Theoretical Computer Science 411 (2010) 617–630

Contents lists available at ScienceDirect

Theoretical Computer Science

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

On a special class of primitive words[☆]

Elena Czeizler[*], Lila Kari, Shinnosuke Seki

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

ARTICLE INFO

Article history:
Received 24 June 2008
Received in revised form 21 September 2009
Accepted 29 September 2009
Communicated by M. Crochemore

Keywords:
Word equations
Fine and Wilf theorem
(Pseudo-)periodicity
(Pseudo-)power
(Pseudo-)primitivity
(Anti-)morphic involution

ABSTRACT

When representing DNA molecules as words, it is necessary to take into account the fact that a word u encodes basically the same information as its Watson–Crick complement $\theta(u)$, where θ denotes the Watson–Crick complementarity function. Thus, an expression which involves only a word u and its complement can be still considered as a repeating sequence. In this context, we define and investigate the properties of a special class of primitive words, called pseudo-primitive words relative to θ or simply θ-primitive words, which cannot be expressed as such repeating sequences. For instance, we prove the existence of a unique θ-primitive root of a given word, and we give some constraints forcing two distinct words to share their θ-primitive root. Also, we present an extension of the well-known Fine and Wilf theorem, for which we give an optimal bound.

1. Introduction

Encoding information as DNA strands as in, e.g., DNA Computing, brings up for investigation new features based on the specific biochemical properties of DNA molecules. Recall that single-stranded DNA molecules can be viewed as words over the quaternary alphabet of bases $\{A, T, C, G\}$. Moreover, one of the main properties of DNA molecules is the Watson–Crick complementarity of the bases A and T and respectively G and C. Because of this property two Watson–Crick complementary single DNA strands with opposite orientation bind together to form a DNA double strand, in a process called base-pairing. Recently, there were several approaches to generalize notions from classical combinatorics on words in order to incorporate this major characteristic of DNA molecules, see, e.g., [1–3]. Along these lines, in this paper, we generalize the concept of *primitivity* and define *pseudo-primitive words*.

The notion of periodicity plays an important role in various fields of theoretical computer science, such as algebraic coding theory, [4], and combinatorics on words, [5,6]. An integer $p \geq 1$ is a period of a word if any of two letters on the word which are distant from each other by p letters are the same. The well-known periodicity theorem by Fine and Wilf states that if a word has two periods p, q and is of length at least $p + q - \gcd(p, q)$, then $\gcd(p, q)$ is also a period of the word, where $\gcd(p, q)$ is the greatest common divisor of p and q [7]. This theorem can be rephrased as: if a power of a word u and a power of a word v share the same prefix of length $|u| + |v| - \gcd(|u|, |v|)$, then u and v are powers of a same word t. This description elucidates the relationship between the Fine and Wilf theorem and the notion of primitivity. A word is called *primitive* if it cannot be decomposed as a power of another word. Investigating the primitivity of a word is often the first step when analyzing its properties. Moreover, how a word can be decomposed and whether two words are powers of a common word are two questions which were widely investigated in language theory, see, e.g., [5,6,8].

☆ The conference version of this paper was published as: E. Czeizler, L. Kari, S. Seki, On a special class of primitive words, in: Proc. MFCS 2008, LNCS 5162, 2008, pp. 265–277.

* Corresponding address: Department of IT, Åbo Akademi University, Turku 20520, Finland. Tel.: +1 519 661 2111.
E-mail addresses: elena.czeizler@abo.fi (E. Czeizler), lila@csd.uwo.ca (L. Kari), sseki@csd.uwo.ca (S. Seki).

0304-3975/$ – see front matter © 2009 Elsevier B.V. All rights reserved.
doi:10.1016/j.tcs.2009.09.037

While, in classical combinatorics on words we look for repetitions of the form u^i for some word u and some $i \geq 2$, when dealing with DNA molecules (i.e., their abstract representation as words) we have to take into account the fact that 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. In other words, we can extend the notion of power to *pseudo-power relative to* θ or simply θ*-power*. A θ-power of u is a word of the form $u_1u_2 \cdots u_n$ for some $n \geq 1$, where $u_1 = u$ and for any $2 \leq i \leq n$, u_i is either u or $\theta(u)$. In this context, we define θ*-primitive words* as strings which cannot be a θ-power of another word. Also, we define the θ*-primitive root* of a word w as the shortest word u such that w is a θ-power of u. In classical combinatorics on words, there exist two equivalent definitions for the *primitive root* of a word w as the shortest word u such that w is a power of u, or the unique primitive word u such that w is a power of u. The first main contribution of this paper is to propose such equivalent definitions for the θ-primitive root of a word, that is, we prove that the θ-primitive root of a word w is the unique θ-primitive word u such that w is a θ-power of u. In the process of obtaining this result, we also prove an extension of the Fine and Wilf theorem. Until now, several extensions of this theorem were proved, see, e.g., [9–14]. In this paper, we look at the case when a θ-power of u and a θ-power of v share a same prefix. If the prefix is longer than a given bound, then we prove that u and v are θ-powers of a same word, that is, they share their θ-primitive root. Our bound is twice the length of the longer word (u or v) plus the length of the other word minus the greatest common divisor of the lengths of u and v. Moreover, we show that this bound is optimal.

The paper is organized as follows. In Section 2, we fix our terminology and recall some basic results. In Section 3 we investigate some basic properties of θ-primitive words. In particular, we give an extension of the Fine and Wilf theorem which implies immediately that we can define the θ-primitive root of a word in the two equivalent ways. In Section 4, we present several constraints forcing two words to share their θ-primitive root. In Section 5, we investigate some connections between the θ-primitive words that we introduced here and the θ-palindrome words, which were proposed and investigated in [2,3]. In Section 6, we present the optimal bound for our extension of the Fine and Wilf theorem.

2. Preliminaries

Let Σ be a finite alphabet. We denote by Σ^* the set of all finite words over the alphabet Σ, by ϵ the empty word, and by Σ^+ the set of all nonempty finite words over Σ. The *length* of a word w, denoted by $|w|$, is the number of letters occurrences, i.e., if $w = a_1 \dots a_n$ with $a_i \in \Sigma$, $1 \leq i \leq n$, then $|w| = n$. For a letter $a \in \Sigma$, let $|w|_a$ denote the number of occurrences of a in w. Therefore, $|w| = \sum_{a\in\Sigma} |w|_a$. We say that u is a *prefix* (resp. a *suffix*) of v, if $v = ut$ (resp. $v = tu$) for some $t \in \Sigma^*$. For any integer $0 \leq k \leq |v|$, we use the notation $\mathrm{pref}_k(v)$ ($\mathrm{suff}_k(v)$) for the prefix (resp. suffix) of length k of a word v, and $\mathrm{Pref}(v)$ ($\mathrm{Suff}(v)$) for the set of all prefixes (resp. all suffixes) of v. In particular $\mathrm{pref}_0(v) = \epsilon$ for any word $v \in \Sigma^*$. An integer $p \geq 1$ is a *period* of a word $w = a_1 \dots a_n$, with $a_i \in \Sigma$ for all $1 \leq i \leq n$, if $a_i = a_{i+p}$ for all $1 \leq i \leq n - p$.

A word $w \in \Sigma^+$ is called *primitive* if it cannot be written as a power of another word; that is, $w = u^n$ implies $n = 1$ and $w = u$. For a word $w \in \Sigma^+$, the shortest $u \in \Sigma^+$ such that $w = u^n$ for some $n \geq 1$ is called the *primitive root* of the word w and is denoted by $\rho(w)$. The following result gives an alternative, equivalent way for defining the primitive root of a word.

Theorem 1. *For each word $w \in \Sigma^*$, there exists a unique primitive word $t \in \Sigma^+$ such that $\rho(w) = t$, i.e., $w = t^n$ for some $n \geq 1$.*

The next result illustrates another property of primitive words.

Proposition 2. *Let $u \in \Sigma^+$ be a primitive word. Then u cannot be a factor of u^2 in a nontrivial way, i.e., if $u^2 = xuy$, then necessarily either $x = \epsilon$ or $y = \epsilon$.*

We say that two words u and v *commute* if $uv = vu$. The following result characterizes the commutation of two words in terms of primitive roots.

Theorem 3. *For $u, v \in \Sigma^*$, the following conditions are equivalent:* (i) *u and v commute;* (ii) *u and v satisfy a non-trivial relation, i.e., an equation where the two sides are not graphically identical;* (iii) *u and v have the same primitive root.*

For two words u and v, we denote by $u \wedge v$ the *maximal common prefix of u and v*. The following result from [6] will be very useful in our future considerations.

Theorem 4. *Let $X = \{x, y\} \subseteq \Sigma^*$ such that $xy \neq yx$. Then, for each words $u, v \in X^*$ we have*

$$u \in xX^+, \qquad v \in yX^+, \quad |u|, |v| \geq |xy \wedge yx|, \ \Rightarrow u \wedge v = xy \wedge yx.$$

The following result is an immediate consequence.

Corollary 5. *Let $X = \{x, y\} \subseteq \Sigma^*$, $u \in xX^*$, and $v \in yX^*$ such that $|u|, |v| \geq |xy|$. If $|u \wedge v| \geq |xy|$, then $\rho(x) = \rho(y)$.*

Two words u and v are said to be *conjugate* if there exist words x and y such that $u = xy$ and $v = yx$. In other words, v can be obtained via a cyclic permutation of u. The next result characterizes the conjugacy of two words.

Theorem 6. *Let $u, v \in \Sigma^+$. Then the following conditions are equivalent:* (i) *u and v are conjugate;* (ii) *there exists a word z such that $uz = zv$; moreover, this holds if and only if $u = pq$, $v = qp$, and $z = (pq)^i p$, for some $p, q \in \Sigma^*$ and $i \geq 0$;* (iii) *the primitive roots of u and v are conjugate.*

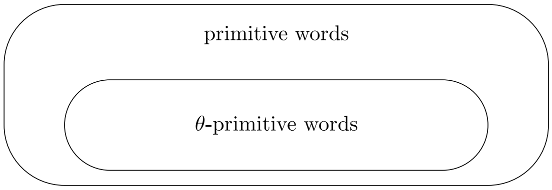

Fig. 1. The sets of primitive and θ-primitive words.

Note that conjugacy is an equivalence relation, the *conjugacy class* of a word w consisting of all conjugates of w. The following is a well-known result.

Proposition 7. *If w is a primitive word, then its conjugacy class contains $|w|$ distinct primitive words.*

The following result, known as the Fine and Wilf theorem in its form for words, see [6,5], illustrates a fundamental periodicity property of words. As usual, $\gcd(n, m)$ denotes the *greatest common divisor of n and m.*

Theorem 8. *Let $u, v \in \Sigma^*$, $n = |u|$, $m = |v|$, and $d = \gcd(n, m)$. If two powers u^i and v^j of u and v have a common prefix of length at least $n + m - d$, then u and v are powers of a common word. Moreover, the bound $n + m - d$ is optimal.*

A mapping $\theta : \Sigma^* \to \Sigma^*$ is called a *morphism* (an *antimorphism*) if for any words $u, v \in \Sigma^*$, $\theta(uv) = \theta(u)\theta(v)$ (resp. $\theta(uv) = \theta(v)\theta(u)$). A mapping $\theta : \Sigma^* \to \Sigma^*$ is called an *involution* if, for all words $u \in \Sigma^*$, $\theta(\theta(u)) = u$. Watson–Crick complementarity is a typical example of antimorphic involutions; in fact, it is defined as the antimorphic involution θ satisfying $\theta(A) = T$, $\theta(T) = A$, $\theta(C) = G$, and $\theta(G) = C$, which is called the Watson–Crick involution.

For a mapping $\theta : \Sigma^* \to \Sigma^*$, a word $w \in \Sigma^*$ is called *θ-palindrome* if $w = \theta(w)$, see [2,3]. We say that a word $w \in \Sigma^+$ is a *pseudo-power of a non-empty word $t \in \Sigma^+$ relative to θ*, or simply *θ-power of t*, if $w \in t\{t, \theta(t)\}^*$. Conversely, t is called a *pseudo-period of w relative to θ*, or simply *θ-period of w* if $w \in t\{t, \theta(t)\}^*$. Hence t is a θ-period of w if and only if w is a θ-power of t. We call a word $w \in \Sigma^+$ *θ-primitive* if there exists no non-empty word $t \in \Sigma^+$ such that w is a θ-power of t and $|w| > |t|$. We define the *θ-primitive root of w*, denoted by $\rho_\theta(w)$, as the shortest word t such that w is a θ-power of t.

