INFORMATION AND COMPUTATION **83**, 140–151 (1989)

Optimal Word Chains for the Thue–Morse Word*

A. ARNOLD

Université Bordeaux I, Laboratoire d'Informatique,[†]
351, cours de la Libération, F33405 Talence, France

AND

S. BRLEK[‡]

Université du Québec à Montréal,
Département de Mathématiques et Informatique, CP 8888,
Succursale A, Montréal, Québec H3C 3P8

Word chains are an extension of addition chains to words and can be used as a complexity measure for languages. Let $\Sigma = \{a, b\}$ and φ be the morphism $\varphi: \Sigma^* \to \Sigma^*$ given by $\varphi(a) = ab$ and $\varphi(b) = ba$. We study word chains for the iterates $\varphi^n(a)$ of the Thue–Morse word. The length of optimal word chains for $\varphi^n(a)$ is proved to be $2n - 1$, and a conjecture on the enumeration of optimal word chains computing $\varphi^n(a)$ is proposed.

1. INTRODUCTION

Fast computation of powers of monomials is a very old problem, and addition chains have been introduced as a general frame for its study (cf. Knuth, 1981). This is nothing but a particular case of the more general problem of optimizing operations in an arbitrary monoid. In order to get a convenient complexity measure for languages. A. A. Diwan (1986) defined the notion of word chain on the free monoid Σ^* over a finite alphabet Σ. This notion appears as a natural generalization of addition chains, and is defined as follows. A sequence of words

$$w_1, ..., w_r$$

* With the support of the PRC "Mathématiques et Informatique," France.

† Unité de Recherche associée au Centre National de la Recherche Scientifique n° 726.

‡ Supported by the PRC, France and FCAR Grant EQ1608, Quebec.

0890-5401/89 $3.00

is a *word chain* if for each w_i, there are indices $j, k < i$ with $w_i = w_j w_k$. (By convention, w_j is a letter of the underlying alphabet if $j \leqslant 0$). The word chain is said to compute a word w if w belongs to the chain. The *chain length* of w is the smallest length of a word chain computing w.

It is well known that the length of a shortest addition chain for some integer n is basically $\log_2(n)$. This is no longer true for word chains. A word of length n over a q-letter alphabet can be computed in $n/\log_q(n)$ steps, and words achieving this bound, up to a constant factor, exist (Berstel and Brlek, 1987). Regularities in words play a major role, since they can be used to improve the chain length. In (Berstel and Brlek, 1987), it is shown that there is a clear improvement in some cases. Here, we prove Diwan's conjecture: the length of optimal chains for the iterates $\varphi^n(a)$ for the Thue–Morse word is $2n-1$, where φ is the morphism $\varphi\colon \Sigma^* \to \Sigma^*$ given by $\varphi(a) = ab$ and $\varphi(b) = ba$.

Definitions and notations are fixed in Section 2, which contains some useful combinatorial properties of the Thue–Morse word as well. Section 3 contains the description of some operations on word chains used in the last section. Section 4 deals mainly with the proof of Diwan's conjecture. An almost complete description of optimal chains is presented, but a conjecture on the number of optimal chains is left.

2. Definitions and Notations

Let Σ be a q-letter alphabet. A *word chain* over Σ is a set

$$\mathbf{c} = \{w_{1-q}, \ldots, w_0, w_1, \ldots, w_r\} \tag{1}$$

of words such that $\Sigma = \{w_{1-q}, \ldots, w_0\}$, and for each i $(1 \leqslant i \leqslant r)$, there exist j, k such that

$$w_i = w_j w_k. \tag{2}$$

Remark that a word chain is, here and from now on, defined as a **set** instead of a sequence as usual (Berstel and Brlek, 1987; Diwan, 1986). This is not really different since any set can be transformed into a sequence by ordering its elements according to length. However, using sets instead of sequences allows the simplification of some proofs, and overall, the final conjecture is about chain sets rather than chain sequences.

