# On Two-Sided Infinite Fixed Points of Morphisms

Jeffrey Shallit* and Ming-wei Wang
Department of Computer Science
University of Waterloo
Waterloo, Ontario, Canada N2L 3G1
shallit@graceland.uwaterloo.ca
m2wang@neumann.uwaterloo.ca

March 31, 1999

**Abstract**

Let $\Sigma$ be a finite alphabet, and let $h : \Sigma^* \to \Sigma^*$ be a morphism. Finite and infinite fixed points of morphisms — i.e., those words $w$ such that $h(w) = w$ — play an important role in formal language theory. Head characterized the finite fixed points of $h$, and later, Head and Lando characterized the one-sided infinite fixed points of $h$. Our paper has two main results. First, we complete the characterization of fixed points of morphisms by describing all two-sided infinite fixed points of $h$, for both the "pointed" and "unpointed" cases. Second, we completely characterize the solutions to the equation $h(xy) = yx$ in finite words.

## 1 Introduction and definitions

Let $\Sigma$ be a finite alphabet, and let $h : \Sigma^* \to \Sigma^*$ be a morphism on the free monoid, i.e., a map satisfying $h(xy) = h(x)h(y)$ for all $x, y \in \Sigma^*$. If a word $w$ (finite or infinite) satisfies the equation $h(w) = w$, then we call $w$ a *fixed point* of $h$. Both finite and infinite fixed points of morphisms have long been studied in formal languages. For example, in one of the earliest works on formal languages, Axel Thue [21, 3] proved that the one-sided infinite word

$$\mathbf{t} = 0110100110010110\cdots$$

is overlap-free, that is, contains no subword of the form $axaxa$, where $a \in \{0, 1\}$, and $x \in (0 + 1)^*$. Define a morphism $\mu$ by $\mu(0) = 01$ and $\mu(1) = 10$. The word $\mathbf{t}$, now

*Research supported in part by a grant from NSERC.

called the Thue-Morse infinite word, is the unique one-sided infinite fixed point of $\mu$ which starts with 0. In fact, nearly every explicit construction of an infinite word avoiding certain patterns involves the fixed point of a morphism; for example, see [8, 15, 24, 20]. One-sided infinite fixed points of uniform morphisms also play a crucial role in the theory of automatic sequences; see, for example, [1].

Because of their importance in formal languages, it is of great interest to characterize *all* the fixed points, both finite and infinite, of a morphism $h$. This problem was first studied by Head [9], who characterized the finite fixed points of $h$. Later, Head and Lando [10] characterized the one-sided infinite fixed points of $h$. (For different proofs of these characterizations, see Hamm and Shallit [7].) In this paper we complete the description of all fixed points of morphisms by characterizing the *two-sided* infinite fixed points of $h$. Related work was done by Lando [14]. Two-sided infinite words (sometimes called *bi-infinite words* or *bi-infinite sequences*) play an important role in symbolic dynamics [16], and have also been studied in automata theory [18, 19], cellular automata [12], and the theory of codes [22, 5].

We first introduce some notation, some of which is standard and can be found in [11]. For single letters, that is, elements of $\Sigma$, we use the lower case letters $a, b, c, d$. For finite words, we use the lower case letters $t, u, v, w, x, y, z$. For infinite words, we use bold-face letters $\mathbf{t}, \mathbf{u}, \mathbf{v}, \mathbf{w}, \mathbf{x}, \mathbf{y}, \mathbf{z}$. We let $\epsilon$ denote the empty word. If $w \in \Sigma^*$, then by $|w|$ we mean the length of, or number of symbols in $w$. If $S$ is a set, then by Card $S$ we mean the number of elements of $S$. We say $x \in \Sigma^*$ is a *subword* of $y \in \Sigma^*$ if there exist words $w, z \in \Sigma^*$ such that $y = wxz$.

If $h$ is a morphism, then we let $h^j$ denote the $j$-fold composition of $h$ with itself. If there exists an integer $j \geq 1$ such that $h^j(a) = \epsilon$, then the letter $a$ is said to be *mortal*; otherwise $a$ is *immortal*. The set of mortal letters associated with a morphism $h$ is denoted by $M_h$. The *mortality exponent* of a morphism $h$ is defined to be the least integer $t \geq 0$ such that $h^t(a) = \epsilon$ for all $a \in M_h$. We write the mortality exponent as $\exp(h) = t$. It is easy to prove that $\exp(h) \leq$ Card $M_h$.

We let $\Sigma^\omega$ denote the set of all one-sided right-infinite words over the alphabet $\Sigma$. Most of the definitions above extend to $\Sigma^\omega$ in the obvious way. For example, if $\mathbf{w} = c_1 c_2 c_3 \cdots$, then $h(\mathbf{w}) = h(c_1)h(c_2)h(c_3)\cdots$. If $L \subseteq \Sigma^*$ is a language, then we define

$$L^\omega := \{w_1 w_2 w_3 \cdots \ : \ w_i \in L - \{\epsilon\} \text{ for all } i \geq 1\}.$$

Perhaps slightly less obviously, we can also define a limiting word $\vec{h^\omega}(a) := \lim_{n\to\infty} h^n(a)$ for a letter $a$, provided $h(a) = wax$ and $w \in M_h^*$. In this case, there exists $t \geq 0$ such that $h^t(w) = \epsilon$. Then we define

$$\vec{h^\omega}(a) := h^{t-1}(w) \cdots h(w)\, w\, a\, x\, h(x)\, h^2(x) \cdots ,$$

which is infinite if and only if $x \notin M_h^*$. Note that the factorization of $h(a)$ as $wax$, with $w \in M_h^*$ and $x \notin M_h^*$, if it exists, is unique.

In a similar way, we let ${}^{\omega}\Sigma$ denote the set of all left-infinite words, which are of the form $\mathbf{w} = \cdots c_{-2}c_{-1}c_0$. We write $h(\mathbf{w}) = \cdots h(c_{-2})h(c_{-1})h(c_0)$. We define ${}^{\omega}L$ to be the set of left-infinite words formed by concatenating infinitely many words from $L$, that is,

$$ {}^{\omega}L := \{\cdots w_{-2}w_{-1}w_0 \ : \ w_i \in L - \{\epsilon\} \text{ for all } i \leq 0\}.$$

If $h(a) = wax$, and $w \notin M_h^*$, $x \in M_h^*$, then we define the left-infinite word

$$\overleftarrow{h^{\omega}}(a) := \cdots h^2(w)\, h(w)\, w\, a\, x\, h(x)\, \cdots h^{t-1}(x),$$

where $h^t(x) = \epsilon$. Again, if the factorization of $h(a)$ as $wax$ exists, with $w \notin M_h^*$, $x \in M_h^*$, then it is unique.

We can convert left-infinite to right-infinite words (and vice versa) using the reverse operation, which is denoted $\mathbf{w}^R$. For example, if $w = c_0c_1c_2\cdots$, then $\mathbf{w}^R = \cdots c_2c_1c_0$.

We now turn to the notation for two-sided infinite words. These have been much less studied in the literature than one-sided words, and the notation has not been standardized. Some authors consider 2 two-sided infinite words to be identical if they agree after applying a finite shift to one of the words. Other authors do not. (This distinction is sometimes called "unpointed" vs. "pointed" [2, 17].) In this paper, we consider both the pointed and unpointed versions of the equation $h(\mathbf{w}) = \mathbf{w}$. As it turns out, the "pointed" version of this equation is quite easy to solve, based on known results, while the "unpointed" case is significantly more difficult. The latter is our first main result, which appears as Theorem 5.