3. Properties of θ-primitive words

In this section, we consider $\theta : \Sigma^* \to \Sigma^*$ to be either a morphic or an antimorpic involution, other than the identity function. We start by looking at some basic properties of θ-primitive words.

Proposition 9. *If a word $w \in \Sigma^+$ is θ-primitive, then it is also primitive. Moreover, the converse is not always true.*

Proof. Suppose that w is a θ-primitive word but not primitive. Then there exists some $t \in \Sigma^+$ such that $w = t^n$ with $n \geq 2$. By definition of θ-power, w is a θ-power of t. However, this contradicts the θ-primitivity of w because $|t| < |w|$. For the converse, since θ is not the identity function, there exists a letter a such that $\theta(a) \neq a$. Then, if we take $w = a\theta(a)$, it is obvious that w is primitive, but not θ-primitive. □

Thus, the class of θ-primitive words is strictly included in the set of primitive ones, as illustrated in Fig. 1.

Proposition 10. *The θ-primitive root of a word is θ-primitive.*

Proof. Let $w \in \Sigma^+$ and $t = \rho_\theta(w)$ be its θ-primitive root, that is, w is a θ-power of t. Suppose, now that t is not θ-primitive. Then there exists a word $s \in \Sigma^*$ such that t is a θ-power of s and $|s| < |t|$. Note that $\theta(t)$ is a θ-power of either s or $\theta(s)$. Thus, w is a θ-power of s. However, this contradicts t being the θ-primitive root of w because $|s| < |t|$. □

We also obtain the following result as an immediate consequence.

Corollary 11. *The θ-primitive root of a word is primitive.*

Contrary to the case of primitive words, a conjugate of a θ-primitive word need not be θ-primitive, as shown by the following two examples.

Example 1. Let $\theta : \{A, T, C, G\}^* \to \{A, T, C, G\}^*$ be the Watson–Crick involution defined in Section 2. Then the word $w = GCTA$ is θ-primitive, while its conjugate $w' = AGCT = AG\theta(AG)$ is not.

Example 2. Let $\theta : \{a, b, c, d\}^* \to \{a, b, c, d\}^*$ be a morphic involution defined by $\theta(a) = c$, $\theta(c) = a$, $\theta(b) = d$, and $\theta(d) = b$. Then the word $w = abadcb$ is θ-primitive, while its conjugate $w' = babadc = (ba)^2\theta(ba)$ is not.

So, we can formulate the following result.

Proposition 12. *The class of θ-primitive words is not necessarily closed under circular permutations.*

Fine and Wilf's result on words (Theorem 8) constitutes one of the fundamental periodicity properties of words. Thus, a natural question is whether we can obtain an extension of this result when for two words u, v, instead of taking a power of u and a power of v, we look at a θ-power of u and a θ-power of v. First, we analyze the case when θ is a morphic involution; it turns out that in this case we can obtain the same bound as in Theorem 8. However, since the proof of this result is analogous to the one for Theorem 8, see for instance [5], we will not include it here.

Theorem 13. *Let $\theta : \Sigma^* \to \Sigma^*$ be a morphic involution, $u, v \in \Sigma^+$ with $n = |u|$, $m = |v|$, and $d = \gcd(n, m)$, $\alpha(u, \theta(u)) \in u\{u, \theta(u)\}^*$, and $\beta(v, \theta(v)) \in v\{v, \theta(v)\}^*$. If the two θ-powers $\alpha(u, \theta(u))$ and $\beta(v, \theta(v))$ have a common prefix of length at least $n + m - d$, then there exists a word $t \in \Sigma^+$ such that $u, v \in t\{t, \theta(t)\}^*$, i.e., $\rho_\theta(u) = \rho_\theta(v)$. Moreover, the bound $n + m - d$ is optimal.*

However, as illustrated by the following example, if the mapping θ is an antimorphic involution, then the bound given by Theorem 13 is no longer enough.

Example 3. Let $\theta : \{a, b\}^* \to \{a, b\}^*$ be the mirror mapping defined as follows: $\theta(a) = a$, $\theta(b) = b$, and $\theta(w_1 \dots w_n) = w_n \dots w_1$, where $w_i \in \{a, b\}$ for all $1 \le i \le n$. Obviously, θ is an antimorphic involution on $\{a, b\}^*$. Let now $u = (ab)^k b$ and $v = ab$. Then, u^2 and $v^k \theta(v)^{k+1}$ have a common prefix of length $2|u| - 1 > |u| + |v| - \gcd(|u|, |v|)$. However u and v do not have the same θ-primitive root, that is, $\rho_\theta(u) \ne \rho_\theta(v)$.

Before stating an analogous result also for the case of antimorphic involutions, we introduce the mapping $\varphi : \Sigma^* \times \Sigma \to \mathbb{N}$ defined as $\varphi(u, a) = |u|_a + |u|_{\theta(a)}$, that is, the number of occurrences of the letters a and $\theta(a)$ in the word u. Note that for any letter a and any word u, $\varphi(u, a) = \varphi(u, \theta(a)) \le |u|$, with equality only when $u \in \{a, \theta(a)\}^*$. We will call this mapping the *characteristic function on the alphabet Σ*. Moreover, $\mathrm{lcm}(n, m)$ denotes, as usual, the *least common multiple of n and m.*

Theorem 14. *Let $\theta : \Sigma^* \to \Sigma^*$ be an antimorphic involution, $u, v \in \Sigma^+$, and $\alpha(u, \theta(u)) \in u\{u, \theta(u)\}^*$, $\beta(v, \theta(v)) \in v\{v, \theta(v)\}^*$ be two θ-powers sharing a common prefix of length at least $\mathrm{lcm}(|u|, |v|)$. Then, there exists a word $t \in \Sigma^+$ such that $u, v \in t\{t, \theta(t)\}^*$, i.e., $\rho_\theta(u) = \rho_\theta(v)$. In particular, if $\alpha(u, \theta(u)) = \beta(v, \theta(v))$, then $\rho_\theta(u) = \rho_\theta(v)$.*

Proof. The proof of this result uses the techniques from [11]. First, we can suppose, without loss of generality that $\gcd(|u|, |v|) = 1$ and thus $\mathrm{lcm}(|u|, |v|) = |u||v|$. Otherwise, i.e., $\gcd(|u|, |v|) = d \ge 2$, we consider a new alphabet $\Sigma' = \Sigma^d$, where the new letters are words of length d in the original alphabet, and we look at the words u and v as elements of $(\Sigma')^+$. In the larger alphabet $\gcd(|u|, |v|) = 1$, and if we can prove the theorem there it immediately gives the general proof. Let now $|u| = n$ and $|v| = m$. If we denote by $\alpha'(u, \theta(u)) \in u\{u, \theta(u)\}^*$ and $\beta'(v, \theta(v)) \in v\{v, \theta(v)\}^*$ the prefixes of length $\mathrm{lcm}(n, m) = nm$ of $\alpha(u, \theta(u))$ and $\beta(v, \theta(v))$, respectively, then we actually have $\alpha'(u, \theta(u)) = \beta'(v, \theta(v))$.

Since the mapping θ is an involution, we can easily notice that for any word w and any letter a, $\varphi(w, a) = \varphi(\theta(w), a)$. Moreover, since $\alpha'(u, \theta(u)) = \beta'(v, \theta(v))$, whenever, for a letter a, $\varphi(u, a) > 0$, we also have that $\varphi(v, a) > 0$.

Suppose now that there exist two letters a and b such that $\{a, \theta(a)\} \cap \{b, \theta(b)\} = \emptyset$, $\varphi(u, a) > 0$, and $\varphi(u, b) > 0$. Then, since $n = |u| = \sum_{c \in \Sigma} |u|_c$, we have that $\varphi(u, a) < n$. Let us look next at the number of occurrences of a and $\theta(a)$ in the two sides of the equality $\alpha'(u, \theta(u)) = \beta'(v, \theta(v))$. Since $|\alpha'(u, \theta(u))| = |\beta'(v, \theta(v))| = nm$, where $|u| = n$, and $|v| = m$, we obtain $m\varphi(u, a) = n\varphi(v, a)$. However this contradicts the fact that $\gcd(n, m) = 1$ and $\varphi(u, a) < n$. So, there exists a letter $a \in \Sigma$ such that $u \in \{a, \theta(a)\}^+$. Since $\alpha'(u, \theta(u)) = \beta'(v, \theta(v))$, this implies that also $v \in \{a, \theta(a)\}^+$. Thus, $\rho_\theta(u) = \rho_\theta(v)$. □

Note that, in many cases there is a big gap between the bounds given in Theorems 13 and 14. Moreover, Theorem 14 does not give the optimal bound for the general case when θ is an antimorphic involution. In Section 6, we show that this optimal bound for the general case is $2|u| + |v| - \gcd(|u|, |v|)$, where $|u| > |v|$, while for some particular cases we obtain bounds as low as $|u| + |v| - \gcd(|u|, |v|)$. As an immediate consequence of Theorems 13 and 14, we obtain the following result.

Corollary 15. *For any word $w \in \Sigma^+$ there exists a unique θ-primitive word $t \in \Sigma^+$ such that $w \in t\{t, \theta(t)\}^*$, i.e., $\rho_\theta(w) = t$.*

Let us note now that, maybe even more importantly, just as in the case of primitive words, this result provides us with an alternative, equivalent way for defining the θ-primitive root of a word w, i.e., *the θ-primitive word t such that $w \in t\{t, \theta(t)\}^*$*. This proves to be a very useful tool in our future considerations.

Moreover, we also obtain the following two results as immediate consequences of Theorems 13 and 14.

Corollary 16. *Let $u, v \in \Sigma^+$ be two words such that $\rho(u) = \rho(v) = t$. Then $\rho_\theta(u) = \rho_\theta(v) = \rho_\theta(t)$.*

Corollary 17. *If we have two words $u, v \in \Sigma^+$ such that $u \in v\{v, \theta(v)\}^*$, then $\rho_\theta(u) = \rho_\theta(v)$.*

4. Relations imposing θ-periodicity

It is well-known, due to Theorem 3, that any non-trivial equation over two distinct words forces them to be powers of a common word, i.e., to share a common primitive root.Thus, a natural question is whether this would also be the case when we want two distinct words to be θ-powers of a common word, i.e., to share a common θ-primitive root. From [1], we already know that the equation $uv = \theta(v)u$ imposes $\rho_\theta(u) = \rho_\theta(v)$ only when θ is a morphic involution. In this section, we give several examples of equations over $\{u, \theta(u), v, \theta(v)\}$ forcing $\rho_\theta(u) = \rho_\theta(v)$ in the case when $\theta : \Sigma^* \to \Sigma^*$ is an antimorphic involution.

The first equation we look at is very similar to the commutation equation of two words, but it involves also the mapping θ.

Theorem 18. *Let $\theta : \Sigma^* \to \Sigma^*$ be an antimorphic involution over the alphabet Σ and $u, v \in \Sigma^+$. If $uv\theta(v) = v\theta(v)u$, then $\rho_\theta(u) = \rho_\theta(v)$.*

Proof. Since $uv\theta(v) = v\theta(v)u$, we already know, due to Theorem 3, that there exists a primitive word $t \in \Sigma^+$ such that $u = t^i$ and $v\theta(v) = t^j$, for some $i, j \geq 0$. If $j = 2k$ for some $k \geq 0$, then we obtain immediately that $v = \theta(v) = t^k$, i.e., $\rho(u) = \rho(v) = t$. Thus, $\rho_\theta(u) = \rho_\theta(t) = \rho_\theta(v)$. Otherwise, i.e., $j = 2k + 1$, we can write $v = t^k t_1$ and $\theta(v) = t_2 t^k$, where $t = t_1 t_2$ and $|t_1| = |t_2| > 0$. Hence, $\theta(v) = \theta(t_1)\theta(t)^k = t_2 t^k$, which implies $t_2 = \theta(t_1)$. In conclusion, $u, v \in t_1\{t_1, \theta(t_1)\}^*$, for some word $t_1 \in \Sigma^+$, i.e., $\rho_\theta(u) = \rho_\theta(t_1) = \rho_\theta(v)$. □

Example 4. Let $\theta : \{a, b\}* \to \{a, b\}^*$ be defined as $\theta(a) = b$ and $\theta(b) = a$, and let $u = ab$ and $v = aba$. Then $uv\theta(v) = v\theta(v)u = (ab)^4$ and $\rho_\theta(u) = \rho_\theta(v) = a$.

Next, we modify the previous equation, such that on one side, instead of $v\theta(v)$, we take its conjugate $\theta(v)v$.