In order to avoid confusion with concatenation in Σ^*, when a word w_i in $\mathbf{c}$ satisfies condition (2), it will be said to *factorize* in $\mathbf{c}$, and the factorization will be denoted, whenever needed, by

$$w_i = w_j \circ w_k.$$

Clearly, addition chains are exactly word chains over a 1-letter alphabet. The *length* of the word chain $\mathbf{c}$ is the integer r and is equal to $|\mathbf{c} - \Sigma|$. The word chain $\mathbf{c}$ is said to *compute* a word w if $w = w_i$ for some $i \in \{1 - q, ..., r\}$. The *chain length* of a word w is the integer

$$l(w) = \min\{|\mathbf{c} - \Sigma| : \mathbf{c} \text{ computes } w\}. \tag{3}$$

Straightforward extensions are given for sets of words as follows. For every finite non empty set $S \subset \Sigma^*$, $\mathbf{c}$ computes S, if and only if

$$\forall s \in S, \qquad s \in \mathbf{c},$$

and the chain length $l(S)$ of S, is defined as in (3).

Observe that in chain (1), $|w_i| \leqslant 2^i$ for $0 \leqslant i \leqslant r$. Therefore, for any non-empty word w, $l(w) \geqslant \log(|w|)$. Moreover, it is clear that every nonempty word w is computed from the alphabet in $|w| - 1$ steps, by concatenation of one letter at each step. We shall see later that more precise bounds can be given. In particular, when a word has regularities, better results are in general achieved.

We recall now from Lothaire (1983), some basic terminology on words which shall be used in the text. The empty word is denoted by ε. Then, given a word w, a factor u of w is a word such that w factorizes in Σ^*, that is

$$\exists x, \; y \in \Sigma^* : w = xuy.$$

If $x = \varepsilon$ (resp. $y = \varepsilon$), then u is a *prefix* (resp. *suffix*) of w. The set of factors of length h of w is denoted $\mathscr{F}_w(h)$, and the set of all nonempty factors by $\mathscr{F}_w$. The "mirror image" ($\tilde{}$) operation is defined, as usual, by the relations

$$\tilde{a} = a; \qquad \tilde{b} = b; \qquad w = w_1 w_2 \Leftrightarrow \tilde{w} = \tilde{w}_2 \tilde{w}_1.$$

and, on the two-letters alphabet $\{a, b\}$, the inversion ($\bar{}$) is the monoid homomorphism generated by

$$\bar{a} = b; \qquad \bar{b} = a.$$

Let $\Sigma = \{a, b\}$ and φ be the morphism $\varphi : \Sigma^* \to \Sigma^*$ given by $\varphi(a) = ab$ and $\varphi(b) = ba$. The Thue–Morse word $\mathbf{M}$ is defined as the limit of iterates of φ as follows:

$\varphi^2(a) = abba$

$\varphi^3(a) = abbabaab$

$\varphi^4(a) = abbabaabbaababba$

$\vdots$

$\mathbf{M} = abbabaabbaababbabaababbaabbabaabbaababbaabbabaababbabaabbaabab....$

The combinatorial properties of **M** used in the text will be listed below. We omit the proofs and refer the reader to the literature (for instance, Brlek, 1987 or Lothaire, 1983). In particular, an alternate recursive definition of **M** is given by the algorithm in Property 1, which yields, as we shall see later, an optimal word chain for $\varphi^n(a)$.

PROPERTY 1. *Let $U_i = \varphi^i(a)$ and $V_i = \varphi_i(b)$. Then, the following relations hold*:

$$\begin{array}{rcl} U_0 = a; & & V_0 = b; \\ U_{n+1} = U_n V_n; & & V_{n+1} = V_n U_n; \\ U_n = \overline{V_n} & \textit{and} & V_n = \overline{U_n}; \\ U_{2n} = \tilde{U}_{2n}; & & V_{2n} = \tilde{V}_{2n}; \\ U_{2n+1} = \tilde{V}_{2n+1}. & & \end{array}$$

Also, **M** *is cube-free and has no overlapping factors, e.g., factors of the form xuxux.*

Let us say that $w \in \mathscr{F}_{\mathbf{M}}$ is of *even type* (resp. *odd type*) if and only if there exist $u \in \Sigma^*$ of even length (resp. odd length) and $v \in \Sigma^*$ such that $uwv = U_n$ for some n. Every word in $\mathscr{F}_{\mathbf{M}}$ is of some type, possibly both as a and b. The type of words in $\mathscr{F}_{\mathbf{M}}$ are characterized below. First let us state the following property which is an immediate consequence of the definition of $U_n = \varphi^n(a)$.

