the shortest word in Z, say v, is strictly shorter than $\sqrt{w}$. Let $|v| = \ell'$. Then $Z_{\ell'}Y_n = Y_nZ_{\ell'}$, i.e., $Z_{\ell'}w = wZ_{\ell'}$. Lemma 23 results in $|Z_{\ell'}| = 1$. Let $Z_{\ell'} = \{v\}$. Now we have $vw = wv$. This implies that $\sqrt{v} = \sqrt{w}$, which contradicts the fact that $|v| < |\sqrt{w}|$ and $v \neq \lambda$. □

6. Conclusion

This paper generalizes the notion of f-symmetric words to an arbitrary mapping f. For an involution ι, we propose the notion of the ι-twin-roots of an ι-symmetric word, show their uniqueness, and the fact that the catenation of the ι-twin-roots of a word equals its primitive root. Moreover, for a morphic or antimorphic involution δ, we prove several additional properties of twin-roots. We use these results to make steps toward solving pseudo-commutativity equations on languages.

Acknowledgements

This research was supported by The Natural Sciences and Engineering Council of Canada Discovery Grant and Canada Research Chair Award to L.K.

References

[1] L. Adleman, Molecular computation of solutions to combinatorial problems, Science 266 (1994) 1021–1024.
[2] N. Chomsky, M.P. Schützenberger, The algebraic theory of context-free languages, in: P. Bradford, D. Hirschberg (Eds.), Computer Programming and Formal Languages, North Holland, Amsterdam, 1963, pp. 118–161.
[3] P.M. Cohn, Factorization in noncommuting power series rings, Proceedings of the Cambridge Philosophical Society 58 (1962) 452–464.
[4] E. Czeizler, L. Kari, S. Seki, On a special class of primitive words, in: Proc. Mathematical Foundations of Computer Science (MFCS 2008), in: LNCS, vol. 5162, Springer, Torun, Poland, 2008, pp. 265–277.
[5] N.J. Fine, H.S. Wilf, Uniqueness theorem for periodic functions, Proceedings of American Mathematical Society 16 (1965) 109–114.
[6] C.C. Huang, S.S. Yu, Solutions to the language equation $LB = AL$, Soochow Journal of Mathematics 29 (2) (2003) 201–213.
[7] L. Kari, K. Mahalingam, Watson–Crick conjugate and commutative words, in: M. Garzon, H. Yan (Eds.), DNA 13, in: LNCS, vol. 4848, 2008, pp. 273–283.
[8] M. Lothaire, Combinatorics on Words, Cambridge University Press, 1983.
[9] A.D. Luca, A.D. Luca, Pseudopalindrome closure operators in free monoids, Theoretical Computer Science 362 (2006) 282–300.
[10] R. Lyndon, M. Schützenberger, The equation $a^M = b^N c^P$ in a free group, Michigan Mathematical Journal 9 (1962) 289–298.
[11] G. Rozenberg, A. Salomaa (Eds.), Handbook of Formal Languages, Springer-Verlag, Berlin, Heidelberg, 1997.
[12] S.S. Yu, Languages and Codes, in: Lecture Notes, Department of Computer Science, National Chung-Hsing University, Taichung, Taiwan, 402, 2005.