Theorem 19. *Let $\theta : \Sigma^* \to \Sigma^*$ be an antimorphic involution over the alphabet Σ and $u, v \in \Sigma^+$. If $v\theta(v)u = u\theta(v)v$, then $\rho_\theta(u) = \rho_\theta(v)$.*

Proof. If we concatenate the word $\theta(v)$ to the right on both sides of the equation $v\theta(v)u = u\theta(v)v$, then we obtain $(v\theta(v))(u\theta(v)) = (u\theta(v))(v\theta(v))$. Due to Theorem 3, this means that there exists a primitive word $t \in \Sigma^+$ such that $v\theta(v) = t^i$ and $u\theta(v) = t^j$, for some $i, j \geq 0, j \geq \lceil i/2 \rceil$. If $i = 2k$ for some $k \geq 0$, then $\theta(v) = v = t^k$ and thus also $u = t^{j-k}$, i.e., $\rho(u) = \rho(v) = t$. Henceforth, $\rho_\theta(u) = \rho_\theta(t) = \rho_\theta(v)$. Otherwise, i.e., $j = 2k + 1$, we can write $v = t^k t_1$ and $\theta(v) = t_2 t^k$, where $t = t_1 t_2$ and $|t_1| = |t_2| > 0$. Hence, we achieve again $t_2 = \theta(t_1)$, which implies that $v \in t_1\{t_1, \theta(t_1)\}^*$. Moreover, since $u\theta(v) = t^j$, we also obtain $u = t^{j-k-1}t_1 \in t_1\{t_1, \theta(t_1)\}^*$. Thus, $\rho_\theta(u) = \rho_\theta(t_1) = \rho_\theta(v)$. □

Example 5. Using Σ defined in Example 4, let $u = a$ and $v = aba$. Then $v\theta(v)u = u\theta(v)v = abababa$ and $\rho_\theta(u) = \rho_\theta(v) = a$.

The next result gives an example of a more intricate equation which also imposes θ-periodicity.

Theorem 20. *Let $\theta : \Sigma^* \to \Sigma^*$ be an antimorphic involution over the alphabet Σ and $u, v \in \Sigma^*$. If $u^2 v = vu\theta(u)$, then $u = \theta(u)$ and $\rho(u) = \rho(v)$.*

Proof. Since $u^2 v = vu\theta(u)$, due to Theorem 6, there exist some words $z, t \in \Sigma^*$ and some integer $k \geq 0$ such that $u^2 = zt$, $u\theta(u) = tz$, and $v = (zt)^k z$. This representation clarifies that $u\theta(u)$ can be obtained by cyclically permuting u^2. Note that this operation preserves the property of the word being square. Thus, $u\theta(u) = w^2$ for some $w \in \Sigma^*$, and in fact we have $u = \theta(u)$ because θ is length-preserving. As a result, the given equation becomes $u^2 v = vu^2$ so that $\rho(u) = \rho(v)$. □

Recall that the primitive root of a θ-palindromic word is θ-palindrome. As such, Theorem 20 means that $u^2 v = vu\theta(u)$ implies $v = \theta(v)$. Examples of u and v satisfying $u^2 v = vu\theta(u)$ are hence quite trivial like $u = w^i$ and $v = w^j$ for some θ-palindrome w and $i, j \geq 0$.

Next, we look at the case when both uv and vu are θ-palindromic words, which also proves to be enough to impose that $u, v \in \{t, \theta(t)\}^*$ for some $t \in \Sigma^+$.

Theorem 21. *Let $u, v \in \Sigma^*$ be two words such that both uv and vu are a θ-palindrome and let $t = \rho(uv)$. Then, $t = \theta(t)$ and either $\rho(u) = \rho(v) = t$ or $u = (t_1\theta(t_1))^i t_1$ and $v = \theta(t_1)(t_1\theta(t_1))^j$, where $t = t_1\theta(t_1)$ and $i, j \geq 0$.*

Proof. The equality $uv = \theta(uv)$ immediately implies that $t = \theta(t)$. Moreover, if u and v commute, then $\rho(u) = \rho(v) = \rho(uv) = t$. Assume now that u and v do not commute. Since $\rho(u) \neq \rho(v)$ and $uv = t^n$ for some $n \geq 1$, we can write $u = t^i t_1$ and $v = t_2 t^{n-i-1}$ for some $i \geq 0$ and $t_1, t_2 \in \Sigma^+$ such that $t = t_1 t_2$. Thus, $vu = t_2 t^{n-1} t_1 = (t_2 t_1)^n$ and since $vu = \theta(vu)$ we obtain that also $t_2 t_1$ is a θ-palindrome, i.e., $t_2 t_1 = \theta(t_2 t_1) = \theta(t_1)\theta(t_2)$. Now, if $|t_1| = |t_2|$, then $t_2 = \theta(t_1)$ and thus $t = t_1\theta(t_1)$, $u = t^i t_1$, and $v = \theta(t_1)t^{n-i-1}$. Otherwise, either $|t_1| > |t_2|$ or $|t_1| < |t_2|$. We consider next only the case $|t_1| > |t_2|$, the other one being similar. Since $t_2 t_1 = \theta(t_1)\theta(t_2)$, we can write $\theta(t_1) = t_2 x$ and $t_1 = x\theta(t_2)$ for some word $x \in \Sigma^+$ with $x = \theta(x)$. Then, since $t = \theta(t)$ we have that $t = t_1 t_2 = x\theta(t_2)t_2 = \theta(x\theta(t_2)t_2) = \theta(t_2)t_2 x$. Hence, x and $\theta(t_2)t_2$ commute, which contradicts the primitivity of t. □

Example 6. With θ defined in Example 4, let $u = aba$ and $v = babab$. Then both uv and vu are a θ-palindrome. For such u and v, $t = \rho(uv) = ab = a\theta(a)$.

As an immediate consequence we obtain the following result.

Corollary 22. *For $u, v \in \Sigma^*$, if $uv = \theta(uv)$ and $vu = \theta(vu)$, then $\rho_\theta(u) = \rho_\theta(\theta(v))$. In particular, there exists some $t \in \Sigma^+$ such that $u, v \in \{t, \theta(t)\}^*$.*

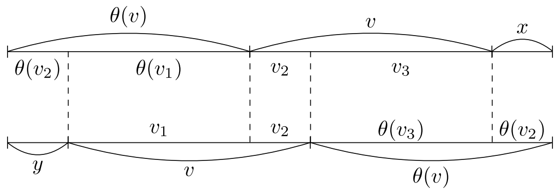

Fig. 2. The equation $\theta(v)vx = yv\theta(v)$.

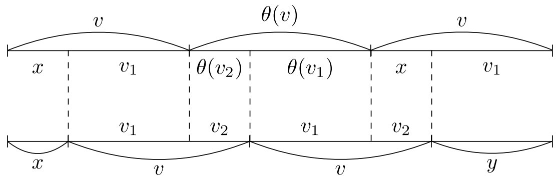

Fig. 3. The equation $v\theta(v)v = xv^2y$.

5. On θ-primitive and θ-palindromic words

In this section, we investigate some word equations under which a θ-primitive word must be a θ-palindrome. Throughout this section we consider $\theta : \Sigma^* \to \Sigma^*$ to be an antimorphic involution over the alphabet Σ.

Theorem 23. *Let $\theta : \Sigma^* \to \Sigma^*$ be an antimorphic involution over the alphabet Σ and $v \in \Sigma^+$ be a θ-primitive word. If $\theta(v)vx = yv\theta(v)$ for some words $x, y \in \Sigma^*$ with $|x|, |y| < |v|$, then v is a θ-palindrome and $x = y = \epsilon$.*

Proof. Assume there exist some words $x, y \in \Sigma^*$ with $|x|, |y| < |v|$, such that $\theta(v)vx = yv\theta(v)$, as illustrated in Fig. 2.

Then, we can write $v = v_1v_2 = v_2v_3$, with $v_1, v_2, v_3 \in \Sigma^*$, $y = \theta(v_2) = x$, $v_1 = \theta(v_1)$, $v_3 = \theta(v_3)$. Since $v_1v_2 = v_2v_3$, we can write $v_1 = pq$, $v_3 = qp$, $v_2 = (pq)^ip$, and $v = (pq)^{i+1}p$ for some words $p, q \in \Sigma^*$ and some $i \geq 0$. Thus, $pq = \theta(pq)$ and $qp = \theta(qp)$, which, due to Theorem 21, leads to one of the following two cases. First, if $p = t^kt_1$ and $q = \theta(t_1)t^j$, where $k, j \geq 0$ and $t = t_1\theta(t_1)$ is the primitive root of pq, then we obtain that $v = t^{(k+j+1)(i+1)+k}t_1$ with $(k+j+1)(i+1)+k \geq 1$, which contradicts the θ-primitivity of v. Second, if $\rho(p) = \rho(q) = t$, then also $v \in \{t\}^*$ where $t = \theta(t)$. Thus, $v = \theta(v)$, and the initial identity becomes $v^2x = yv^2$. However, since v is θ-primitive and thus also primitive, we immediately obtain, due to Proposition 2, that $x = y = \epsilon$. $\square$

In other words, the previous result states that if v is a θ-primitive word, then $\theta(v)v$ cannot overlap with $v\theta(v)$ in a nontrivial way. However, the following example shows that this is not the case anymore if we look at the overlaps between $\theta(v)v$ and v^2, or between $v\theta(v)$ and v^2, respectively, even if we consider the larger class of primitive words.

Example 7. Let $\theta : \Sigma^* \to \Sigma^*$ be an antimorphic involution over the alphabet Σ, $p, q \in \Sigma^+$ such that $\rho(p) \neq \rho(q)$, $p = \theta(p)$, and $q = \theta(q)$, and let $v = p^2q^2p$ and $u = pq^2p^2$. It is easy to see that u and v are primitive words. In addition, if we take $\Sigma = \{a, b\}$, the mapping θ to be the mirror image, $p = a$, and $q = b$, then u and v are actually θ-primitive words. Since $\theta(v) = pq^2p^2$ and $\theta(u) = p^2q^2p$, we can write $xv^2 = v\theta(v)y$ and $y\theta(u)u = u^2z$ where $x = p^2q^2$, $y = pq^2p$, and $z = q^2p^2$. Thus, for primitive (resp. θ-primitive) words u and v, $v\theta(v)$ can overlap with v^2 and $\theta(u)u$ with u^2 in a nontrivial way.

Maybe even more surprisingly, the situation changes again if we try to fit v^2 inside $v\theta(v)v$, as shown by the following result.

Theorem 24. *Let $\theta : \Sigma^* \to \Sigma^*$ be an antimorphic involution over the alphabet Σ and $v \in \Sigma^+$ be a primitive word. If $v\theta(v)v = xv^2y$ for some words $x, y \in \Sigma^*$, then v is θ-palindrome and either $x = \epsilon$ and $y = v$ or $x = v$ and $y = \epsilon$.*

Proof. Suppose that $v\theta(v)v = xv^2y$ for some words $x, y \in \Sigma^*$, as illustrated in Fig. 3.

If we look at this identity from left to right, then we can write $v = xv_1 = v_1v_2$, with $v_1, v_2 \in \Sigma^*$ such that $|x| = |v_2|$ and $\theta(v) = \theta(v_2)\theta(v_1)$. Then, if we look at the right sides of this identity, then we immediately obtain that $x = v_2$ and $v_1 = y$. Thus, $v = xy = yx$, implying that $x, y \in \{t\}^*$, for some primitive word t. However, since v is primitive, this means that either $x = \epsilon$ and $y = v$ or $x = v$ and $y = \epsilon$. Moreover, in both cases we also obtain $v = \theta(v)$. $\square$

6. A shorter bound for the Fine and Wilf theorem (antimorphic case)

Throughout this section we take $\theta : \Sigma^* \to \Sigma^*$ to be an antimorphic involution, $u, v \in \Sigma^+$ with $|u| > |v|$, $\alpha(u, \theta(u))$ be a θ-power of u, and $\beta(v, \theta(v))$ be a θ-power of v. Recall that $\alpha(u, \theta(u))$ starts with u and $\beta(v, \theta(v))$ starts with v. We start our analysis with the case when v is θ-palindrome.

Theorem 25. *Let u and v be two words with $|u| > |v|$ and $v = \theta(v)$. If there exist two θ-powers $\alpha(u, \theta(u)) \in u\{u, \theta(u)\}^*$ and $\beta(v, \theta(v)) \in v\{v, \theta(v)\}^*$ having a common prefix of length at least $|u| + |v| - \gcd(|u|, |v|)$, then $\rho_\theta(u) = \rho_\theta(v)$.*

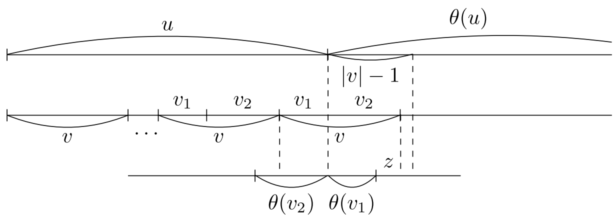

Fig. 4. The common prefix of $u\theta(u)$ and v^n of length $|u| + |v| - 1$.