We let $\Sigma^{\mathbb{Z}}$ denote the set of all two-sided infinite words over the alphabet $\Sigma$, which are of the form $\cdots c_{-2}c_{-1}c_0.c_1c_2\cdots$. In displaying an infinite word as a concatenation of words, we use a decimal point to the left of the character $c_1$, to indicate how the word is indexed. Of course, the decimal point is not part of the word itself. We define the *shift* $\sigma(\mathbf{w})$ to be the two-sided infinite word obtained by shifting $\mathbf{w}$ to the left one position, so that

$$\sigma(\cdots c_{-2}c_{-1}c_0.c_1c_2c_3\cdots) = \cdots c_{-1}c_0c_1.c_2c_3c_4\cdots .$$

Similarly, for $k \in \mathbb{Z}$ we define

$$\sigma^k(\cdots c_{-2}c_{-1}c_0.c_1c_2c_3\cdots) = \cdots c_{k-1}c_k.c_{k+1}c_{k+2}\cdots .$$

If $\mathbf{w}, \mathbf{x}$ are 2 two-sided infinite words, and there exists an integer $k$ such that $\mathbf{x} = \sigma^k(\mathbf{w})$, then we call $\mathbf{w}$ and $\mathbf{x}$ *conjugates*, and we write $\mathbf{w} \sim \mathbf{x}$. It is easy to see that $\sim$ is an equivalence relation. We extend this notation to languages as follows: if $L$ is a set of two-sided infinite words, then by $\mathbf{w} \sim L$ we mean there exists $\mathbf{x} \in L$ such that $\mathbf{w} \sim \mathbf{x}$.

If $w$ is a nonempty finite word, then by $w^{\mathbb{Z}}$ we mean the two-sided infinite word $\cdots www.www\cdots$. Using concatenation, we can join a left-infinite word $\mathbf{w} = \cdots c_{-2}c_{-1}c_0$ with a right-infinite word $\mathbf{x} = d_0d_1d_2\cdots$ to form a new two-sided infinite word, as follows:

$$\mathbf{w}.\mathbf{x} := \cdots c_{-2}c_{-1}c_0.d_0d_1d_2\cdots .$$

If $L \subseteq \Sigma^*$ is a set of words, then we define

$$L^{\mathbb{Z}} := \{\cdots w_{-2}w_{-1}w_0.w_1w_2\cdots \ : \ w_i \in L - \{\epsilon\} \text{ for all } i \in \mathbb{Z}\}.$$

If $\mathbf{w} = \cdots c_{-2}c_{-1}c_0.c_1c_2\cdots$, and $h$ is a morphism, then we define

$$h(\mathbf{w}) := \cdots h(c_{-2})h(c_{-1})h(c_0).h(c_1)h(c_2)\cdots \tag{1}$$

Finally, if $i = |wa|$, $h(a) = wax$, and $w, x \notin M_h^*$, then we define

$$\overleftrightarrow{h^{\omega;i}}(a) := \cdots h^2(w)\, h(w)\, w\, .a\, x\, h(x)\, h^2(x)\cdots ,$$

a two-sided infinite word. Note that in this case the factorization of $h(a)$ as $wax$ is *not* necessarily unique, and we use the superscript $i$ to indicate which $a$ is being chosen.

We can produce one-sided infinite words from two-sided infinite words by ignoring the portion to the right or left of the decimal point. Suppose $\mathbf{w} = \cdots c_{-2}c_{-1}c_0.c_1c_2c_3\cdots$. We define

$$\mathrm{L}(\mathbf{w}) = \cdots c_{-2}c_{-1}c_0,$$

a left-infinite word, and

$$\mathrm{R}(\mathbf{w}) = c_1c_2c_3\cdots ,$$

a right-infinite word.

# 2 Finite and one-sided infinite fixed points

In this section we recall the results of Head [9] and Head and Lando [10]. We assume $h : \Sigma^* \to \Sigma^*$ is a morphism that is extended to the domains $\Sigma^\omega$ and ${}^\omega\Sigma$ in the manner discussed above.

Define

$$A_h = \{a \in \Sigma \ : \ \exists\, x, y \in \Sigma^* \text{ such that } h(a) = xay \text{ and } xy \in M_h^*\}$$

and

$$F_h = \{h^t(a) \ : \ a \in A_h \text{ and } t = \exp(h)\}.$$

Note that there is at most one way to write $h(a)$ in the form $xay$ with $xy \in M_h^*$.

**Theorem 1** *A finite word $w \in \Sigma^*$ has the property that $w = h(w)$ if and only if $w \in F_h^*$.*

**Theorem 2** *The right-infinite word $\mathbf{w}$ is a fixed point of $h$ if and only if at least one of the following two conditions holds:*

*(a)* $\mathbf{w} \in F_h^\omega$; *or*

(b) $\mathbf{w} \in F_h^* \overrightarrow{h^\omega}(a)$ *for some* $a \in \Sigma$, *and there exist* $x \in M_h^*$ *and* $y \notin M_h^*$ *such that* $h(a) = xay$.

There is also an evident analogue of Theorem 2 for left-infinite words:

**Theorem 3** *The left-infinite word* $\mathbf{w}$ *is a fixed point of* $h$ *if and only if at least one of the following two conditions holds:*

(a) $\mathbf{w} \in {}^\omega F_h$; *or*

(b) $\mathbf{w} \in \overleftarrow{h^\omega}(a) F_h^*$ *for some* $a \in \Sigma$, *and there exist* $x \notin M_h^*$ *and* $y \in M_h^*$ *such that* $h(a) = xay$.

# 3 Two-sided infinite fixed points: the "pointed" case

We assume $h : \Sigma^* \to \Sigma^*$ is a morphism that is extended to the domain $\Sigma^{\mathbb{Z}}$ in the manner discussed above. In this section, we consider the equation $h(\mathbf{w}) = \mathbf{w}$ for two-sided infinite words.

**Proposition 4** *The equation* $h(\mathbf{w}) = \mathbf{w}$ *has a solution if and only if at least one of the following conditions holds:*

(a) $\mathbf{w} \in F_h^{\mathbb{Z}}$; *or*

(b) $\mathbf{w} \in \overleftarrow{h^\omega}(a) F_h^* . F_h^\omega$ *for some* $a \in \Sigma$, *and there exist* $x \notin M_h^*$, $y \in M_h^*$ *such that* $h(a) = xay$; *or*

(c) $\mathbf{w} \in {}^\omega F_h . F_h^* \overrightarrow{h^\omega}(a)$ *for some* $a \in \Sigma$, *and there exist* $x \in M_h^*$, $y \notin M_h^*$ *such that* $h(a) = xay$; *or*

(d) $\mathbf{w} \in \overleftarrow{h^\omega}(a) F_h^* . F_h^* \overrightarrow{h^\omega}(b)$ *for some* $a, b \in \Sigma$ *and there exist* $x, z \notin M_h^*$, $y, w \in M_h^*$, *such that* $h(a) = xay$ *and* $h(b) = wbz$.

**Proof.** Let $\mathbf{w} = \cdots c_{-2}c_{-1}c_0.c_1c_2c_3\cdots$. By definition, we have

$$h(\mathbf{w}) = \cdots h(c_{-2})h(c_{-1})h(c_0).h(c_1)h(c_2)h(c_3)\cdots,$$

so if $h(\mathbf{w}) = \mathbf{w}$, then we have $h(c_1c_2c_3\cdots) = c_1c_2c_3\cdots$ and $h(\cdots c_{-2}c_{-1}c_0) = \cdots c_{-2}c_{-1}c_0$.