PROPERTY 2. *If $w \in \mathscr{F}_{\mathbf{M}}$ is of even type, then*

$$w = \begin{cases} \varphi(v) & \textit{if } |w| \textit{ is even} \\ \varphi(v)\,y & \textit{if } |w| \textit{ is odd,} \end{cases}$$

and, if w is of odd type, then

$$w = \begin{cases} x\varphi(v)\,y & \textit{if } |w| \textit{ is even} \\ x\varphi(v) & \textit{if } |w| \textit{ is odd,} \end{cases}$$

where $x, y \in \Sigma$, and $v \in \mathscr{F}_{\mathbf{M}}$.

PROPERTY 3. *The type of the factors is given in the conditions*:

(i) *a, b, ab, ba, aba, and bab are of both types*;

(ii) *aab and bba are only of odd type*;

(iii) *abb and baa are only of even tye*;

(iv) *every word w, such that $|w| \geqslant 4$, has only one type.*

Proof. The first three points are obvious. Now, assume that $w = x_1x_2x_3x_4w'$ is of both types. Then, there exist $u, v, u', v' \in \Sigma^*$, $x \in \Sigma$, with u and u' of even length, such that $uwv = U_n$ and $u'xwv' = U_n$. Therefore, there exists $z_1, z_2, z_3, z_4 \in \Sigma$ such that $\varphi(z_1) = x_1x_2$, $\varphi(z_2) = x_3x_4$, $\varphi(z_3) = xx_1$, and, $\varphi(z_4) = x_2x_3$. It implies $x = \bar{x}_1 = x_2 = \bar{x}_3 = x_4$, hence $u'xwv'$ contains the factor $x\,\bar{x}\,x\,\bar{x}\,x$ which is impossible. ∎

3. Word Chains for $\varphi^n(a)$

As already mentioned, word chains take into account the structure of the factors of the word they compute. It will be shown, here, that the chain length of $\varphi^n(a)$ can be improved, using regularities. We recall without proof the following result and we apply it to $\varphi^n(a)$.

Proposition 3.1. (Berstel and Brlek, 1987). *Let w be a word of length n, and assume that there are constants $C \geqslant 1$, $p \in \mathbb{N}$, $p \geqslant 1$ such that*

$$|\mathcal{F}_w(h)| \leqslant Ch^p \qquad (1 \leqslant h \leqslant \lceil n^{1/(p+1)} \rceil).$$

Then

$$l(w) < 6Cn^{p/(p+1)}.$$

The numbers of factors of $\mathbf{M}$ is a linearly growing function (Brlek, 1987), and is bounded by

$$\mathcal{F}_{\mathbf{M}}(m) \leqslant \tfrac{10}{3}m.$$

Hence, the chain length, according to Proposition 3.1, satisfies the inequality

$$l(\varphi^n(a)) < 6\,\tfrac{10}{3}\,(2^n)^{1/2}.$$

As we shall see in Section 4, the bound given here is not optimal.