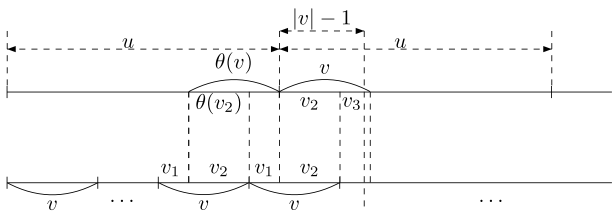

Fig. 5. The common prefix of u^2 and $\beta(v, \theta(v))$ of length $|u| + |v| - 1$.

Proof. First, we can suppose, without loss of generality that $\gcd(|u|, |v|) = 1$. Otherwise, i.e., $\gcd(|u|, |v|) = d \geq 2$, we consider a new alphabet $\Sigma' = \Sigma^d$, where the new letters are words of length d in the original alphabet, and we look at the words u and v as elements of $(\Sigma')^+$. In the larger alphabet $\gcd(|u|, |v|) = 1$, and if we can prove the theorem there it immediately gives the general proof.

Since $v = \theta(v)$, $\beta(v, \theta(v)) = v^n$ for some $n \geq 2$. Moreover, if $v \in \Sigma$, then trivially $u \in v\{v, \theta(v)\}^*$, i.e., $\rho_\theta(u) = \rho_\theta(v)$. So, suppose next that $|v| \geq 2$ and, since $\gcd(|u|, |v|) = 1$, $u = v^i v_1$, where $i \geq 1$ and $v = v_1 v_2$ with $v_1, v_2 \in \Sigma^+$.

If $\alpha(u, \theta(u)) = u^2\alpha'(u, \theta(u))$, then u^2 and v^n have a common prefix of length at least $|u| + |v| - \gcd(|u|, |v|)$, which, due to Theorem 8, implies that $\rho(u) = \rho(v) = t$, for some primitive word $t \in \Sigma^+$, and thus $\rho_\theta(u) = \rho_\theta(t) = \rho_\theta(v)$.

Otherwise, $\alpha(u, \theta(u)) = u\theta(u)\alpha'(u, \theta(u))$ for some $\alpha'(u, \theta(u)) \in \{u, \theta(u)\}^*$. Now, we have two cases depending on $|v_1|$ and $|v_2|$. We present here only the case when $|v_1| \leq |v_2|$, see Fig. 4, the other one being symmetric. Now, since θ is an antimorphism, $\theta(\mathrm{suff}_{|v|-1}(u)) = \mathrm{pref}_{|v|-1}(\theta(u))$. So, we can write $v_2 = \theta(v_1)z$ for some $z \in \Sigma^*$, since $|v_1| \leq |v_2| \leq |v| - 1 = |v| - \gcd(|u|, |v|)$. Now, to the left of the border-crossing v there is at least one occurrence of another v, so we immediately obtain $z = \theta(z)$, as $v_2 = \theta(v_1)z$ and $\theta(v_2) = \theta(z)v_1$. Then, $v = v_1\theta(v_1)z = zv_1\theta(v_1) = \theta(v)$ which implies, due to Theorem 18, that $\rho_\theta(v_1) = \rho_\theta(z)$. So, since $v = v_1\theta(v_1)z$ and $u = v^i v_1 = (v_1\theta(v_1)z)^i v_1$, we obtain $\rho_\theta(u) = \rho_\theta(v)$. □

Let us look next at the case when u is θ-palindrome.

Theorem 26. *Let u and v be two words with $|u| > |v|$ and $u = \theta(u)$. If there exist two θ-powers $\alpha(u, \theta(u)) \in u\{u, \theta(u)\}^*$ and $\beta(v, \theta(v)) \in v\{v, \theta(v)\}^*$ having a common prefix of length at least $|u| + |v| - \gcd(|u|, |v|)$, then $\rho_\theta(u) = \rho_\theta(v)$.*

Proof. As in the previous proof, we can suppose without loss of generality that $\gcd(|u|, |v|) = 1$. Also, since $u = \theta(u)$, we actually have $\alpha(u, \theta(u)) = u^n$ for some $n \geq 2$. Moreover, since u starts with v and $u = \theta(u)$, we also know that u ends with $\theta(v)$. Now, if $v \in \Sigma$, then trivially $u \in v\{v, \theta(v)\}^*$, i.e., $\rho_\theta(u) = \rho_\theta(v)$. So, we can suppose next that $|v| \geq 2$ and thus, since $\gcd(|u|, |v|) = 1$, we have $u = \beta'(v, \theta(v))v'$, where $\beta'(v, \theta(v))$ is a prefix of $\beta(v, \theta(v))$ and $v' \in \Sigma^+$, $v' \in \mathrm{Pref}(v) \cup \mathrm{Pref}(\theta(v))$.

Case 1: We begin our analysis with the case when the border between the first two u's falls inside a v, as illustrated in Fig. 5. Then, we can write $v = v_1v_2 = v_2v_3$ where $v_1, v_2, v_3 \in \Sigma^+$, implying that $v_1 = xy$, $v_3 = yx$, and $v_2 = (xy)^j x$ for some $j \geq 0$ and $x, y \in \Sigma^*$. Moreover, since u ends with $\theta(v)$, we also have $v_1 = \theta(v_1)$, i.e., $xy = \theta(y)\theta(x)$. If $x = \epsilon$, then $v_1, v_2, v_3, v \in \{y\}^*$, which implies that also $u \in y\{y, \theta(y)\}^*$, i.e., $\rho_\theta(u) = \rho_\theta(v) = \rho_\theta(y)$; moreover, since $\gcd(|u|, |v|) = 1$ we actually must have $y \in \Sigma$. Similarly, we also obtain $\rho_\theta(u) = \rho_\theta(v)$ when $y = \epsilon$. So, from now on we can suppose that $x, y \in \Sigma^+$.

Let us consider next the case when, before the border-crossing v we have an occurrence of another v, as illustrated in Fig. 5. Then, we have that $v_2 = \theta(v_2)$, i.e., $(xy)^j x = (\theta(x)\theta(y))^j\theta(x)$. If $j \geq 1$, then this means that $x = \theta(x)$ and $y = \theta(y)$. Then, the equality $xy = \theta(y)\theta(x)$ becomes $xy = yx$. So, there exists a word $t \in \Sigma^+$ such that $x, y \in \{t\}^*$, and thus also $v \in \{t\}^+$ and $u \in t\{t, \theta(t)\}^*$, i.e., $\rho_\theta(u) = \rho_\theta(v)$. Otherwise, $j = 0$ and we have $x = \theta(x)$. But then, the equality $xy = \theta(y)\theta(x)$ becomes $xy = \theta(y)x$, implying that $x = p(qp)^n$ and $y = (qp)^m$ for some $m \geq 1$, $n \geq 0$, and some words p and q with $p = \theta(p)$ and $q = \theta(q)$, see [1]. Since u^2 and $\beta(v, \theta(v))$ share a common prefix of length at least $|u| + |v| - \gcd(|u|, |v|) = |u| + |v| - 1$, v_3 and some $\beta'(v, \theta(v))$ share a prefix of length $|v_3| - 1$. Furthermore, as $v_3 = yx = (qp)^m p(qp)^n$, $v = v_1v_2 = p(qp)^{m+n}p(qp)^n$, and $\theta(v) = (pq)^n p(pq)^{m+n}p$, this means that independently of what follows to the right the border-crossing v, either v or $\theta(v)$, we have two expressions over p and q sharing a common prefix of length at least $|p| + |q|$. So, due to Corollary 5, $p, q \in \{t\}^*$ for some $t \in \Sigma^+$, which implies that also $x, y, v \in \{t\}^+$ and $u \in \{t, \theta(t)\}^+$, i.e., $\rho_\theta(u) = \rho_\theta(v)$.

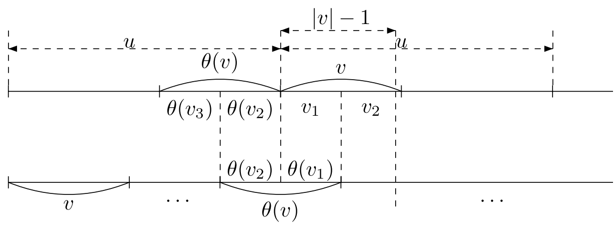

Fig. 6. The common prefix of u^2 and $\beta(v, \theta(v))$ of length $|u| + |v| - 1$.

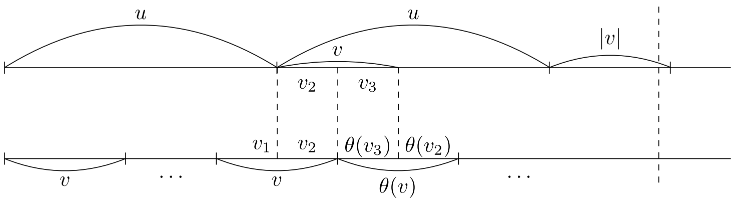

Fig. 7. The prefix of $u^2\alpha'(u, \theta(u))$ and $\beta(v, \theta(v))$ of length $2|u| + |v| - 1$.

Now, suppose that before the border-crossing v we have an occurrence of $\theta(v)$. If $|u| < 2|v| + |v_1|$, then, since $\beta(v, \theta(v))$ starts with v, we must have $v = \theta(v)$, in which case we can use Theorem 25 to conclude that $\rho_\theta(u) = \rho_\theta(v)$. Otherwise, $|u| \geq 2|v| + |v_1|$ and since $u = \theta(u)$, u ends either with $v\theta(v)$ or with $\theta(v)\theta(v)$. In the first case, we obtain $v_3 = \theta(v_3)$, i.e., $yx = \theta(yx)$, which together with $xy = \theta(xy)$ imply, due to Corollary 22, that $x, y \in \{t, \theta(t)\}^*$, for some $t \in \Sigma^+$ and thus, $\rho_\theta(u) = \rho_\theta(v)$. In the second case, we obtain $v_1 = v_3$, i.e., $xy = yx$. So, $x, y \in \{t\}^*$, and thus also $v \in \{t\}^+$ and $u \in t\{t, \theta(t)\}^*$, i.e., $\rho_\theta(u) = \rho_\theta(v)$.
Case 2: Let us consider now the case when the border between the first two u's falls inside $\theta(v)$, as illustrated in Fig. 6. Then, we can write again $v = v_1v_2 = v_2v_3$ where $v_1, v_2, v_3 \in \Sigma^+$, which implies that $v_1 = xy$, $v_3 = yx$, and $v_2 = (xy)^jx$ for some $j \geq 0$ and $x, y \in \Sigma^*$. Just as before, if $x = \epsilon$ or $y = \epsilon$, we immediately obtain that $\rho_\theta(u) = \rho_\theta(v)$. So, we can suppose that $x, y \in \Sigma^+$. Moreover, $v_1 = \theta(v_1)$, i.e., $xy = \theta(xy)$. Now, if the border-crossing $\theta(v)$ is preceded by an occurrence of v, then we also have $v_3 = \theta(v_3)$, i.e., $yx = \theta(yx)$. Then, due to Corollary 22, there exists some $t \in \Sigma^+$ such that $x, y \in \{t, \theta(t)\}^*$, implying that $\rho_\theta(u) = \rho_\theta(v)$, since $v = (xy)^{j+1}x$ and $u = \beta'(v, \theta(v))\theta(v_2)$. If, on the other hand, the border-crossing $\theta(v)$ is preceded by another $\theta(v)$, then we immediately obtain $v_1 = v_3$, i.e., $xy = yx$. So, $x, y \in \{t\}^*$, for some $t \in \Sigma^+$, and thus also $v \in \{t\}^+$ and $u \in t\{t, \theta(t)\}^*$, i.e., $\rho_\theta(u) = \rho_\theta(v)$. $\square$

Although the previous two results give a very short bound, i.e., $|u| + |v| - \gcd(|u|, |v|)$, this is not enough in the general case, as illustrated in Example 3. Nevertheless, we can prove that, independently of how the θ-power $\alpha(u, \theta(u))$ starts, $2|u| + |v| - \gcd(|u|, |v|)$ is enough to impose $\rho_\theta(u) = \rho_\theta(v)$. The first case we consider is when $\alpha(u, \theta(u))$ starts with u^2.