We may now apply Theorem 2 (resp., Theorem 3) to R($\mathbf{w}$) (resp., L($\mathbf{w}$)). There are 2 cases to consider for each side, giving $2 \cdot 2 = 4$ total cases. ■

*Example.* Let $\mu$ be the Thue-Morse morphism, which maps $\mathtt{0} \to \mathtt{01}$, and $\mathtt{1} \to \mathtt{10}$. Define $g = \mu^2$. Then $g(\mathtt{0}) = \mathtt{0110}$, $g(\mathtt{1}) = \mathtt{1001}$. Let $\mathbf{t} = \mathtt{01101001}\cdots$, the one-sided Thue-Morse infinite word. Then there are exactly 4 two-sided infinite fixed points of $g$, as follows:

$$\begin{aligned}
\mathbf{t}^R.\mathbf{t} &= \cdots\mathtt{10010110.01101001}\cdots \\
\overline{\mathbf{t}}^R.\mathbf{t} &= \cdots\mathtt{01101001.01101001}\cdots \\
\overline{\mathbf{t}}^R.\overline{\mathbf{t}} &= \cdots\mathtt{01101001.10010110}\cdots \\
\mathbf{t}^R.\overline{\mathbf{t}} &= \cdots\mathtt{10010110.10010110}\cdots .
\end{aligned}$$

All of these fall under case (d) of Proposition 4. Incidentally, all four of these words are overlap-free.

# 4 Two-sided infinite fixed points: the "unpointed" case

We assume $h : \Sigma^* \to \Sigma^*$ is a morphism that is extended to the domain $\Sigma^{\mathbb{Z}}$ in the manner discussed above. In this section, we characterize the two-sided infinite fixed points of a morphism in the "unpointed" case. That is, our goal is to characterize the solutions to $h(\mathbf{w}) \sim \mathbf{w}$. The following theorem is the first of our two main results.

**Theorem 5** *Let $h$ be a morphism. Then the two-sided infinite word $\mathbf{w}$ satisfies the relation $h(\mathbf{w}) \sim \mathbf{w}$ if and only if at least one of the following conditions holds:*

*(a)* $\mathbf{w} \sim F_h^{\mathbb{Z}}$; *or*

*(b)* $\mathbf{w} \sim \overleftarrow{h^\omega}(a).F_h^\omega$ *for some $a \in \Sigma$, and there exist $x \notin M_h^*$ and $y \in M_h^*$ such that $h(a) = xay$; or*

*(c)* $\mathbf{w} \sim {}^\omega F_h.\ \overrightarrow{h^\omega}(a)$ *for some $a \in \Sigma$, and there exist $x \in M_h^*$ and $y \notin M_h^*$ such that $h(a) = xay$; or*

*(d)* $\mathbf{w} \sim \overleftarrow{h^\omega}(a).F_h^*\ \overrightarrow{h^\omega}(b)$ *for some $a, b \in \Sigma$ and there exist $x, z \notin M_h^*$, $y, w \in M_h^*$, such that $h(a) = xay$ and $h(b) = wbz$; or*

*(e)* $\mathbf{w} \sim \overleftrightarrow{h^{\omega;i}}(a)$ *for some $a \in \Sigma$, and there exist $x, y \notin M_h^*$ such that $h(a) = xay$ with $|xa| = i$; or*

*(f)* $\mathbf{w} = (xy)^{\mathbb{Z}}$ *for some $x, y \in \Sigma^+$ such that $h(xy) = yx$.*

Before we begin the proof of Theorem 5, we state and prove three useful lemmas.

**Lemma 6** *Suppose* $\mathbf{w}$, $\mathbf{x}$ *are* 2 *two-sided infinite words with* $\mathbf{w} \sim \mathbf{x}$. *Then* $h(\mathbf{w}) \sim h(\mathbf{x})$.

**Proof.** Since $\mathbf{w} \sim \mathbf{x}$, there exists $j$ such that $\mathbf{x} = \sigma^j(\mathbf{w})$. Then $h(\mathbf{x}) = \sigma^k(h(\mathbf{w}))$, where

$$k = \begin{cases} |h(c_1 c_2 \cdots c_j)|, & \text{if } j \geq 0; \\ -|h(c_{j+1} c_{j+2} \cdots c_{-1} c_0)|, & \text{if } j < 0. \end{cases} \tag{2}$$

■

Our second lemma concerns periodicity of infinite words. We say a two-sided infinite word

$$\mathbf{w} = \cdots c_{-2} c_{-1} c_0 . c_1 c_2 \cdots$$

is *periodic* if there exists a nonempty word $x$ such that $\mathbf{w} = x^{\mathbb{Z}}$, i.e., if there exists an integer $p \geq 1$ such that $\mathbf{w} = \sigma^p(\mathbf{w})$. The integer $p$ is called a *period* of $\mathbf{w}$.

**Lemma 7** *Suppose* $\mathbf{w} = \cdots c_{-2} c_{-1} c_0 . c_1 c_2 \cdots$ *is a two-sided infinite word such that there exists a one-sided right-infinite word* $\mathbf{x}$ *and infinitely many negative indices* $0 > i_1 > i_2 > \cdots$ *such that*

$$\mathbf{x} = c_{i_j} c_{i_j+1} c_{i_j+2} \cdots$$

*for* $j \geq 1$. *Then* $\mathbf{w}$ *is periodic.*

**Proof.** By assumption

$$\mathbf{x} = c_{i_j} c_{i_j+1} c_{i_j+2} \cdots = c_{i_{j+1}} c_{i_{j+1}+1} c_{i_{j+1}+2} \cdots$$

for $j \geq 1$. Hence $c_{i_j+k} = c_{i_{j+1}+k}$ for all $k \geq 0$, and so the right-infinite word $\mathbf{x}$ is periodic of period $i_j - i_{j+1}$. Since this is true for all $j \geq 1$, it follows that $\mathbf{x}$ is periodic of period $g = \gcd_{j \geq 1}(i_j - i_{j+1})$, i.e., $c_{i_j+k} = c_{i_j+g+k}$ for all $j \geq 1, k \geq 0$. Since $i_j \to -\infty$, it follows that $c_k = c_{k+g}$ for all $k$, and so $\mathbf{w}$ is periodic of period $g$. ■

Our third lemma concerns the growth functions of iterated morphisms.

**Lemma 8** *Let* $h : \Sigma^* \to \Sigma^*$ *be a morphism. Then*

*(a) there exist integers* $i, j$ *with* $0 \leq i < j$ *and* $|h^i(w)| \leq |h^j(w)|$ *for all* $w \in \Sigma^*$; *and*

*(b) there exists an integer* $M$ *depending only on* $k = \text{Card } \Sigma$ *such that for all* $h : \Sigma^* \to \Sigma^*$, *we have* $j \leq M$.

We note that part (a) was asserted without proof by Cobham [4]. However, the proof easily follows from a result of Dickson [6] that $\mathbb{N}^k$ contains no infinite antichains under the usual partial ordering; see also König [13]. For completeness, we give the following proof, suggested by S. Astels (personal communication).

**Proof.** (a) Suppose $\Sigma = \{a_1, a_2, \ldots, a_r\}$. First, choose $i_{1,1}$ to be the least index such that $|h^{i_{1,1}}(a_1)| = \min_{i \geq 0} |h^i(a_1)|$. Next, successively choose $i_{1,2}, i_{1,3}, i_{1,4}, \ldots$ such that $|h^{i_{1,n+1}}(a_1)| = \min_{i > i_{1,n}} |h^i(a_1)|$ for $n \geq 1$. Clearly $|h^{i_{1,n}}(a_1)| \leq |h^{i_{1,n+1}}(a_1)|$ for all $n \geq 1$. Let $S_1 = \{i_{1,1}, i_{1,2}, i_{1,3}, \ldots\}$.

Now, choose $i_{2,1}$ to be the least index $i \in S_1$ such $|h^{i_{2,1}}(a_2)| = \min_{i \in S_1} |h^i(a_2)|$. Next, successively choose $i_{2,2}, i_{2,3}, i_{2,4}, \ldots \in S_1$ such that $|h^{i_{2,n+1}}(a_2)| = \min_{i \in S_1; i > i_{2,n}} |h^i(a_2)|$ for $n \geq 1$. Clearly $|h^{i_{2,n}}(a_j)| \leq |h^{i_{2,n+1}}(a_j)|$ for $j = 1, 2$ and all $n \geq 1$. Let $S_2 = \{i_{2,1}, i_{2,2}, i_{2,3}, \ldots\}$. Note that $S_2 \subseteq S_1$.