Proposition 3.2. *If $\mathbf{c}$ is a chain computing $\varphi^n(a)$, then $\Sigma \cup \varphi(\mathbf{c})$ computes $\varphi^{n+1}(a)$, and $|\Sigma \cup \varphi(\mathbf{c})| = |\mathbf{c}| + 2$. Moreover,*

$$l(\varphi^{n+1}(a)) \leqslant |\varphi(\mathbf{c})|.$$

Proof. Let $\mathbf{c} = \{a, b, w_1, ..., \varphi^n(a)\}$. Then, taking the image under φ, we get $\Sigma \cup \varphi(\mathbf{c}) = \{a, b, ab, ba, \varphi(w_1), ..., \varphi^{n+1}(a)\}$, where $\varphi(w_i) = \varphi(w_jw_k) = \varphi(w_j)\,\varphi(w_k)$. Moreover, $l(\varphi^{n+1}(a)) \leqslant |\Sigma \cup \varphi(\mathbf{c}) - \Sigma| = |\varphi(\mathbf{c})|$. ∎

PROPOSITION 3.3. *Let* $\mathbf{c}$ *be a chain computing* $\varphi^n(a)$, *such that all its elements but* a *and* b *are of even length. Then, there exist* $\mathbf{c}'$, *a chain computing* $\varphi^{n-1}(a)$, *such that*

$$|\mathbf{c}'| \leqslant |\mathbf{c}| - 2 \qquad \text{and} \qquad \varphi(\mathbf{c}') \subset \mathbf{c}.$$

Proof. If $w = w_1 \circ w_2$ is of even type and if w_1 and w_2 are of even length, then w_1 and w_2 are of even type too. Hence, $\varphi^n(a)$ can be computed by a subset of $\mathbf{c}$ containing a, b and only words of even type and even length. Let $\{a, b\} \cup \{w_1, ..., w_k\}$ be this subset. By Property 2, for every i there exists v_i such that $w_i = \varphi(v_i)$ and let $\mathbf{c}'$ be $\{v_1, ..., v_k\}$. It remains to prove that $\mathbf{c}'$ is a chain computing $\varphi^{n-1}(a)$. The only nontrivial point is to prove the inclusion $\Sigma \subset \mathbf{c}'$, i.e., ab and ba are in $\mathbf{c}'' = \{w_1, ..., w_k\}$. Since all these words are of even length, they are products of words of length 2 in $\mathbf{c}''$. Hence $\mathbf{c}''$ contains ab and ba. ∎

A mapping $\Psi: \mathscr{F}_{\mathbf{M}} \to \mathscr{P}(\mathscr{F}_{\mathbf{M}})$ is defined on the set of factors of the Thue–Morse word $\mathbf{M}$, with values in its power set, by

$$\begin{aligned}\Psi(w) = {} & \{\bar{x}x\varphi(v)\colon w = x\varphi(v), \text{ and } w \text{ of odd type and odd length}\}\\ & \cup \{\varphi(v)\colon w = \varphi(v)\,y, \text{ and } w \text{ of even type and odd length}\}\\ & \cup \{\varphi(v)\colon w = \varphi(v), \text{ and } w \text{ of even type and even length}\}\\ & \cup \{\bar{x}x\varphi(v)\colon w = x\varphi(v)\,y, \text{ and } w \text{ of odd type and even length}\}\end{aligned}$$

where $x, y \in \Sigma$, and $v \in \mathscr{F}_{\mathbf{M}}$.

This mapping is then extended to the set $\mathscr{P}(\mathscr{F}_{\mathbf{M}})$ in the natural way. As an example, $\Psi(w)$ is given on words of length $\leqslant 3$, wich will be used later:

$$\begin{aligned}&\Psi(a) = \{ba, \varepsilon\}; && \Psi(aab) = \{baab\};\\ &\Psi(b) = \{ab, \varepsilon\}; && \Psi(aba) = \{baba, ab\};\\ &\Psi(ab) = \{ab, ba\}; && \Psi(abb) = \{ab\};\\ &\Psi(ba) = \{ab, ba\}; && \Psi(baa) = \{ba\};\\ &\Psi(aa) = \{ba\}; && \Psi(bab) = \{abab, ba\};\\ &\Psi(bb) = \{ab\}; && \Psi(bba) = \{abba\}.\end{aligned}$$

For all other words, by Property 3, $|\Psi(w)| = 1$, and we will denote the unique element of $\Psi(w)$ by $\mathbf{w}$.