Theorem 27. *Given two words $u, v \in \Sigma^+$ with $|u| > |v|$, if there exist two θ-powers $\alpha(u, \theta(u)) \in u\{u, \theta(u)\}^*$ and $\beta(v, \theta(v)) \in v\{v, \theta(v)\}^*$ having a common prefix of length at least $2|u| + |v| - \gcd(|u|, |v|)$ and, moreover, $\alpha(u, \theta(u)) = u^2\alpha'(u, \theta(u))$ for some $\alpha'(u, \theta(u)) \in \{u, \theta(u)\}^+$, then $\rho_\theta(u) = \rho_\theta(v)$.*

Proof. Just as we did before, we can suppose, without loss of generality, that $\gcd(|u|, |v|) = 1$. Now, if $v \in \Sigma$, then trivially $u \in v\{v, \theta(v)\}^*$, i.e., $\rho_\theta(u) = \rho_\theta(v)$. So, we can suppose next that $|v| \geq 2$ and thus, since $\gcd(|u|, |v|) = 1$, we have $u = \beta'(v, \theta(v))v'$, where $\beta'(v, \theta(v))$ is a prefix of $\beta(v, \theta(v))$ and $v' \in \Sigma^+$ is a prefix of either v or $\theta(v)$.
Case 1: Let us look first at the case when the border between the first two u's falls inside v, i.e., $u = \beta'(v, \theta(v))v_1$ for some $v_1 \in \Sigma^+$ such that $v = v_1v_2$ and $\beta'(v, \theta(v)) \in v\{v, \theta(v)\}^*$ is a prefix of $\beta(v, \theta(v))$. Moreover, if this border-crossing v is followed to the right by another v, then $v^2 = v_1vv_2$, since $\text{pref}_{|v|}(u) = v$. Thus, $v_1v_2 = v_2v_1$, meaning that there exists a primitive word $t \in \Sigma^+$ such that $v_1, v_2 \in \{t\}^+$ and thus $v \in \{t\}^+$. Moreover, since $u = \beta'(v, \theta(v))v_1$, we also have $u \in t\{t, \theta(t)\}^*$, i.e., $\rho_\theta(u) = \rho_\theta(v)$. Otherwise, the border-crossing v is followed to the right by $\theta(v)$, as illustrated in Fig. 7. Thus, we can write $v = v_1v_2 = v_2v_3$ with $v_1, v_2, v_3 \in \Sigma^+$, $|v_1| = |v_3|$, and $v_3 = \theta(v_3)$. But then, Theorem 6 implies that there exist some $i \geq 0$ and some $x, y \in \Sigma^*$ such that $v_1 = xy$, $v_3 = yx$, $v_2 = (xy)^ix$, and $v = (xy)^{i+1}x$. If $x = \epsilon$, then we have that $v_1, v_2, v_3, v \in \{y\}^+$, which implies that also $u \in y\{y, \theta(y)\}^*$, i.e., $\rho_\theta(u) = \rho_\theta(v)$. Similarly, we also obtain $\rho_\theta(u) = \rho_\theta(v)$ when $y = \epsilon$. So, from now on we can suppose that $x, y \in \Sigma^+$.

Suppose first that $i \geq 1$. If we take $|\beta'(v, \theta(v))| = k|v|$ with $k \geq 1$, then the length of the first u is $|u| = k|v| + |v_1| = k(i+1)|xy| + k|x| + |xy|$. Since the second u starts with $v_2 = (xy)^ix$, using length arguments, we must have that its right end will fall inside either v or $\theta(v)$, after exactly $2|xy|$ characters. If the right end of the second u falls inside $\theta(v) = (yx)^{i+1}\theta(x)$, then $\text{suff}_{|xy|}(u) = yx$. But, the first u ended with $v_1 = xy$. So, $xy = yx$, which implies that there exists a primitive word $t \in \Sigma^+$ such that $x, y \in \{t\}^*$, and thus also $v \in \{t\}^+$ and $u \in t\{t, \theta(t)\}^*$, i.e., $\rho_\theta(u) = \rho_\theta(t) = \rho_\theta(v)$. Otherwise, the right end of the second u falls inside v, i.e., $\text{suff}_{2|xy|}(u) = xyxy$. Actually, depending on what precedes to the left this second border-crossing v, either v or $\theta(v)$, we have $\text{suff}_{|x|+2|xy|}(u) \in \{xxyxy, \theta(x)xyxy\}$. Next, we look at the suffix of the first u and we have again two cases depending on what precedes the first border-crossing v. If there is a v to the left of this border-crossing v, then

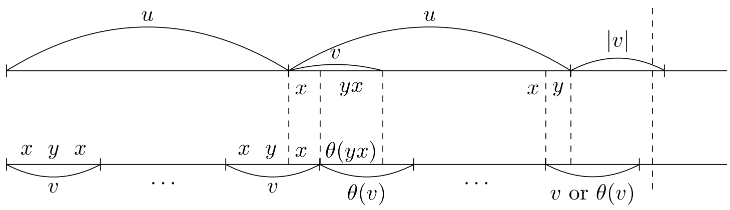

Fig. 8. The prefix of $u^2\alpha'(u, \theta(u))$ and $\beta(v, \theta(v))$ of length $2|u| + |v| - 1$.

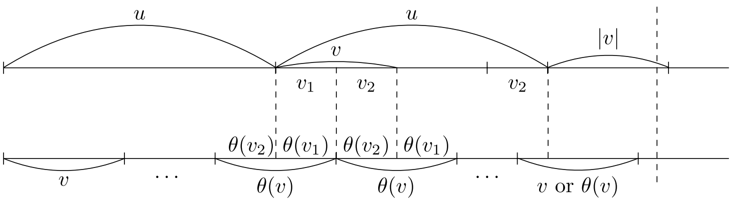

Fig. 9. The prefix of $u^2\alpha'(u, \theta(u))$ and $\beta(v, \theta(v))$ of length $2|u| + |v| - 1$.

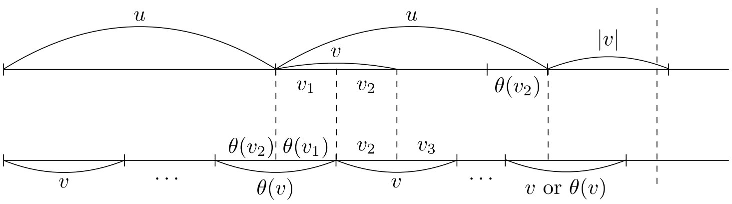

Fig. 10. The prefix of $u^2\alpha'(u, \theta(u))$ and $\beta(v, \theta(v))$ of length $2|u| + |v| - 1$.

$\mathrm{suff}_{|x|+2|xy|}(u) = xyxv_1$, and thus we obtain immediately that $xy = yx$. So, in this case there exists a primitive word $t \in \Sigma^+$, such that $v \in \{t\}^+$ and $u \in t\{t, \theta(t)\}^*$, i.e., $\rho_\theta(u) = \rho_\theta(v)$. Otherwise, there is a $\theta(v)$ to the left of the border-crossing v, i.e., $\mathrm{suff}_{|x|+2|xy|}(u) = yx\theta(x)v_1$. Thus, in this case we obtain that either $yx\theta(x) = xxy$ or $yx\theta(x) = \theta(x)xy$. However, in both cases, due to Theorems 19 and 20, we obtain $x, y \in \{t, \theta(t)\}^*$ for some $t \in \Sigma^+$, which immediately implies $\rho_\theta(v) = \rho_\theta(u)$.

Suppose next that $i = 0$, i.e., $v_1 = xy$, $v_3 = yx$, $v_2 = x$, $v = xyx$, and $\theta(yx) = yx$, as illustrated in Fig. 8. Now, if we compute the length of the first u, then we have $|u| = k|v| + |xy|$ for some $k \geq 1$. Since the second u starts with $v_2 = x$, we must have that its right end will fall inside either v or $\theta(v)$, after exactly $|y|$ characters. Now, we have two cases depending on what occurs to the left of this second border-crossing point.

First, if there is a v occurring before this border-crossing point, then $\mathrm{suff}_{2|xy|}(u) = xyxy$. Next, we turn again to look at the suffix of the first u. Depending on whether there is v or $\theta(v)$ to the left of the first border-crossing v, we have $\mathrm{suff}_{2|xy|}(u) \in \{yxxy, \theta(y)\theta(x)xy\}$. Thus, either $yx = xy$ or $\theta(xy) = xy$. However, since also $\theta(yx) = yx$, we obtain that either $x, y \in \{t\}^*$ or $x, y \in \{t, \theta(t)\}^*$ for some $t \in \Sigma^+$, and thus $\rho_\theta(u) = \rho_\theta(v)$.

Second, if $\theta(v) = \theta(x)\theta(y)\theta(x)$ occurs to the left of the second border-crossing point, since $\mathrm{suff}_{|xy|}(u) = v_1 = xy$, then we obtain immediately that $x = \theta(x)$. But, we already knew that $yx = \theta(yx)$, i.e., $yx = x\theta(y)$, which implies $x = p(qp)^j$ and $y = (pq)^k$ for some $j \geq 0$, $k \geq 1$, and some words p and q such that $p = \theta(p)$ and $q = \theta(q)$, see [1]. Now, since $\alpha(u, \theta(u))$ and $\beta(v, \theta(v))$ have a common prefix of length $2|u| + |v| - \gcd(|u|, |v|) = 2|u| + |v| - 1$, we can also look at the prefix of length $|v| - 1$ of the third word from $\alpha(u, \theta(u))$, which is either u or $\theta(u)$. However, in all cases, after we reduce the common prefix, we have two distinct expressions over p and q of length longer than $|p| + |q|$, which implies, due to Corollary 5, that $pq = qp$. Thus, also in this case $\rho_\theta(u) = \rho_\theta(v)$.

Case 2: Consider now the case when the border between the first two u's falls inside $\theta(v)$. If this border-crossing $\theta(v)$ is followed to the right by another $\theta(v)$, as illustrated in Fig. 9, then there exist some $v_1, v_2 \in \Sigma^+$ such that $v = v_1v_2$, $v_1 = \theta(v_1)$, and $v_2 = \theta(v_2)$. Thus, obviously $v, \theta(v), u, \theta(u) \in \{v_1, v_2\}^+$, i.e., $\alpha(u, \theta(u))$ and $\beta(v, \theta(v))$ are actually two expressions over $\{v_1, v_2\}$ having a common prefix of length $2|u| + |v| - \gcd(|u|, |v|) = 2|u| + |v| - 1$. Moreover, since $|u| = k|v| + |v_2|$ for some $k \geq 1$ and the second u begins with v_1, its right end cuts a v or $\theta(v)$ after exactly $(2|v_2| \bmod |v|) \neq |v_2|$ characters. Thus, the two expressions over $\{v_1, v_2\}$ have to differ at some point, and moreover, after we eliminate the common prefix we remain with two distinct expressions over v_1 and v_2 of length longer than $|v_1| + |v_2|$, which implies, due to Corollary 5, that $v_1v_2 = v_2v_1$. Thus, also in this case $\rho_\theta(u) = \rho_\theta(v)$.

Hence, the border-crossing $\theta(v)$ is followed to the right by v, as illustrated in Fig. 10. Then, we can write $v = v_1v_2 = v_2v_3$ for some $v_1, v_2, v_3 \in \Sigma^+$ with $|v_1| = |v_3|$ and $v_1 = \theta(v_1)$. Thus, due to Theorem 6, there exist some words $x, y \in \Sigma^*$ and some $i \geq 0$ such that $v_1 = xy$, $v_3 = yx$, $v_2 = (xy)^ix$, and $v = (xy)^{i+1}x$. Again, if either $x = \epsilon$ or $y = \epsilon$, then we obtain immediately that $\rho_\theta(u) = \rho_\theta(v)$. So, from now on, we can suppose that $x, y \in \Sigma^+$. Moreover, since u ends with $\theta(v_2)$, we also know that $\theta(u)$ starts with $v_2 = (xy)^ix$.

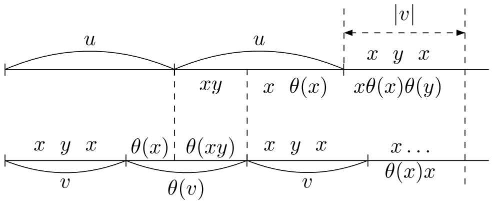

Fig. 11. The prefixes of $u^2\alpha'(u,\theta(u))$ and $\beta(v,\theta(v))$ of length $2|u|+|v|$.