Continuing in this fashion, we produce an infinite sequence of indices $i_{r,1}, i_{r,2}, i_{r,3}, \ldots$ such that $|h^{i_{r,n}}(a_j)| \leq |h^{i_{r,n+1}}(a_j)|$ for $j = 1, 2, \ldots, r$ and all $n \geq 1$. We can then choose $i = i_{r,1}$ and $j = i_{r,2}$.

(b) We omit the proof, although we observe that we can take $M = 2^k$. See [23]. ■

Now we can prove Theorem 5.

**Proof.** ($\Longleftarrow$): Suppose case (a) holds, and $\mathbf{w} \sim F_h^{\mathbb{Z}}$. Then there exists $\mathbf{x} \in F_h^{\mathbb{Z}}$ with $\mathbf{w} \sim \mathbf{x}$. Since $\mathbf{x} \in F_h^{\mathbb{Z}}$, we can write $\mathbf{x} = \cdots x_{-2}x_{-1}x_0.x_1x_2\cdots$, where $x_i \in F_h$ for all $i \in \mathbb{Z}$. Since $x_i \in F_h$, we have $h(x_i) = x_i$ for all $i \in \mathbb{Z}$. It follows that $h(\mathbf{x}) = \mathbf{x}$. Now, applying Lemma 6, we conclude that $h(\mathbf{w}) \sim h(\mathbf{x}) = \mathbf{x} \sim \mathbf{w}$.

Next, suppose case (b) holds, and $\mathbf{w} \sim \overleftarrow{h^\omega}(a).F_h^\omega$. Then $\mathbf{w} \sim \mathbf{x}$ for some $\mathbf{x}$ of the form

$$\mathbf{x} = \overleftarrow{h^\omega}(a).x_1x_2x_3\cdots,$$

where $x_i \in F_h$ for all $i \geq 1$, and $h(a) = xay$ with $x \notin M_h^*$ and $y \in M_h^*$. Then we have $h(\mathbf{x}) = \mathbf{x}$, and by Lemma 6, we conclude that $h(\mathbf{w}) \sim h(\mathbf{x}) = \mathbf{x} \sim \mathbf{w}$.

Cases (c), (d), and (e) are similar to case (b).

Finally, if case (f) holds, then

$$h(\mathbf{w}) = h(\cdots xyxy.xyxy\cdots) = \cdots yxyx.yxyx\cdots,$$

and so $h(\mathbf{w}) = \sigma^k(\mathbf{w})$ for $k = |x|$.

($\Longrightarrow$): Suppose $\mathbf{w} = \cdots c_{-2}c_{-1}c_0.c_1c_2\cdots$, and there exists $k$ such that $h(\mathbf{w}) = \sigma^k(\mathbf{w})$. Let

$$s(i) := \begin{cases} |h(c_1c_2\cdots c_i)| + k, & \text{if } i \geq 0; \\ k - |h(c_{i+1}c_{i+2}\cdots c_0)|, & \text{if } i < 0. \end{cases} \tag{3}$$

Then it is not hard to see that

$$h(c_i) = c_{s(i-1)+1}\cdots c_{s(i)} \tag{4}$$

for $i \in \mathbb{Z}$; see Figure 1. Note that $s(0) = k$.

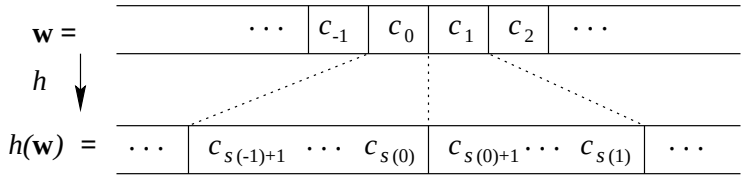


Figure 1: Interpretation of the function $s$

We define the set $C$ as follows: $C = \{i \in \mathbb{Z} \ : \ s(i) = i\}$. Our argument is divided into two major cases, depending on whether or not $C$ is empty.

*Case 1:* $C \neq \emptyset$. In this case, there exists $j$ such that $s(j) = j$. Now consider the pointed word $\mathbf{x} = \cdots c_{j-2}c_{j-1}c_j.c_{j+1}c_{j+2}\cdots$. We have $\mathbf{x} \sim \mathbf{w}$ and by Eq. (4) we have $h(\mathbf{x}) = \mathbf{x}$. Then, by Proposition 4, one of cases (a)–(d) must hold.

*Case 2:* $C = \emptyset$. There are several subcases to consider.

*Case 2a:* There exist integers $i, j$ with $i < j$ such that

$$s(i) > i \text{ but } s(j) < j. \tag{5}$$

Among all pairs $(i, j)$ satisfying (5), choose one with $j - i$ minimal. Suppose there exists an integer $k$ with $i < k < j$. If $s(k) < k$, then $(i, k)$ is a pair satisfying (5) with smaller difference, while if $k < j$, then $(k, j)$ is a pair satisfying (5) with smaller difference. Hence $s(k) = k$. But this is impossible by our assumption. It follows that $j = i + 1$. Then $s(i) > i$, but $s(i + 1) < i + 1$, a contradiction, since $s(i) \leq s(i + 1)$. Hence this case cannot occur.

*Case 2b:* There exists an integer $r$ such that $s(i) < i$ for all $i < r$, and $s(i) > i$ for all $i \geq r$. Then $h(c_r) = c_{s(r-1)+1} \cdots c_{s(r)}$, which by the inequalities contains $c_{r-1}c_rc_{r+1}$ as a subword. Therefore, letting $a = c_r$, it follows that

$$\mathbf{w} \sim \mathbf{u}\, x\, .\, a\, y\, \mathbf{v},$$

where $\mathbf{u} = \cdots c_{s(r-1)-1}c_{s(r-1)}$ is a left-infinite word, $x = c_{s(r-1)+1} \cdots c_{r-1}$ and $y = c_{r+1} \cdots c_{s(r)}$ are finite words, and $\mathbf{v} = c_{s(r)+1}c_{s(r)+2} \cdots$ is a right-infinite word. Furthermore, we have $h(\mathbf{u}x) = \mathbf{u}$, $h(a) = xay$, and $h(y\mathbf{v}) = \mathbf{v}$.

Now the equation $h(y\mathbf{v}) = \mathbf{v}$ implies that $h(y)$ is a prefix of $\mathbf{v}$, and by an easy induction we have $h(y)h^2(y)h^3(y)\cdots$ is a prefix of $\mathbf{v}$. Suppose this prefix is finite. Then $y \in M_h^*$, and so $h(y)h^2(y)h^3(y)\cdots = h(y)h^2(y)\cdots h^t(y)$, where $t = \exp(h)$. Define $z = h(y)h^2(y)\cdots h^t(y)$. Then $s(r + |y| + |z|) = r + |y| + |z|$, a contradiction, since we have assumed $C = \emptyset$. It follows that $\mathbf{z} := h(y)h^2(y)h^3(y)\cdots$ is right-infinite and hence $y \notin M_h^*$.

By exactly the same reasoning, we find that $\cdots h^3(x)\, h^2(x)\, h(x)$ is a left-infinite suffix of $\mathbf{u}$. We conclude that $\mathbf{w} \sim \overleftrightarrow{h^{\omega;i}}(a)$, and hence case (e) holds.

*Case 2c:* $s(i) > i$ for all $i \in \mathbb{Z}$. Let $\mathbf{w} = \cdots c_{-2}c_{-1}c_0.c_1c_2\cdots$.