LEMMA 3.4. *Let* $w = w_1 w_2 \in \mathscr{F}_{\mathbf{M}}$. *Then* $\Psi(w) \subset \Psi(w_1)\,\Psi(w_2)$.

Proof. There are four cases to consider, according to the parity of the lengths of w_1 and w_2. All these cases are proved in the same way, so we shall only deal with the case $|w_1|$ odd and $|w_2|$ even.

First, if $w_1 w_2$ is of even type, then w_1 is of even type and w_2 of odd type, and by Property 2 and from the definition of Ψ, we have

$$w_1 = \varphi(v_1)\, y_1, \qquad \varphi(v_1) \in \Psi(w_1);$$
$$w_2 = x_2 \varphi(v_2)\, y_2, \qquad \bar{x}_2 x_2 \varphi(v_2) \in \Psi(w_2);$$

and $w = \varphi(v_1)\, y_1 x_2 \varphi(v_2)\, y_2$. Since w is of even type, $w = \varphi(v)\, y_2$, with $v = v_1 z v_2$ and $\varphi(z) = y_1 x_2$. Hence, $y_1 = \bar{x}_2$ and $\varphi(v) \in \Psi(w)$; but $\varphi(v) = \varphi(v_1)\, \bar{x}_2 x_2 \varphi(v_2) \in \Psi(w_1)\, \Psi(w_2)$.

Second, if $w_1 w_2$ is of odd type, w_1 is of odd type and w_2 of even type, and

$$w_1 = x_1 \varphi(v_1), \qquad \bar{x}_1 x_1 \varphi(v_1) \in \Psi(w_1);$$
$$w_2 = \varphi(v_2), \qquad \varphi(v_2) \in \Psi(w_2);$$

and $w = x_1 \varphi(v_1 v_2)$. Since w is of odd type, one has $\bar{x}_1 x_1 \varphi(v_1 v_2) \in \Psi(w)$, but $\bar{x}_1 x_1 \varphi(v_1 v_2) \in \Psi(w_1)\, \Psi(w_2)$.

Thus, $\Psi(w) \subset \Psi(w_1)\, \Psi(w_2)$. ∎

LEMMA 3.5. *Let* $\mathbf{c}$ *be a chain computing* $\varphi^n(a)$. *Then* $\mathbf{c}_* = \Psi(\mathbf{c}) - \varepsilon + \{a, b\}$ *is a chain computing* $\varphi^n(a)$.

Proof. Let $w' \in \mathbf{c}_*$, such that $|w'| > 1$. By definition of $\mathbf{c}_*$, $w' \in \Psi(\mathbf{c})$. Hence, there exist $w \in \mathbf{c}$ such that $w' \in \Psi(w)$. If $|w| = 1$, then $w \in \{a, b\}$ and therefore $w' \in \{ab, ba, \varepsilon\}$. If $|w| > 1$, w factorizes in $\mathbf{c}$ as $w = u \circ v$, and by Lemma 3.4, there exist $u' \in \Psi(u), v' \in \Psi(v)$ such that $w' = u'v' \subset \Psi(u)\, \Psi(v)$. ∎

EXAMPLE. The chain $\mathbf{c} = \{a, b, ab, abb, aab, abba, abbab, abbabaab\}$ computes $\varphi^3(a)$. Then, $\Psi(\mathbf{c}) = \{\varepsilon, ab, ba, baab, abba, abbabaab\}$ and $\mathbf{c}_* = \{a, b, ab, ba, baab, abba, abbabaab\}$ computes $\varphi^3(a)$.

4. OPTIMAL WORD CHAINS FOR $\varphi^n(a)$

Clearly, $l(\varphi^n(a)) \leqslant 2n - 1$, because $2n - 1$ is the length of the particular chain

$$\mathbf{c} = \{a, b, ab, ba, ..., U_i, V_i, ..., U_n\}, \tag{4}$$

which computes $U_n = \varphi^n(a)$ according to Property 1. The following conjecture was proposed by A. A. Diwan (1986).

Conjecture (Diwan, 1986). The length of a shortest chain computing $\varphi^n(a)$ is

$$l(\varphi^n(a)) = 2n - 1.$$

The next result is immediate.