Suppose first that $i \geq 1$. Then, the length of the first u is $|u| = k|v| + |v_2| = k|v| + i|xy| + |x|$ for some $k \geq 1$. Since the second u starts with $\theta(v_1) = xy$, its right end will cut either v or $\theta(v)$ after exactly $|x| + (i-1)|xy|$ characters. If this second border point falls inside v, since both u and $\theta(u)$ start with xy, we obtain $xy = yx$. That is, there exists a primitive word $t \in \Sigma^+$ such that $x, y, v \in \{t\}^+$ and $u \in t\{t, \theta(t)\}^*$, i.e., $\rho_\theta(u) = \rho_\theta(v)$. Otherwise, this second border point cuts $\theta(v) = \theta(x)(xy)^{i+1}$ after exactly $|x| + (i-1)|xy|$ characters. Then, since u ends with $\theta(v_2) = \theta(x)(xy)^i$, depending on whether to the left of this second border-crossing $\theta(v)$ we have either v or $\theta(v)$, we obtain either $yx\theta(x) = \theta(x)xy$ or $xy\theta(x) = \theta(x)xy$. In the first case, Theorem 19 implies $x, y \in \{t, \theta(t)\}^*$ for some $t \in \Sigma^+$, while in the latter one we obtain $x = \theta(x)$ and $\rho(x) = \rho(y)$. Since $v = (xy)^{i+1}x$ and $u = \beta'(v, \theta(v))\theta(v_2)$, we conclude again that $\rho_\theta(u) = \rho_\theta(v)$.

Otherwise, we have $i = 0$, i.e., $v_1 = xy$, $v_3 = yx$, $v_2 = x$, $v = xyx$, and $\theta(v) = \theta(x)xy$. Using length arguments again, we notice that the right end of the second u cuts either v or $\theta(v)$ after exactly $2|x|$ characters.

Let us look first at the case when this second border point falls inside $\theta(v)$. Then $x = \theta(x)$, as u ends with $\theta(v_2) = \theta(x)$. Since $\alpha(u, \theta(u))$ and $\beta(v, \theta(v))$ have a common prefix of length $2|u| + |v| - \gcd(|u|, |v|) = 2|u| + |v| - 1$, we can also look at the prefix of length $|v| - 1$ of the third word from $\alpha(u, \theta(u))$, which is either u or $\theta(u)$. Since u ends with $\theta(v_2) = \theta(x)$, we know that both u and $\theta(u)$ start with x. Furthermore, since $\theta(xy) = xy$, we actually have two distinct expressions over $\{x, y\}^+$, one starting with x and the other with y, having a common prefix longer than $|x| + |y|$, implying, due to Corollary 5, that $xy = yx$. So, also in this case $\rho_\theta(u) = \rho_\theta(v)$.

Next, we turn to the case when the second border point falls inside v and we analyze two cases depending on the length of u. Firstly, if $|u| > 2|v|$, then the first u starts either with v^2 or with $v\theta(v)$ and we look at the prefix of the second u, see Fig. 10. In the former case, we obtain immediately that $xy = yx$, which implies that there exists a primitive word $t \in \Sigma^+$ such that $x, y, v \in \{t\}^+$ and $u \in t\{t, \theta(t)\}^*$, i.e., $\rho_\theta(u) = \rho_\theta(v)$. In the latter case, we obtain $yx = \theta(yx)$, which together with $xy = \theta(xy)$ implies, due to Corollary 22, that $x, y \in \{t, \theta(t)\}^*$ for some $t \in \Sigma^+$, and thus also $\rho_\theta(u) = \rho_\theta(v)$.

Second, if $|u| < 2|v|$, then we actually must have $u = v\theta(v_2) = xyx\theta(x)$, as illustrated in Fig. 11. Since $\alpha(u, \theta(u))$ and $\beta(v, \theta(v))$ have a common prefix of length $2|u|+|v|-1$, after eliminating the common prefix, we obtain one of the following four equations, depending on whether the third block of $\alpha(u, \theta(u))$ is u or $\theta(u)$, and the fourth block of $\beta(v, \theta(v))$ is v or $\theta(v)$.

- If we have $\theta(x)xy\ \mathrm{pref}_{|x|-1}(x) = yxx\ \mathrm{pref}_{|x|-1}(yx)$, then $\mathrm{pref}_{|x|}(yx) = \theta(x)$, and thus we obtain $\mathrm{pref}_{|x|-1}(x) = \mathrm{pref}_{|x|-1}(\theta(x))$. Now, if we denote $x = x_1 \ldots x_n$ with $x_1, \ldots, x_n \in \Sigma$, then the equation $\mathrm{pref}_{|x|-1}(x) = \mathrm{pref}_{|x|-1}(\theta(x))$ becomes $x_1 \ldots x_{n-1} = \theta(x_n) \ldots \theta(x_2)$. Depending on whether $|x|$ is even or odd, this equality implies $x = x_1 \ldots x_k\theta(x_1 \ldots x_k)$ or $x = x_1 \ldots x_k x_{k+1}\theta(x_1 \ldots x_k)$ with $x_{k+1} = \theta(x_{k+1})$. However, on both cases, we obtain $x = \theta(x)$. Then, from the initial equation $\theta(x)xy\ \mathrm{pref}_{|x|-1}(x) = yxx\ \mathrm{pref}_{|x|-1}(yx)$ we obtain $x^2y = yx^2$, which implies $\rho(x) = \rho(y)$. Hence, also $\rho_\theta(u) = \rho_\theta(v)$.
- If $\theta(x)xy = yx\theta(x)$, then, due to Theorem 19, we immediately obtain $x, y \in \{t, \theta(t)\}^*$ for some $t \in \Sigma^+$, and thus $\rho_\theta(u) = \rho_\theta(v)$.
- If $\theta(x)x\ \mathrm{pref}_{|xy|-1}(\theta(x)\theta(y)) = yxx\ \mathrm{pref}_{|x|-1}(yx)$, then we can write $yx = \theta(x)z$ for some word $z \in \Sigma^+$ with $|z| = |y|$. If we substitute this equation into the initial one, we obtain $x\theta(z)\ \mathrm{pref}_{|x|-1}(x) = zx\ \mathrm{pref}_{|x|-1}(\theta(x))$, which implies that $x_1 \ldots x_{n-1} = \theta(x_n) \ldots \theta(x_2)$, where $x = x_1 \ldots x_n$ with $x_1, \ldots, x_n \in \Sigma$. Just as before we can again derive $x = \theta(x)$. Since $xy = \theta(xy)$, we can write $xy = \theta(y)x$ which implies that $x = p(qp)^j$ and $y = (qp)^k$, for some $j \geq 0$, $k \geq 1$, and some words p and q such that $p = \theta(p)$ and $q = \theta(q)$, see [1]. Then, using these relations, the initial equation becomes a nontrivial identity over p and q of length more than $|p| + |q|$. Thus, due to Corollary 5, there exists a primitive word t such that $p, q, x, y \in \{t\}^+$. So, $\rho_\theta(u) = \rho_\theta(v)$.
- If $\theta(x)x\ \mathrm{pref}_{|xy|-1}(\theta(x)\theta(y)) = yx\theta(x)\ \mathrm{pref}_{|x|-1}(x)$, then we can write again $yx = \theta(x)z$ for some word $z \in \Sigma^+$ with $|z| = |y|$. Thus, the initial equation becomes $x\theta(z) = z\theta(x)$. If in the equation $xy = \theta(y)\theta(x)$ we concatenate $x\theta(x)$ both to the left and to the right, then we derive $x\theta(x)xyx\theta(x) = x\theta(yx)\theta(x)x\theta(x)$. Substituting $yx = \theta(x)z$ and $\theta(yx) = \theta(z)x$, we derive $x\theta(x)x\theta(x)z\theta(x) = x\theta(z)x\theta(x)x\theta(x)$. Now, since $x\theta(z) = z\theta(x)$, this becomes $(x\theta(x))^2x\theta(z) = x\theta(z)(x\theta(x))^2$, which implies that there exists a primitive word $t \in \Sigma^+$ such that $x\theta(x), x\theta(z) \in \{t\}^*$. If $x\theta(x) = t^{2j}$ for some $j \geq 0$, then $x = \theta(x) = t^j$, $t = \theta(t)$, $z, y \in \{t\}^*$, and thus $\rho_\theta(u) = \rho_\theta(v)$. If $x\theta(x) = t^{2j+1}$ for some $j \geq 1$, then we actually have $x = t^jt_1$, $\theta(x) = \theta(t_1)t^j$, and $\theta(z) = \theta(t_1)t^k$ where $t = t_1\theta(t_1)$ and $k \geq 0$. Now, from the equation $yx = \theta(x)z$ we also obtain that $y \in \{t_1, \theta(t_1)\}^+$. So, also in this case we can conclude that $\rho_\theta(u) = \rho_\theta(v)$. $\square$

Next, let us look at the case when $\alpha(u, \theta(u))$ starts with $u\theta(u)u$.

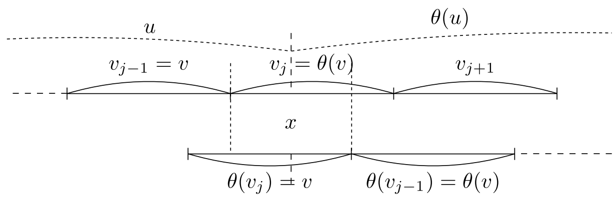

Fig. 12. The case where n is even, $v_{j-1} = v$, $v_j = \theta(v)$, and $v_{j+1} = v$.

Theorem 28. *Given two words $u, v \in \Sigma^+$ with $|u| > |v|$, if there exist two θ-powers $\alpha(u, \theta(u)) \in u\{u, \theta(u)\}^*$ and $\beta(v, \theta(v)) \in v\{v, \theta(v)\}^*$ having a common prefix of length at least $2|u|+|v|-\gcd(|u|, |v|)$ and, moreover, $\alpha(u, \theta(u)) = u\theta(u)u\alpha'(u, \theta(u))$ with $\alpha'(u, \theta(u)) \in \{u, \theta(u)\}^*$, then $\rho_\theta(u) = \rho_\theta(v)$.*

Proof. Let us suppose again, just as we did before, that $\gcd(|u|, |v|) = 1$. If we denote $u' = u\theta(u)$, then $u'u'$ and $\beta(v, \theta(v))$ have a common prefix of length $|u'|+|v|-\gcd(|u'|, |v|) = |u'|+|v|-1$ and, moreover, $u' = \theta(u')$. Thus, due to Theorem 26, $\rho_\theta(v) = \rho_\theta(u')$; let this θ-primitive root be t. Then, $u\theta(u) = \gamma(t, \theta(t))$, for some θ-power $\gamma(t, \theta(t)) \in t\{t, \theta(t)\}^+$, which implies, due to Theorem 14, that $\rho_\theta(u) = t = \rho_\theta(v)$. $\square$

The only case which remains to be considered now is when $\alpha(u, \theta(u))$ starts with $u\theta(u)\theta(u)$. Next, we give two intermediate results concerning θ-palindromic words, which will be very helpful in the proof of Theorem 31.

Lemma 29. *Let $w \in \Sigma^+$ and x, y, z be θ-palindromes. If $w = xy = yz$, then there exists a θ-palindromic primitive word $p \in \Sigma^+$ such that $w, x, y, z \in \{p\}^+$.*

Proof. Since $w = xy$ with $x = \theta(x)$ and $y = \theta(y)$, we know from [15], that there exist two θ-palindrome words p, q and an integer $n \geq 1$ such that $w = (pq)^n$, where pq is a primitive word, $p \neq \epsilon$, $x = (pq)^i p$, $y = q(pq)^{n-i-1}$, $y = (pq)^j p$, and $z = q(pq)^{n-j-1}$ for some integers $0 \leq i, j < n$. If $n - i - 1, j \geq 1$, then $pq, qp \in \mathrm{Pref}(y)$, i.e., $pq = qp$. Since pq is primitive, this means that $q = \epsilon$. Therefore, p is a primitive word and $w, x, y, z \in \{p\}^+$. If $n-i-1 \geq 1$ and $j = 0$, then $q(pq)^{n-i-1} = p$, which implies that $n-i-1 = 1$ and hence $q = \epsilon$, and we reached the same conclusion as above. If $n-i-1 = 0$ and $j \geq 1$, then $q = (pq)^j p$, which cannot hold for any $j \geq 1$ because $p \neq \epsilon$. If both $n - i - 1$ and j are 0, then $p = q$, which contradicts the primitivity of pq. $\square$

Lemma 30. *Let $w \in \Sigma^+$ and x, y, z be θ-palindromes. If $w = xy^2 = yz$, then there exists a θ-palindrome primitive word $p \in \Sigma^+$ such that $w, x, y, z \in \{p\}^+$.*

Proof. Since $w = yz$ with $y = \theta(y)$ and $z = \theta(z)$, we know from [15], that there exist two θ-palindrome words p, q and an integer $n \geq 1$ such that $w = (pq)^n$, where pq is a primitive word, $p \neq \epsilon$, $x = (pq)^i p$, $y^2 = q(pq)^{n-i-1}$, $y = (pq)^j p$, and $z = q(pq)^{n-j-1}$ for some integers $0 \leq i, j < n$. If $n - i - 1, j \geq 1$, then, just as in the proof of Lemma 29, $pq = qp$. Since pq is primitive, $q = \epsilon$, and hence p is primitive and $x, y, z \in \{p\}^+$. If $n-i-1 \geq 1$ and $j = 0$, then $y = p$. Since $y^2 = q(pq)^{n-i-1}$, we have that $p^2 = q(pq)^{n-i-1}$, which means, due to Theorem 3, that $p, q \in \{t\}^*$ for some primitive word t. Since pq is primitive, this implies that $q = \epsilon$, $p = t$, and $x, y, z \in \{p\}^+$. If $n - i - 1 = 0$ and $j \geq 1$, then $y^2 = q$ and $y = (pq)^j p$, which are clearly contradictory. If both $n - i - 1$ and j are 0, then $y^2 = q$ and $y = p$, which contradicts the primitivity of pq. $\square$

Now, we can state the following result which considers the last case of our analysis.