Now consider the following factorization of certain conjugates of $\mathbf{w}$, as follows: for $i \leq 0$, we have $\mathbf{w} \sim \mathbf{x}_i\, y_i\, .\, \mathbf{z}_i$, where $\mathbf{x}_i = \cdots c_{i-2}c_{i-1}$ (a left-infinite word), $y_i = c_i \cdots c_{s(i-1)}$ (a finite word), and $\mathbf{z}_i = c_{s(i-1)+1}c_{s(i-1)+2}\cdots$ (a right-infinite word). Note that $i - 1 < s(i-1)$ by assumption, so $i \leq s(i-1)$; hence $y_i$ is nonempty. Evidently we have

$$\begin{aligned} h(\mathbf{x}_i) &= \mathbf{x}_i\, y_i; \quad \text{and} \\ h(y_i\, \mathbf{z}_i) &= \mathbf{z}_i. \end{aligned} \tag{6}$$

Now the equation $h(y_i\mathbf{z}_i) = \mathbf{z}_i$ implies that $h(y_i)$ is a prefix of $\mathbf{z}_i$. Now an easy induction, as in Case 2b, shows that $v := h(y_i)h^2(y_i)h^3(y_i)\cdots$ is a prefix of $\mathbf{z}_i$. If $v$ were finite, then we would have $y_i \in M_h^*$, and so $s(j) = j$ for $j = s(i-1) + |v|$, a contradiction, since $C = \emptyset$. Hence $v$ is right-infinite, and so $y_i \notin M_h^*$. There are now two further subcases to consider: (i) $\sup_{i\leq 0}(s(i) - i) < +\infty$, and (ii) $\sup_{i\leq 0}(s(i) - i) = +\infty$.

*Case 2ci:* Suppose $\sup_{i\leq 0}(s(i) - i) = d < +\infty$. It then follows that $|y_i| \leq d$. Hence there is a finite word $u$ such that $y_i = u$ for infinitely many indices $i \leq 0$. From the above argument we see that the right-infinite word $h(u)h^2(u)h^3(u)\cdots$ is a suffix of $\mathbf{w}$, beginning at position $s(i-1)+1$, for infinitely many indices $i \leq 0$. We now use Lemma 7 to conclude that $\mathbf{w}$ is periodic.

Thus we can write $\mathbf{w} = \cdots c_{-2}c_{-1}c_0.c_1c_2\cdots$, and $\mathbf{w} = \cdots vvv.vvv\cdots$, where $v = c_1c_2\cdots c_p$ for some integer $p \geq 1$. Without loss of generality, we may assume $p$ is minimal.

We claim $|h(v)| = p$. For if not we must have $|h(v)| = q$, for $q \neq p$, and then since $h(\mathbf{w}) \sim \mathbf{w}$, we would have $\mathbf{w}$ is periodic with periods $p$ and $q$, hence periodic of period $\gcd(p, q)$. But since $p$ was minimal we must have $p \,|\, q$. Hence $q \geq 2p$. Now let $s(p) = l$; since $s(i) > i$ for all $i$ we must have $l > 0$. Then

$$h(c_1c_2\cdots c_p) = c_{s(-1)+1}\cdots c_{s(p)} = c_{l-q+1}\cdots c_l.$$

It now follows that

$$s(ip) = l - q + iq \tag{7}$$

for all integers $i$. Now $p < q$, so $p \leq q - 1$, and hence $p < q - 1 + q/l$. Hence, multiplying by $-l$, we get $-lp > l - ql - q$. Now take $i = -l$ in Eq. (7), and we have

$$s(-lp) = l - q - lq < -lp,$$

a contradiction, since $s(i) > i$ for all $i$. It follows that $|h(v)| = p$.

There exists $k$ such that $h(c_1c_2\cdots c_p) = c_{k+1}c_{k+2}\cdots c_{k+p}$. Using the division theorem, write $k = jp + r$, where $0 \leq r < p$. Define

$$y = c_{k+1}\cdots c_{(j+1)p} = c_{r+1}\cdots c_p;$$
$$x = c_{(j+1)p+1}\cdots c_{k+p} = c_1\cdots c_r.$$

We have $h(xy) = yx$, and $v = xy$. Then $\mathbf{w} = v^{\mathbb{Z}} = (xy)^{\mathbb{Z}}$.

By above we know $|v| \geq 1$, so $xy \neq \epsilon$. Suppose $y = \epsilon$. Then $h(x) = x$, and so $x \in F_h^*$. It follows that $\mathbf{w} \in F_h^{\mathbb{Z}}$. A similar argument applies if $x = \epsilon$. However, if $\mathbf{w} \in F_h^{\mathbb{Z}}$, then $C \neq \emptyset$, a contradiction. Thus $x, y \neq \epsilon$, and case (f) holds.

*Case 2cii:* $\sup_{i\leq 0}(s(i) - i) = +\infty$. Recall that $s(i) > i$ for all $i \in \mathbb{Z}$ and $\mathbf{w} = \cdots c_{-2}c_{-1}c_0.c_1c_2\cdots$. Define

$$\begin{aligned} \mathbf{x} &:= \cdots c_{-2}c_{-1}c_0; \\ y &:= c_1c_2\cdots c_{s(0)}; \\ \mathbf{z} &:= c_{s(0)+1}c_{s(0)+2}\cdots . \end{aligned}$$

Then $\mathbf{w} = \mathbf{x}.y\mathbf{z}$ and $h(\mathbf{x}) = \mathbf{x}y$, $h(y\mathbf{z}) = \mathbf{z}$.

Define $B_j(k) = s^j(k) - s^{j-1}(k)$, where $s^j$ denotes the $j$-fold composition of the function $s$ with itself. First we prove the following technical lemma.

**Lemma 9** *For all integers $r \geq 1$ there exists an integer $n \leq 0$ such that $B_j(n) > r$ for $1 \leq j \leq t$.*

**Proof.** By induction on $t$. For $t = 1$ the result follows since

$$\sup_{i\leq 0} B_1(i) = \sup_{i\leq 0}(s(i) - i) = +\infty.$$

Now assume the result is true for $t$; we prove it for $t + 1$. Define $m := \max_{a\in\Sigma} |h(a)|$. By induction there exists an integer $n_1$ such that $B_j(n_1) > mr + m^{t+1}$ for $1 \leq j \leq t$. Then, by the definition of $m$ there exist an integer $n_2 < n_1$ with $n_1 - n_2 < m$, and an integer $n_3$ such that $s(n_3) = n_2$.

Now $h(c_{n_3+1}\cdots c_{n_2}) = c_{s(n_3)+1}\cdots c_{s(n_2)}$, so $s(n_2) - s(n_3) \leq m(n_2 - n_3)$. Similarly, we have

$$s^j(n_2) - s^j(n_3) \leq m^j(n_2 - n_3) \tag{8}$$

for all $j \geq 0$. By the same reasoning, we have

$$s^j(n_1) - s^j(n_2) \leq m^j(n_1 - n_2) \leq m^j(m - 1) \tag{9}$$

for all $j \geq 0$. Thus we find

$$\begin{aligned}
B_1(n_3) &= s(n_3) - n_3 \\
&= n_2 - n_3 \\
&\geq \frac{s(n_2) - s(n_3)}{m} \quad \text{(by Eq. (8))} \\
&= \frac{s(n_2) - n_2}{m} \\
&= \frac{(s(n_1) - n_1) - ((s(n_1) - s(n_2)) - (n_1 - n_2))}{m} \\
&= \frac{B_1(n_1) - ((s(n_1) - s(n_2)) - (n_1 - n_2))}{m} \\
&> \frac{mr + m^{t+1} - m(m-1)}{m} \quad \text{(by induction and Eq. (9))} \\
&> r.
\end{aligned}$$

Similarly, for $2 \leq j \leq t+1$, we have

$$\begin{aligned}
B_j(n_3) &= s^j(n_3) - s^{j-1}(n_3) \\
&= s^{j-1}(n_2) - s^{j-2}(n_2) \\
&= (s^{j-1}(n_1) - s^{j-2}(n_1)) - ((s^{j-1}(n_1) - s^{j-1}(n_2)) - (s^{j-2}(n_1) - s^{j-2}(n_2))) \\
&= B_{j-1}(n_1) - ((s^{j-1}(n_1) - s^{j-1}(n_2)) - (s^{j-2}(n_1) - s^{j-2}(n_2))) \\
&> mr + m^{t+1} - m^{j-1}(m-1) \quad \text{(by Eq. (9))} \\
&\geq r.
\end{aligned}$$