PROPOSITION 4.1. *Let* $S = \{\varphi^i(a): 1 \leqslant i \leqslant n\}$ *and* $S' = \{\varphi^n(a), \varphi^n(b): 1 \leqslant i \leqslant n\}$ *then*:

(i) $l(S) = 2n - 1$,

(ii) $l(S') = 2n$.

Proof. (i) In the chain $\mathbf{c} = \{a, b, \varphi(a), ..., \varphi^2(a), ..., \varphi^i(a), ..., \varphi^{i+1}(a), ..., \varphi^n(a)\}$, for each i, $|\varphi^{i+1}(a)| = 2\,|\varphi^i(a)|$. The chain $\mathbf{c}$ is completed according to the convention that, between $\varphi^i(a)$ and $\varphi^{i+1}(a)$, only the words needed to compute $\varphi^{i+1}(a)$ are written down. Therefore, the length of each of these words is strictly inferior to $|\varphi^{i+1}(a)|$. But $\varphi^{i+1}(a)$ is not a square word. Hence, there is at least one word between $\varphi^i(a)$ and $\varphi^{i+1}(a)$. Consequenctly, $l(S) \geqslant 2n - 1$. On the other hand, the chain given by (4) computes S and its length is $2n - 1$. Point (ii) is easy to get by induction. ∎

Diwan's conjecture will be proved now in two steps; first, we show it is true for $n \leqslant 3$, and then that it still holds for $n > 3$.

THEOREM 4.2. *The length of a shortest chain computing* $\varphi^n(a)$, $1 \leqslant n \leqslant 3$, *is*

$$l(\varphi^n(a)) = 2n - 1.$$

Proof. It is clear that for $n = 1$, $l(ab) = 1$, and for $n = 2$, $l(abba) = 3$. If $n = 3$, then $\varphi^n(a) = abbabaab$. We proceed by contradiction on all possible factorizations. Suppose $l(abbabaab) < 5$, all of the four cases below are rejected:

1. $abba \circ baab$: since $l(abba) = 3$, we would have to compute $baab$ in no steps, which is clearly impossible.

2. $abb \circ abaab$: two steps are needed to compute abb; $abaab$ is not computable with one more step.

3. $ab \circ babaab$: two steps, ab and $\circ$, are already fixed; clearly, $babaab$ cannot be computed in less than two steps.

4. $a \circ bbabaab$: the reader should easily deduce that $bbabaab$ is not computable with 3 more steps, using the same procedure, that is by checking all possible factorizations.

Similar arguments are valid for the symmetric factorizations. ∎

The next step consists in showing that, from every chain $\mathbf{c}$ computing $\varphi^n(a)$, it is possible to construct a chain $\mathbf{c}_*$ with all factors of even length, such that the chain length is not increased. This will be achieved with the morphism Ψ.

Let $\mathbf{c} = \mathbf{c}_1 \cup \mathbf{c}_2 \cup \mathbf{c}_3 \cup \mathbf{c}_4$ be a partition of $\mathbf{c}$, such that $\mathbf{c}_1$ (resp. $\mathbf{c}_2$; $\mathbf{c}_3$) is the subset of elements in $\mathbf{c}$ of length 1 (resp. 2; 3), $\mathbf{c}_4$ is the subset of elements of length $\geqslant 4$, with respective cardinalities $k_i = |\mathbf{c}_i|$, for $i = 1, 2, 3, 4$. Then, the chain $\mathbf{c}_* = \Psi(\mathbf{c}) - \varepsilon + \{a, b\}$ can be expressed as

$$\begin{aligned} \mathbf{c}_* &= \Psi(\mathbf{c}_1) \cup \Psi(\mathbf{c}_2) \cup \Psi(\mathbf{c}_3) \cup \Psi(\mathbf{c}_4) \cup \{a, b\} - \varepsilon \\ &= \{a, b, ab, ba\} \cup \Psi(\mathbf{c}_3) \cup \Psi(\mathbf{c}_4) \\ &= \{a, b, ab, ba\} \cup \Psi(\mathbf{c}_3) \cup \mathsf{C}_4 \end{aligned}$$

where $\mathsf{C}_4 = \{\mathsf{W} : w \in \mathbf{c}_4\}$.