Theorem 31. *Let $u, v \in \Sigma^+$ be two words with $|u| > |v|$. If there exist two θ-powers $\alpha(u, \theta(u)) \in u\theta(u)^2\{u, \theta(u)\}^*$ and $\beta(v, \theta(v)) \in v\{v, \theta(v)\}^*$ having a common prefix of length at least $2|u| + |v| - \gcd(|u|, |v|)$, then $\rho_\theta(u) = \rho_\theta(v)$.*

Proof. Once again, we can suppose that $\gcd(|u|, |v|) = 1$ without loss of generality. If $v \in \Sigma$, then trivially $u \in v\{v, \theta(v)\}^*$, i.e., $\rho_\theta(u) = \rho_\theta(v)$. So, we can suppose next that $|v| \geq 2$ and thus, since $\gcd(|u|, |v|) = 1$, the end of both of u and $u\theta(u)$ falls inside either v or $\theta(v)$. Let $\beta(v, \theta(v)) = v_1 v_2 \dots v_n v_{n+1} v_{n+2} \beta'(v, \theta(v))$ with $v_1 = v$, $v_i \in \{v, \theta(v)\}$ for all $2 \leq i \leq n+2$, and $\beta'(v, \theta(v)) \in \{v, \theta(v)\}^*$ such that the end of $u\theta(u)$ falls inside v_{n+1}. Let $u\theta(u) = v_1 \cdots v_n v'$, where $v' \in \mathrm{Pref}(v_{n+1})$. Note that since $u\theta(u)$ is a θ-palindrome, $u\theta(u) = \theta(v')\theta(v_n) \cdots \theta(v_1)$. Moreover, the end of u falls inside $v_{(n+2)/2}$ if n is even and inside $v_{(n+1)/2}$ if n is odd. So, from now on we take $j = \frac{n+2}{2}$ whenever n is even and $j = \frac{n+1}{2}$ otherwise, i.e., j is chosen such that the border between u and $\theta(u)$ falls inside v_j.

Let us consider first the case when n is even. Then x, a prefix of v_j, overlaps with a suffix of $\theta(v_j)$, see Fig. 12, and the overlap implies $x = \theta(x)$. Note that x is a nonempty and proper prefix of v_j.

Now we focus on v_{j-1}, v_j, and v_{j+1}. Even if $j = n$, we can consider $v_{j+1} = v_{n+1} \in \{v, \theta(v)\}$. Suppose $v_{j-1}v_j = v\theta(v)$. If $v_{j+1} = \theta(v)$, then $\theta(v)^2 = x\theta(v)x'$ for some $x' \in \Sigma^+$. This means that $x, \theta(v) \in \{t\}^+$ for some primitive word t. Since $u\theta(u) = v_1 \cdots v_{j-1} x \theta(v_{j-1}) \cdots \theta(v_1)$, we obtain that $u, v \in \{t, \theta(t)\}^+$. But $v \in \mathrm{Pref}(u)$, which implies $\rho_\theta(u) = \rho_\theta(v)$. Otherwise, $v_{j+1} = v$. Then $v\theta(v)w = wv\theta(v)$ holds for $w \in \mathrm{Pref}(v)$ with $|w| = |x|$, which implies, due to Theorem 18, that $\rho_\theta(v) = \rho_\theta(w) = t$. Then $x \in \{t, \theta(t)\}^+$, and hence $\rho_\theta(u) = \rho_\theta(v)$. The case when $v_{j-1}v_j = \theta(v)v$ also leads to the same conclusion.

Thus, when n is even, only the cases where $v_{j-1}v_j = vv$ or $v_{j-1}v_j = \theta(v)\theta(v)$ remain unsolved yet. Moreover, using exactly the same technique, we can also prove that when n is odd, all we have to consider are the cases when $v_j v_{j+1} = vv$

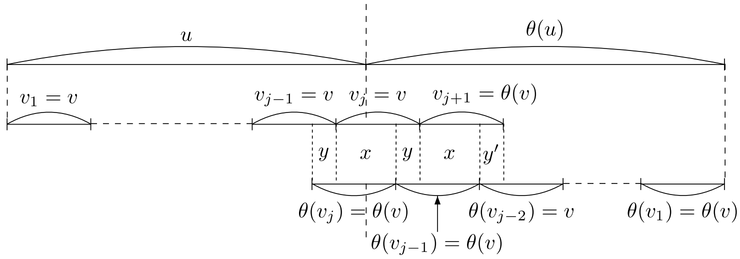

Fig. 13. The case n being even, $v_{j-1} = v_j = v$, $v_{j+1} = \theta(v)$, and $\theta(v_{j-2}) = v$.

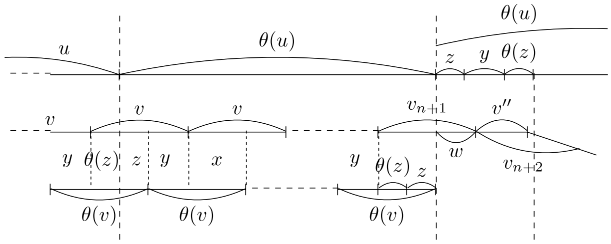

Fig. 14. The case when n is even and $v_1 = \cdots = v_n = v$.

or $v_jv_{j+1} = \theta(v)\theta(v)$. Although we shall discuss only the case when n is even, a similar result can also be obtained for n odd. Assume that n is even, $v_{j-1}v_j = vv$, and let $v_j = v = xy$ such that $y \in \text{Pref}(\theta(v_{j-1}))$, as illustrated in Fig. 13. Then we have $x = \theta(x)$ and $y = \theta(y)$.

Next, we claim that once assuming $v_{j-1}v_j = vv$, we only need to consider the case when $v_1v_2\dots v_n = v^n$, that is, in all the other cases, we obtain $\rho_\theta(u) = \rho_\theta(v)$. If $j = n$, then we are done. Otherwise, i.e., $j < n$, since $j = (n+2)/2$ we have $n > 2$, and hence also $j > 2$. Thus we can also consider v_{j-2}. Suppose first that $v_{j+1} = \theta(v)$. If $\theta(v_{j-2}) = \theta(v)$, then the nontrivial overlap between $\theta(v)^2$ and $\theta(v)$ implies that $\rho(y) = \rho(x) = \rho(\theta(v))$, which, as shown earlier, leads to $\rho_\theta(u) = \rho_\theta(v)$. Otherwise, let $\theta(v_{j-2}) = v$, as illustrated in Fig. 13. Then, let $v_{j+1} = \theta(v) = xy'$ for some $y' \in \text{Pref}(v)$, which implies that $y' = \theta(y')$. Therefore, $v = xy = y'x$, which implies, due to Lemma 29, that $v, x \in \{t\}^+$ for some $t \in \Sigma^+$ and hence $\rho_\theta(u) = \rho_\theta(v)$.

Now suppose that $v_{j+1} = v$, and we consider $\theta(v_{j-2})$. If $j+1 = n$, then $j-2 = 1$ and thus $v_{j-2} = v_1 = v$, i.e., $v_1v_2\dots v_n = v^n$. Otherwise, i.e., $j+1 < n$, suppose $\theta(v_{j-2}) = v$. Moreover, since $j+1 < n$, we can also consider v_{j+2}. But then, independently of whether v_{j+2} is v or $\theta(v)$ we obtain $\rho_\theta(u) = \rho_\theta(v)$. Repeating the whole process leaves only the case $v_{j+1} = v_{j+2} = \cdots = v_n = v$ and $\theta(v_{j-2}) = \theta(v_{j-3}) = \cdots = \theta(v_1) = \theta(v)$ unsolved. That is, when we assume $v_{j-1}v_j = vv$, all we have to consider is the case when $v_1v_2\dots v_n = v^n$. On the other hand, if we start with the assumption that $v_{j-1}v_j = \theta(v)^2$, then the only case remaining to be proved is when $v_1 = v$ and $v_2 = \cdots = v_n = \theta(v)$; in all the other cases, using similar techniques as before, we obtain that $\rho_\theta(u) = \rho_\theta(v)$. However, also in this case, independently of whether v_{n+1} is v or $\theta(v)$, we can conclude that $\rho_\theta(u) = \rho_\theta(v)$. Moreover, using similar arguments as above, if n is odd, then the only case which remains to be solved is $u\theta(u) = v^nv'$. Therefore, independently of the parity of n, the only case we have to consider is when $u\theta(u) = v^nv'$.

Let us look first at the case when n is even. If $v = xy$, as illustrated in Fig. 14, then $u\theta(u) = v^nv' = v^{n/2}x\theta(v)^{n/2}$ with $|v'| = |x|$. But, this actually means that $v' = x$ since $\theta(v) = yx$. Moreover, x can be written as $x = \theta(z)z$ for some $z \in \Sigma^+$. So, the prefix of $\theta(u)$ of length $|v|$ is $zy\theta(z)$. Let $v^nv_{n+1}v'' = \text{pref}_{2|u|+|v|-1}(\beta(v, \theta(v)))$ with $v'' \in \text{Pref}(v_{n+2})$, and $v_{n+1} = \theta(z)zw$ for some $w \in \Sigma^+$.

First, we consider the case $v_{n+1} = \theta(v)$. Since $\theta(z) \in \text{Pref}(v_{n+1})$, $\theta(z)$ is a prefix of both v and $\theta(v)$. Note that $|v''| = 2|z| - 1$ and hence $\theta(z) \in \text{Pref}(v'')$. If $|y| \geq |z|$, then $\theta(z) \in \text{Pref}(y)$, i.e., $z \in \text{Suff}(y)$ because $v_{n+1} = y\theta(z)z$ and $\theta(z) \in \text{Pref}(v_{n+1})$. In Fig. 14, y and v'' overlap with the overlapped part of length $|z|$ so $z = \theta(z)$. Then from the equation $v_{n+1}\theta(z) = \theta(z)zzy = y\theta(z)z\theta(z)$ we derive $z^3y = yz^3$. This means that $\rho(y) = \rho(z)$, and thus $\rho_\theta(u) = \rho_\theta(v)$. Otherwise, i.e., $|y| < |z|$, we have $zy = w\theta(z)$. Then, $z = wt$ and $\theta(z) = ty$ for some $t \in \Sigma^+$, which implies that $w = y = \theta(y)$. Hence $\theta(v) = y\theta(z)z = \theta(z)zy$, which implies, due to Theorem 18 that $\rho_\theta(y) = \rho_\theta(\theta(z))$, and hence $\rho_\theta(u) = \rho_\theta(v)$.

Next we consider the case when $v_{n+1} = v$. If $v_{n+2} = v$, then Theorem 8 immediately implies that $\theta(u)$ and a conjugate of v, that is, $zy\theta(z)$ share the primitive root t. Since $\theta(u) = (zy\theta(z))^{j-1}z$, $z \in \{t\}^+$, and hence $t = \theta(t)$ and $y, \theta(z) \in \{t\}^+$. Thus, $u, v \in \{t\}^+$, and hence $\rho_\theta(u) = \rho_\theta(v)$. Otherwise let $v_{n+2} = \theta(v) = y\theta(z)z$. Now, we have two subcases, depending on the lengths of y and z. First, if $|z| \leq |y|$, then $\text{pref}_{|z|}(v'') \in \text{Pref}(y)$, and hence $zy \in \text{Pref}(y^2)$. Hence $\rho(y) = \rho(z)$, implying that $\rho_\theta(u) = \rho_\theta(v)$. Second, if $|y| < |z|$, then since $y \in \text{Pref}(z)$ we also have $y \in \text{Suff}(\theta(z))$. Thus, $\text{pref}_{|z|-1}(\theta(z)) \in y\text{Pref}(z)$, as illustrated in Fig. 15. Moreover, since $zy^2 = y^2\theta(z)$, we actually have two distinct expressions over $\{y, z\}^+$, one starting with y and the other with z, having a common prefix of length at least $|y| + |z|$. Then, due to Corollary 5, we obtain $\rho(y) = \rho(z)$, which implies $\rho_\theta(u) = \rho_\theta(v)$.