It thus follows that we can take $n = n_3$. This completes the proof of Lemma 9. ■

Now let $M$ be the integer specified in Lemma 8, and define $r := \sup_{1 \leq i \leq M} B_i(0)$. By Lemma 9 there exists an integer $n \leq 0$ such that $B_j(n) > r$ for $1 \leq j \leq M$. Define $w := c_{n+1} \cdots c_0$. We have

$$\begin{aligned}
|h^j(w)| &= s^j(0) - s^j(n); \quad \text{and} \\
|h^{j-1}(w)| &= s^{j-1}(0) - s^{j-1}(n).
\end{aligned}$$

It follows that

$$\begin{aligned}
|h^j(w)| &= (s^j(0) - s^{j-1}(0)) - (s^j(n) - s^{j-1}(n)) + |h^{j-1}(w)| \\
&= B_j(0) - B_j(n) + |h^{j-1}(w)| \\
&< B_j(0) - r + |h^{j-1}(w)| \\
&\leq |h^{j-1}(w)|
\end{aligned}$$

for $1 \le j \le M$. But this contradicts Lemma 8. This contradiction shows that this case cannot occur.

*Case 2d:* $s(i) < i$ for all $i \in \mathbb{Z}$. This case is the mirror image of Case 2c[1], and the proof is identical. The proof of Theorem 5 is complete. ■

# 5 Some examples

In this section we consider some examples of Theorem 5.

*Example 1.* Consider the morphism $f$ defined by $\mathtt{a} \to \mathtt{bb}$, $\mathtt{b} \to \epsilon$, $\mathtt{c} \to \mathtt{aad}$, $\mathtt{d} \to \mathtt{c}$. Let

$$\mathbf{w} = \cdots \mathtt{aadbbbbcaadbbbbc.aadbbbbcaadbbbbc} \cdots .$$

Then

$$f(\mathbf{w}) = \cdots \mathtt{bbbbcaadbbbbcaad.bbbbcaadbbbbcaad} \cdots .$$

This falls under case (f) of Theorem 5.

*Example 2.* Consider the morphism $\varphi$ defined by $\mathtt{0} \to \mathtt{201}$, $\mathtt{1} \to \mathtt{012}$, and $\mathtt{2} \to \mathtt{120}$. Then if

$$\mathbf{w} = \overleftrightarrow{\varphi^{\omega;2}}(\mathtt{0}) = \cdots c_{-2}c_{-1}.c_0c_1c_2 \cdots = \cdots \mathtt{1202.01012} \cdots ,$$

we have $\varphi(\mathbf{w}) \sim \mathbf{w}$. This falls under case (e) of Theorem 5. Incidentally, $c_i$ equals the sum of the digits, modulo 3, in the balanced ternary representation of $i$.

# 6 The equation $h(xy) = yx$ in finite words

It is not difficult to see that it is decidable whether any of conditions (a)–(e) of Theorem 5 hold for a given morphism $h$. However, this is somewhat less obvious for condition (f) of Theorem 5, which demands that the equation $h(xy) = yx$ possess a nontrivial[2] solution. We conclude this paper by discussing the solvability of this equation and, in our second main result, we give a characterization of the solution set.

To do so it is useful to extend the notation $\sim$, previously used for two-sided infinite words, to finite words. We say $w \sim z$ for $w, z \in \Sigma^*$ if $w$ is a cyclic shift of $z$, i.e., if there exist $x, y \in \Sigma^*$ such that $w = xy$ and $z = yx$. It is now easy to verify that $\sim$ is an equivalence relation. Furthermore, if $w \sim z$, and $h$ is a morphism, then $h(w) \sim h(z)$. Thus condition (f) can be restated as $h(z) \sim z$. The following theorem shows that the solvability of the equation $h(xy) = yx$ is decidable.

[1]Note that $s(i) > i$ for all $i$ implies that $s(i-1) > i-1$. Therefore $s(i-1)+1 > i$, and hence Case 2d really *is* the mirror image of Case 2c.

[2]By nontrivial we mean $xy \neq \epsilon$.

**Theorem 10** *Let $h$ be a morphism $h : \Sigma^* \to \Sigma^*$. Then $h(z) \sim z$ possesses a solution $z \neq \epsilon$ if and only if $F_{h^d}$ is nonempty for some $1 \leq d \leq$ Card $\Sigma$.*

**Proof.** $\Longleftarrow$: Suppose $F_{h^d}$ is nonempty for some $d$, say $x \in F_{h^d}$. Then by definition of $F_{h^d}$, $h^d(x) = x$. Let $y = h(x) \cdots h^{d-1}(x)$ and $z = xy$. Then $h(xy) = yx$ and so $h(z) \sim z$.

$\Longrightarrow$: Suppose $h(z) \sim z$. Then $|h^n(z)| = |z|$ for all $n \geq 0$, and so there exist $0 \leq i < j$ such that $h^i(z) = h^j(z)$. In other words, $h^i(z)$ is a finite fixed point of $h^{j-i}$. Hence $F_{h^{j-i}}$ is nonempty. This implies $A_{h^d}$ is nonempty for some $d$ with $1 \leq d \leq$ Card $\Sigma$. Thus $F_{h^d}$ is nonempty. ■

**Remarks.**

1. Note that Theorem 10 does not characterize all the finite solutions of $h(z) \sim z$; it simply gives a necessary and sufficient condition for solutions to exist.

2. As we have seen in Theorem 1, the set of finite solutions to $h(z) = z$ is finitely generated, in that the solution set can be written as $S^*$ for some finite set $T$. However, the set of solutions to $h(z) \sim z$ need not even be context-free. For consider the morphism defined by $h(\mathtt{a}) = \mathtt{b}$, $h(\mathtt{b}) = \mathtt{c}$, $h(\mathtt{c}) = \mathtt{a}$, and let

$$T := \{z \in \{\mathtt{a}, \mathtt{b}, \mathtt{c}\}^* \ : \ h(z) \sim z\}.$$

If $T$ were context-free, then so would be $T \cap \mathtt{a}^*\mathtt{b}^*\mathtt{c}^*$. But

$$T \cap \mathtt{a}^*\mathtt{b}^*\mathtt{c}^* = \{\mathtt{a}^i\mathtt{b}^i\mathtt{c}^i \ : \ i \geq 0\}$$

which is not context-free.

We finish with a discussion of the set $T$ of words $z$ for which $h(z) \sim z$. From the proof of Theorem 10, there exist $i < j$ such that $h^i(z)$ is a fixed point of $h^{j-i}$. Since $h^i(z) \sim z$, we may restrict our attention to the set $S = T \cap (\bigcup_{i \geq 1} F_{h^i}^*)$. Our set $T$ then is the set of all cyclic permutations of words in $S$.

To describe $S$ we introduce an auxiliary morphism $\tilde{h} : \tilde{\Sigma} \to \tilde{\Sigma}$, where $\tilde{\Sigma} \subseteq \Sigma$. A letter $a \in \tilde{\Sigma}$ if and only if the following three conditions hold:

(1) $a$ is an immortal letter of $h$;

(2) $h^i(a)$ contains exactly one immortal letter for all $i \geq 1$; and

(3) $h^i(a)$ contains $a$ for some $i \geq 1$.

We define the morphism $\tilde{h}$ by $\tilde{h}(a) = a'$ where $a'$ is the unique immortal letter in $h(a)$.