Let us denote by k_4 the cardinal $|\mathsf{C}_4|$ of C_4 and by k_3 the cardinal of $\Psi(\mathbf{c}_3) - \{ab, ba\}$. We have $\mathsf{k}_4 \leqslant k_4$, $\mathsf{k}_3 \leqslant k_3$ (because if the image by Ψ of some word of length 3 has two elements, one of them is in $\{ab, ba\}$), and $|\mathbf{c}_*| \leqslant 4 + (\mathsf{k}_3 + \mathsf{k}_4)$.

THEOREM 4.3. *Let $\mathbf{c}$ be a chain computing $\varphi^n(a)$, $n \geqslant 4$, and $\mathbf{c}_* = \Psi(\mathbf{c}) + \{a, b\} - \varepsilon$. Then $\mathbf{c}_*$ is a word chain computing $\varphi^n(a)$ with all elements, except a and b, of even length, and such that $|\mathbf{c}_*| \leqslant |\mathbf{c}|$.*

Proof. Suppose, to the contrary, that the assumption $|\mathbf{c}_*| > |\mathbf{c}|$ holds. Then

$$4 + (\mathsf{k}_3 + \mathsf{k}_4) \geqslant |\mathbf{c}_*| > |\mathbf{c}| = 2 + k_2 + (k_3 + k_4),$$

from which we get

$$2 - k_2 > (k_3 + k_4) - (\mathsf{k}_3 + \mathsf{k}_4).$$

But

$$(k_3 + k_4) \geqslant (\mathsf{k}_3 + \mathsf{k}_4).$$

Therefore, the following inequality holds

$$2 - k_2 > (k_3 + k_4) - (\mathsf{k}_3 + \mathsf{k}_4) \geqslant 0.$$

Finally, this implies that

$$k_2 \leqslant 1.$$

Since k_2 cannot be 0, we have

$$k_2 = 1 \tag{*}$$

and consequently,

$$1 > (k_3 + k_4) - (\mathbf{k}_3 + \mathbf{k}_4) \geqslant 0,$$

which implies

$$(k_3 + k_4) = (\mathbf{k}_3 + \mathbf{k}_4). \tag{**}$$

This means that there is a unique factor of length 2 in the chain $\mathbf{c}$. To identify it, let w be the smallest element of $\mathbf{c}$, with abb as prefix (such an element exists since abb is a prefix of $\varphi^n(a)$). If $w = a \circ w'$, then $\Psi(w') = \Psi(w)$. But this contradicts the injective condition (**), hence $w = ab \circ u$, and $\mathbf{c}_2 = \{ab\}$.

An immediate consequence is the following: neither of the factors baa and bba is computable, since, if it were so, the condition (*) would be violated; the factor abb is not computable since $\Psi(abb) = ab$, hence $\mathbf{k}_3 < k_3$ which violates condition (**).

Let w be now the smallest factor of $\varphi^n(a)$ in $\mathbf{c}$ and containing the factor $bbaa$. It will be shown that w cannot be factorized in $\mathbf{c}$ and satisfy conditions (*) and (**). There are three possible factorizations $w = p \circ s$:

1. $w = p \circ s = ub \circ baav$. The suffix s cannot be factorized: $s = b \circ aav$ is rejected since, if $v = \varepsilon$ then $aa \in \mathbf{c}_2$ contradicts condition (*), and when $v \neq \varepsilon$ then $\Psi(s) = \Psi(aav)$, hence (**) is violated; $s = ba \circ abv$ implies $ba \in \mathbf{c}_2$, and contradicts (*); $s = baa \circ v$ is rejected since baa is not computable.