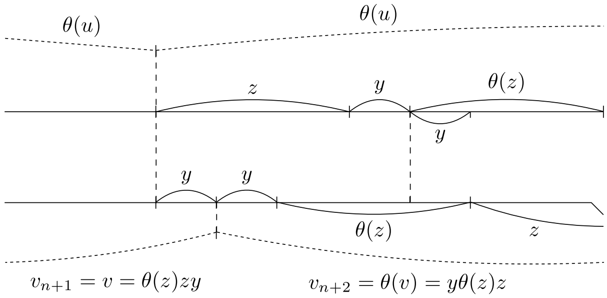

Fig. 15. The case when n is even and $|y| < |z|$.

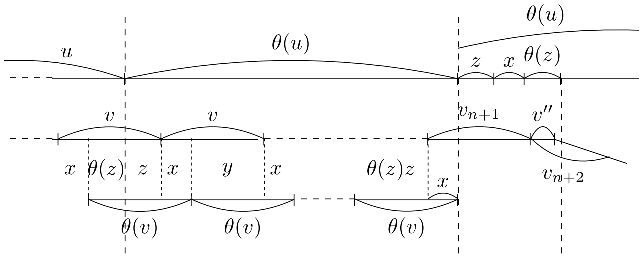

Fig. 16. The case when n is odd and $v_1 = \cdots = v_n = v$.

Next we consider the case when n is odd and $v_1 = \cdots = v_n = v$, see Fig. 16. Let $v = xy$ such that $x = \theta(x)$, $y = \theta(y)$, and $y = \theta(z)z$ for some $x, y, z \in \Sigma^+$. Then $u\theta(u) = v^{(n-1)/2}x\theta(z)zx\theta(v)^{(n-1)/2}$.

If $v_{n+1} = \theta(v)$, then x is a prefix of both v and $\theta(v)$ and thus $v'' = \mathrm{pref}_{|x|-1}(x)$. Hence we have $xzxz_s = v_{n+1}v'' = \theta(z)zxv''$ for some $z_s = \mathrm{pref}_{|z|-1}(\theta(z))$. Depending on the lengths of x and z, we have the following four subcases. Let us consider the first subcase when $|x| = |z|$. Then immediately we have $x = \theta(z)$, and we are done, i.e., obviously $\rho_\theta(u) = \rho_\theta(v)$. The second subcase is when $|x| > |z|$. Then, $xzxz_s = \theta(z)zxv''$ implies that x overlaps non-trivially with xv''. Since $v'' \in \mathrm{Pref}(x)$ and x is a θ-palindrome, we can write $x = x_1x_2 = x_2x_1$ for some θ-palindromes x_1, x_2, where, moreover $x_2 = \theta(z)$. This implies that $x_1, x_2, x \in \{t\}^+$ for some $t \in \Sigma^+$, and hence $\theta(z), z, x \in \{t, \theta(t)\}^+$. Since $u, v \in \{\theta(z), z, x\}^+$, we have $\rho_\theta(u) = \rho_\theta(v)$. The third subcase is when $|x| < |z| \le 2|x|$. Let $\theta(z) = xz_p$ for some $z_p \in \mathrm{Pref}(z)$, which implies $z_p = \theta(z_p)$. Thus, $z = z_px$. Since $xz \in \mathrm{Pref}(\theta(z)z)$, i.e., $xz_px \in \mathrm{Pref}(xz_pz_px)$ and $|z_p| \le |x|$, we have $z_p \in \mathrm{Pref}(x)$. Now since $\theta(z)z \in \mathrm{Pref}(xzx)$, we have $\theta(z)z = xz_pxz_p$, i.e., $z = xz_p$. Therefore, $z = xz_p = z_px$, which implies $\rho(z) = \rho(x)$ and we obtain again $\rho_\theta(u) = \rho_\theta(v)$. The fourth subcase is when $2|x| < |z|$. As in the third subcase, $\theta(z) = xz'_p$ for some θ-palindrome z'_p. Since $xzx \in \mathrm{Pref}(\theta(z)z)$ holds in this case, let $\theta(z)z = xzxz'_s$ for some $z'_s \in \mathrm{Pref}(\theta(z))$. By substituting $z = z'_px$ into this equation, we obtain $z = x^2z'_s$. Then $z'_s = \theta(z'_s)$. Hence, $z = z'_px = x^2z'_s$, which implies, due to Lemma 30, that $\rho(x) = \rho(z)$ and hence $\rho_\theta(u) = \rho_\theta(v)$.

Finally we consider the case $v_{n+1} = v = x\theta(z)z$. Then, as illustrated in Fig. 16, $z = \theta(z)$ and thus $v_{n+1} = xz^2$. If $v_{n+2} = v$, then as above, we can employ Theorem 8 to conclude that $\rho_\theta(u) = \rho_\theta(v)$. Otherwise, $v_{n+2} = \theta(v) = z^2x$. Now we have four subcases depending on the lengths of x and z. The first subcase is when $|x| \le |z|$. Note that $z^2 \in \mathrm{Pref}(zx\theta(z))$. Hence $z = xz_s$ for some $z_s \in \mathrm{Pref}(\theta(z))$, which implies that $z_s = \theta(z_s)$. Since $z = \theta(z)$, $z = xz_s = z_sx$. This means $\rho(x) = \rho(z)$ and we obtain again $\rho_\theta(u) = \rho_\theta(v)$. The second subcase is when $|z| < |x| \le 2|z|$. Since $|v''| = |x| - 1$ and v'' is a prefix of $v_{n+2} = z^2x$, we have that $z \in \mathrm{Pref}(v'')$. Then, $z^3 \in \mathrm{Pref}(zx\theta(z))$, and we can conclude $\rho(x) = \rho(z)$ as done in the first subcase. Thus, $\rho_\theta(u) = \rho_\theta(v)$. The third subcase is when $2|z| < |x| \le 3|z|$. Then, we actually have $z^2 \in \mathrm{Pref}(v'')$. Thus, $z^4 \in \mathrm{Pref}(zx\theta(z))$ and again we have $\rho(x) = \rho(z)$, and hence $\rho_\theta(u) = \rho_\theta(v)$. The last subcase is when $3|z| < |x|$. Recall that $v_{n+2} = z^2x$. Since $x = \theta(x)$, we can rewrite this as $v_{n+2} = z^2\theta(x)$. As $|v''| = |x| - 1$, this means that $v'' = z^2x_1$ for some $x_1 \in \mathrm{Pref}(\theta(x))$ satisfying $|x_1| = |x| - 2|z| - 1$, which is positive. Since $zx \in \mathrm{Pref}(z^2v'')$, there exists $x_2 \in \mathrm{Pref}(x_1)$ such that $zx = z^4x_2$, i.e., $x_2 \in \mathrm{Suff}(x)$. However, since $x_2 \in \mathrm{Pref}(\theta(x))$, we obtain $x_2 = \theta(x_2)$. Thus, $x = z^3x_2 = x_2z^3$, which implies, due to Lemma 29, that $\rho(x) = \rho(z)$, so we conclude again that $\rho_\theta(u) = \rho_\theta(v)$. $\square$

Example 8. Let $\theta : \{a, b\}^* \to \{a, b\}^*$ be the mirror involution, $u = a^2ba^3b$, and $v = a^2ba$. Then, $\gcd(|u|, |v|) = 1$, u^3 and $v^2\theta(v)^2v$ have a common prefix of length $2|u| + |v| - 2$, but $\rho_\theta(u) \ne \rho_\theta(v)$.

Example 9. Let $\theta : \{a, b\}^* \to \{a, b\}^*$ be the mirror involution, $u = ba^2baba$, and $v = ba^2ba$. Then, $\gcd(|u|, |v|) = 1$, $u\theta(u)^2$ and v^4 have a common prefix of length $2|u| + |v| - 2$, but $\rho_\theta(u) \ne \rho_\theta(v)$.

Combining all results obtained in this section together, we have the extended Fine and Wilf theorem for an antimorphic involution θ:

Corollary 32. *Let $u, v \in \Sigma^*$ be two words with $|u| > |v|$. If there exist two θ-powers $\alpha(u, \theta(u)) \in u\{u, \theta(u)\}^*$ and $\beta(v, \theta(v)) \in v\{v, \theta(v)\}^*$ having a common prefix of length $2|u| + |v| - \gcd(|u|, |v|)$, then $\rho_\theta(u) = \rho_\theta(v)$. Furthermore, this bound is optimal.*

7. Conclusion

In this paper, we extended the notion of a primitive word, being motivated by encoding information into DNA molecules. Then we investigated various relations on words u, v (word equations, extended Fine and Wilf theorem) which imply $\rho_\theta(u) = \rho_\theta(v)$. A future research topic is to generalize the extended Fine and Wilf theorem as is being done for the original Fine and Wilf theorem (e.g., arbitrary number of periods, for partial words or bidimensional words). Another direction is to study relations on words which force some of the involved words to share their θ-primitive root (see [16]).

Acknowledgements

We gratefully acknowledge the anonymous reviewers for their constructive comments. This research was supported by Natural Sciences and Engineering Research Council of Canada Discovery Grant and Canada Research Chair Award to Lila Kari.

References

[1] L. Kari, K. Mahalingam, Watson–Crick conjugate and commutative words, in: Proc. of DNA 13, in: LNCS, vol. 4848, Springer-Verlag, Berlin, 2008, pp. 273–283.
[2] L. Kari, K. Mahalingam, Watson–Crick palindromes in DNA computing, Natural Computing doi:10.1007/s11047-009-9131-2.
[3] A. de Luca, A. De Luca, Pseudopalindrome closure operators in free monoids, Theoret. Comput. Sci. 362 (2006) 282–300.
[4] H.J. Shyr, G. Thierrin, Disjunctive languages and codes, in: Proc. FCT77, in: LNCS, vol. 56, Springer-Verlag, Berlin, Heidelberg, New York, 1977, pp. 171–176.
[5] M. Lothaire, Combinatorics on Words, in: Encyclopedia of Mathematics and its Applications, vol. 17, Addison-Wesley, 1983.
[6] C. Choffrut, J. Karhumäki, Combinatorics of words, in: G. Rozenberg, A. Salomaa (Eds.), in: Handbook of Formal Languages, vol. 1, Springer-Verlag, Berlin, Heidelberg, New York, 1997, pp. 329–438.
[7] N.J. Fine, H.S. Wilf, Uniqueness theorem for periodic functions, Proc. Amer. Math. Soc. 16 (1) (1965) 109–114.
[8] S.S. Yu, Languages and Codes, Tsang Hai Book Company Co., Taichung, Taiwan, 2005.
[9] J. Berstel, L. Boasson, Partial words and a theorem of Fine and Wilf, Theoret. Comput. Sci. 218 (1) (1999) 135–141.
[10] S. Constantinescu, L. Ilie, Generalized Fine and Wilf's theorem for arbitrary number of periods, Theoret. Comput. Sci. 339 (1) (2005) 49–60.
[11] S. Constantinescu, L. Ilie, Fine and Wilf's theorem for Abelian periods, Bull. EATCS 89 (2006) 167–170.
[12] F. Mignosi, A. Restivo, P. V. Silva, On Fine and Wilf's theorem for bidimensional words, Theoret. Comput. Sci. 292 (2003) 245–262.
[13] R. Tijdeman, L. Zamboni, Fine and Wilf words for any periods, Indag. Math. 14 (1) (2003) 135–147.
[14] R. Tijdeman, L. Zamboni, Fine and Wilf words for any periods ii, Theoret. Comput. Sci. 410 (2009) 3027–3034.
[15] L. Kari, K. Mahalingam, S. Seki, Twin-roots of words and their properties, Theoret. Comput. Sci. 410 (2009) 2393–2400.
[16] E. Czeizler, E. Czeizler, L. Kari, S. Seki, An extension of the Lyndon Schützenberger result to pseudoperiodic words, in: Proc. DLT09, in: LNCS, vol. 5583, Springer-Verlag, Berlin, 2009, pp. 183–194.