The relation of $\tilde{h}$ to $S$ is as follows. If $z \in S$, then $z \in F_{h^i}^*$ for some $i$. Hence there exists an integer $p$ such that $z = z_1 \cdots z_p$ where $z_j = x_j a_j y_j \in F_{h^i}$, and $a_j$ is an immortal letter for $1 \leq j \leq p$. It follows easily that $a_j \in \tilde{\Sigma}$. Hence $h$ cyclically shifts $z$ iff $\tilde{h}$ cyclically shifts $\tilde{z} = a_1 \cdots a_p$. (The words $x_j$ and $y_j$ are uniquely specified by $i$ and $a_j$.)

**Theorem 11** *We have*

$$\text{Card} \bigcup_{i \geq 1} F_{h^i} < \infty.$$

**Proof.** Suppose $a \in \tilde{\Sigma}$. Define $a_j$, $x_j$ and $y_j$ by $a_0 = a$ and $h(a_j) = x_j a_{j+1} y_j$ for $j \geq 0$, where $a_{j+1} \in \tilde{\Sigma}$. It is clear that there is a $t \leq \text{Card } \tilde{\Sigma}$ such that if $j \equiv k \pmod{t}$ then $a_j = a_k$, $x_j = x_k$ and $y_j = y_k$. Define $e_i = \exp(h^i)$. By the definition of $F_{h^i}$, all words in $F_{h^i}$ are of the form

$$h^{e_i-1}(x_{j_0}) h^{e_i-2}(x_{j_1}) \cdots h(x_{j_{e_i-2}}) x_{j_{e_i-1}} a_{e_i} y_{j_{e_i-1}} h(y_{j_{e_i-2}}) \cdots h^{e_i-2}(y_{j_1}) h^{e_i-1}(y_{j_0})$$

for some $a = a_0 \in \tilde{\Sigma}$. Since there are only finitely many $a_j$, $x_j$ and $y_j$ and $e_i \leq \text{Card } \tilde{\Sigma}$ for all $i \geq 1$, the result follows. ■

Therefore, we now concentrate on the set $\tilde{T}$ of words $\tilde{z}$ that are cyclically shifted by $\tilde{h}$.

Suppose $\tilde{\Sigma} = \{a_1, \ldots, a_s\}$. Since $\tilde{h}$ acts as a permutation $P$ on $\tilde{\Sigma}$, there exists a unique factorization of $P$ into disjoint cycles. Suppose $c = (d_0, \ldots, d_{t-1})$ is a cycle appearing in the factorization of $P$, and let $|c|$ denote the length $t$ of the cycle $c$. Define the language $L(c)$ as follows:

$$L(c) = (d_0 d_1 d_2 \cdots d_{t-1})^* + (d_1 d_2 \cdots d_{t-1} d_0)^* + \cdots + (d_{t-1} d_0 d_1 \cdots d_{t-2})^*.$$

For example, if $c = (0, 1, 2)$ then $L(c) = (012)^* + (120)^* + (201)^*$. Note that the definition of $L(c)$ is independent of the particular representation chosen for the cycle.

Now define the finite collection $\mathcal{R}'$ of regular languages as follows:

$$\mathcal{R}' = \{L(c^v) \ : \ c \text{ is a cycle of } P \text{ and } 1 \leq v \leq |c| \text{ and } \gcd(v, |c|) = 1\}.$$

We now define a finite collection $\mathcal{R}$ of regular languages. Each language in $\mathcal{R}$ is the union of some languages of $\mathcal{R}'$. The union is defined as follows. Each language $L(c^v)$ in $\mathcal{R}'$ is associated with a pair $(t, v)$ where $t = |c|$ and $v$ is an integer relatively prime to $t$. Then the languages $L(c_1^{v_1}), \ldots, L(c_m^{v_m})$ in $\mathcal{R}'$ are each a subset of the same language of $\mathcal{R}$ if and only if the system of congruences

$$\begin{aligned} v_1 x &\equiv 1 \pmod{t_1} \\ v_2 x &\equiv 1 \pmod{t_2} \\ &\vdots \\ v_m x &\equiv 1 \pmod{t_m} \end{aligned} \tag{10}$$

possesses an integer solution $x$, where $t_j = |c_j|$ for $1 \leq j \leq m$. Note that a language in $\mathcal{R}'$ may be a subset of several languages of $\mathcal{R}$.

We say a word $w$ is the *perfect shuffle* of words $w_1, \ldots, w_j$ if $|w_1| = \cdots = |w_j|$ and the first $j$ symbols of $w$ are the first symbols of $w_1, \ldots, w_j$ in that order, the second $j$ symbols of $w$ are the second symbols of $w_1, \ldots, w_j$ in that order, and so on. We write $w = \text{Ш}(w_1, w_2, \ldots, w_j)$. The following theorem characterizes the set $\tilde{T}$, and is our second main result.

**Theorem 12** *Let $\tilde{z} \in \tilde{\Sigma}^*$, and let $\tilde{h}$ permute $\tilde{\Sigma}$. Then $\tilde{h}(\tilde{z}) \sim \tilde{z}$ if and only if $\tilde{z}$ is the perfect shuffle of some finite number of words contained in some single language of $\mathcal{R}$.*

**Proof.** Let $\tilde{h}$ permute $\tilde{\Sigma}$, with induced permutation $P$. Let $\tilde{z} = b_0 b_1 \cdots b_{n-1}$.

($\Longleftarrow$): Suppose $\tilde{z}$ is the perfect shuffle of some finite number of words contained in a single language of $\mathcal{R}$. For simplicity of notation we consider the case where $\tilde{z}$ is the perfect shuffle of two such words; the general case is similar and is left to the reader.

Thus assume $\tilde{z} = \text{Ш}(w, \hat{w})$. Further, assume $w \in L(c^v)$ for some cycle $c$ and integer $v$ relatively prime to $t = |c|$, and $\hat{w} \in L(\hat{c}^{\hat{v}})$ for some cycle $\hat{c}$ and integer $\hat{v}$ relatively prime to $\hat{t} = |\hat{c}|$.

Then $w = (d_0 d_v d_{2v} \cdots d_{vt-1})^r$ for some cycle $(d_0, d_1, \ldots, d_{t-1})$ of $P$ with $\tilde{h}(d_s) = d_{s+1}$ for $0 \leq s < t$. (Here the indices are assumed to be taken modulo $t$.)

Then $\hat{w} = (\hat{d}_0 \hat{d}_{\hat{v}} \hat{d}_{2\hat{v}} \cdots \hat{d}_{\hat{v}\hat{t}-1})^{\hat{r}}$ for some cycle $(\hat{d}_0, \hat{d}_1, \ldots, \hat{d}_{\hat{t}-1})$ of $P$ with $\tilde{h}(\hat{d}_s) = \hat{d}_{s+1}$ for $0 \leq s < \hat{t}$. (Here the indices are assumed to be taken modulo $\hat{t}$.)

By hypothesis there exists an integer $x$ such that $vx \equiv 1 \pmod{t}$, and $\hat{v}x \equiv 1 \pmod{\hat{t}}$. A simple calculation shows that we may assume $0 \leq x < tr = \hat{t}\hat{r}$. Then $\tilde{z} = d_0 \hat{d}_0 \cdots$ and $\tilde{h}(\tilde{z}) = d_1 \hat{d}_1 \cdots = d_{vx} \hat{d}_{\hat{v}x} \cdots = b_{2x} b_{2x+1} \cdots$ (indices of $a$ taken mod $n$), and so $\tilde{h}(\tilde{z}) \sim \tilde{z}$.

($\Longrightarrow$): Suppose $\tilde{h}(\tilde{z}) \sim \tilde{z}$. Then there exists an integer $y$ such that $\tilde{h}(b_0 b_1 \cdots b_{n-1}) = b_y b_{y+1} \cdots b_{y-1}$, where the indices are taken modulo $n$. Define $g = \gcd(y, n)$ and $m = n/g$. Then, considering its action on $b_0 b_1 \cdots b_{n-1}$, the morphism $\tilde{h}$ induces a permutation of the indices $0, 1, \ldots, n-1$ sending $j \to j + y \pmod{n}$ which, by elementary group theory, factors into $g$ disjoint cycles, each of length $m$.

Now, for $0 \leq i < g$, define the words

$$w_i := b_i b_{g+i} b_{2g+i} \cdots b_{(m-1)g+i}.$$

It is clear that $\tilde{z} = \text{Ш}(w_0, w_1, \ldots, w_{g-1})$. Then

$$\begin{aligned} \tilde{h}(w_i) &= \tilde{h}(b_i\, b_{g+i}\, b_{2g+i} \cdots b_{(m-1)g+i}) \\ &= b_{i+y}\, b_{g+i+y}\, b_{2g+i+y} \cdots b_{(m-1)g+i+y} \\ &= b_{i+(\frac{y}{g})g}\, b_{i+(\frac{y}{g}+1)g}\, b_{i+(\frac{y}{g}+2)g} \cdots b_{i+(\frac{y}{g}+m-1)g}, \end{aligned}$$

and so it follows that $\tilde{h}$ cyclically shifts each $w_i$ by $y/g$.

Now $\gcd(m, y/g) = 1$, so for each $k$ there is a unique solution $t \pmod{m}$ of the congruence

$$t\frac{y}{g} \equiv k \pmod{m}.$$

Multiplying through by $g$, we find

$$ty \equiv kg \pmod{n}$$

has a solution $t$, so

$$ty + i \equiv kg + i \pmod{n}$$

has a solution $t$. But $\tilde{h}^t(b_i) = b_{ty+i}$, so each symbol $b_{kg+i}$ of $w_i$ is in the orbit of $\tilde{h}$ on $z_i$. It follows that each symbol of $w_i$ is contained in the same cycle $c_i$ of $P$. Suppose $c_i$ has length $t_i$. Then $\tilde{h}^{t_i}(b_i) = b_i$, and furthermore $t_i$ is the least positive integer with this property. However, we also have $\tilde{h}^m(b_i) = b_{i+ym} = b_{i+\frac{y}{g}n} = b_i$, and so $t_i \mid m$.

Since $\gcd(y/g, m) = 1$, there is a solution $v$ to the congruence $v \cdot \frac{y}{g} \equiv 1 \pmod{m}$. Then $vy \equiv g \pmod{n}$. Using the division theorem, write $v = q_i t_i + v_i$, where $0 \leq v_i < t_i$, for $0 \leq i < g$. Since $\gcd(v, m) = 1$, and $t_i \mid m$, we must have $\gcd(v, t_i) = 1$. Thus $\gcd(v_i, t_i) = 1$.

Now

$$\tilde{h}^{v_i}(b_{kg+i}) = \tilde{h}^{v-q_i t_i}(b_{kg+i}) = \tilde{h}^{v}(b_{kg+i}) = b_{kg+i+vy} = b_{kg+i+g} = b_{(k+1)g+i}.$$

Then for $0 \leq i < g$ we have

$$w_i = (b_i \, \tilde{h}^{v_i}(b_i) \, \tilde{h}^{2v_i}(b_i) \cdots \tilde{h}^{(t_i-1)v_i}(b_i))^{m/t_i} \in L(c_i^{v_i}).$$

From $\tilde{h}(b_0 b_1 b_2 \cdots) = b_y b_{y+1} b_{y+2} \cdots$, it follows that

$$\tilde{h}^{\frac{y}{g}v_i}(b_i) = b_{y+i} = \tilde{h}(b_i),$$

and so $\frac{y}{g}v_i \equiv 1 \pmod{t_i}$. Thus the system of equations (10) possesses a solution $x = y/g$. This completes the proof. ■

# References


[1] J.-P. Allouche. Automates finis en théorie des nombres. *Exposition. Math.* **5** (1987), 239–266.

[2] D. Beaquier. Ensembles reconnaissables de mots bi-infinis. In M. Nivat and D. Perrin, editors, *Automata on Infinite Words*, Vol. 192 of *Lecture Notes in Computer Science*, pp. 28–46. Springer-Verlag, 1985.

[3] J. Berstel. *Axel Thue's Papers on Repetitions in Words: a Translation.* Number 20 in Publications du Laboratoire de Combinatoire et d'Informatique Mathématique. Université du Québec à Montréal, February 1995.

[4] A. Cobham. On the Hartmanis-Stearns problem for a class of tag machines. In *IEEE Conference Record of 1968 Ninth Annual Symposium on Switching and Automata Theory*, pp. 51–60, 1968. Also appeared as IBM Research Technical Report RC-2178, August 23 1968.

[5] J. Devolder and E. Timmerman. Finitary codes for biinfinite words. *RAIRO Inform. Théor. App.* **26** (1992), 363–386.

[6] L. E. Dickson. Finiteness of the odd perfect and primitive abundant numbers with distinct factors. *Amer. J. Math.* **35** (1913), 413–422.

[7] D. Hamm and J. Shallit. Characterization of finite and one-sided infinite fixed points of morphisms on free monoids. Manuscript, submitted June, 1998.

[8] D. Hawkins and W. E. Mientka. On sequences which contain no repetitions. *Math. Student* **24** (1956), 185–187.

[9] T. Head. Fixed languages and the adult languages of $0L$ schemes. *Internat. J. Comput. Math.* **10** (1981), 103–107.

[10] T. Head and B. Lando. Fixed and stationary $\omega$-words and $\omega$-languages. In G. Rozenberg and A. Salomaa, editors, *The Book of L*, pp. 147–156. Springer-Verlag, 1986.

[11] J. E. Hopcroft and J. D. Ullman. *Introduction to Automata Theory, Languages, and Computation.* Addison-Wesley, 1979.

[12] L. P. Hurd. Recursive cellular automata invariant sets. *Complex Systems* **4** (1990), 119–129.

[13] D. König. *Theorie der endlichen und unendlichen Graphen: kombinatorische Topologie der Streckenkomplexe.* Akademische Verlagsgesellschaft, Leipzig, 1936. English translation, Birkhäuser, 1990.

[14] B. Lando. Periodicity and ultimate periodicity of D0L systems. *Theoret. Comput. Sci.* **82** (1991), 19–33.

[15] J. Leech. A problem on strings of beads. *Math. Gazette* **41** (1957), 277–278.

[16] D. Lind and B. Marcus. *An Introduction to Symbolic Dynamics and Coding.* Cambridge University Press, 1995.

[17] P. Narbel. The limit set of recognizable substitution systems. In *STACS 93, Proc. 10th Symp. Theoretical Aspects of Comp. Sci.*, Vol. 665 of *Lecture Notes in Computer Science*, pp. 226–236, 1993.

[18] M. Nivat and D. Perrin. Ensembles reconnaissables de mots biinfinis. In *Proc. Fourteenth Ann. ACM Symp. Theor. Comput.*, pp. 47–59. ACM, 1982.

[19] M. Nivat and D. Perrin. Ensembles reconnaissables de mots biinfinis. *Canad. J. Math.* **38** (1986), 513–537.

[20] P. A. B. Pleasants. Non-repetitive sequences. *Proc. Cambridge Phil. Soc.* **68** (1970), 267–274.

[21] A. Thue. Über die gegenseitige Lage gleicher Teile gewisser Zeichenreihen. *Norske vid. Selsk. Skr. Mat. Nat. Kl.* **1** (1912), 1–67. Reprinted in *Selected Mathematical Papers of Axel Thue*, T. Nagell, editor, Universitetsforlaget, Oslo, 1977, pp. 413–478.

[22] D. L. Van, D. G. Thomas, K. G. Subramanian, and R. Siromoney. Bi-infinitary codes. *RAIRO Inform. Théor. App.* **24** (1990), 67–87.

[23] M.-w. Wang and J. Shallit. An inequality for non-negative matrices. *Linear Algebra and Its Applications* **290** (1999), 135–144.

[24] T. Zech. Wiederholungsfreie Folgen. *Z. Angew. Math. Mech.* **38** (1958), 206–209.