2. $w = p \circ s = ubb \circ aav$. Here, p does not factorize in $\mathbf{c}$: $u = \varepsilon$ contradicts (*); if $u \neq \varepsilon$ then $p = u'abb$ and, $p = u'ab \circ b$ contradicts (**), $p = u'a \circ bb$ contradicts (*), while $p = u' \circ abb$ is rejected since abb is not computable.

3. $w = p \circ s = ubba \circ av$. Again p cannot be factorized: $p = u \circ bba$ is rejected since bba is not computable; $p = ub \circ ba$ contradicts (*); $p = ubb \circ a$ is rejected since it has been shown in 2, that ubb is not computable.

We conclude the proof by remarking that the word w exists if $n \geqslant 4$ because $bbaa$ is a factor of $\varphi^n(a)$. But w is not factorizable under the hypothesis $|\mathbf{c}_*| > |\mathbf{c}|$, hence $\mathbf{c}$ is not a word chain. Contradiction. ∎

Putting together the results of Theorlems 4.2 and 4.3, Diwan's conjecture is established.

COROLLARY 1. *The length of a shortest chain computing $\varphi^n(a)$ is*

$$l(\varphi^n(a)) = 2n - 1.$$

Proof. In view of Theorem 4.2, it remains only to show it in the case $n>3$. We proceed by contradiction. Let m be the smallest integer such that a minimal chain $\mathbf{c}$ for $\varphi^m(a)$ verifies $|\mathbf{c}|-2=l(\varphi^m(a))<2m-1$. The previous theorem states that there exist a chain $\mathbf{c}_*$ with all elements, but a and b, of even length such that $|\mathbf{c}_*|\leqslant|\mathbf{c}|$. By Proposition 3.3, there exist $\mathbf{c}'$ computing $\varphi^{m-1}(a)$ with $|\mathbf{c}'|\leqslant|\mathbf{c}_*|-2$ and therefore

$$l(\varphi^{m-1}(a))\leqslant|\mathbf{c}'|\leqslant|\mathbf{c}_*|-2\leqslant|\mathbf{c}|-2<2m-3.$$

Contradiction. ∎

In Proposition 3.2, it has been established that new chains are constructed by morphism iteration, but preserving minimality was not ensured. But, according to Corollary 1, this is true now for the computation of the iterates $\varphi^n(a)$.

COROLLARY 2. *If* $\mathbf{c}$ *is a minimal chain computing* $\varphi^n(a)$, *then* $\Sigma\cup\varphi(\mathbf{c})$ *is a minimal chain computing* $\varphi^{n+1}(a)$.

Proof. If $\mathbf{c}$ is minimal, then from Corollary 1, $|\mathbf{c}|-2=2n-1$. By Proposition 3.3, $\mathbf{c}'=\Sigma\cup\varphi(\mathbf{c})$ computes $\varphi^{n+1}(a)$ and

$$|\mathbf{c}'|-2=|\Sigma\cup\varphi(\mathbf{c})|-2=|\mathbf{c}|=2n+1. \quad ∎$$

COROLLARY 3. $l(\{\varphi^n(a),\varphi^n(b)\})=2n$.

Proof. Since $U_n=\bar{V}_n$ (Property 1), $l(\varphi^n(b))=2n-1$ obviously. Therefore, we have $l(\{\varphi^n(a),\varphi^n(b)\})>2n-1$. But the chain given by (4) extends to the chain

$$\mathbf{c}^+=\{a,b,ab,ba,...,U_i,V_i,...,U_n,V_n\} \tag{5}$$

which computes the set $\{\varphi^n(a),\varphi^n(b)\}$ and whose length is $2n$. ∎

Table I lists the number of chains of each length for $\varphi^n(a)$. The results were computed on a SUN 3/50 workstation by systematic enumeration. It contains the particular results:

1. $\Sigma\mathbf{C}_r(\varphi^n(a))=\text{Catalan}(2^n-1)$, $n\leqslant 3$.
2. $\mathbf{C}_{\min}(\varphi^n(a))=19$, $n=3, 4, 5, 6$.

The first is not surprising, since $\varphi^n(a)$ has no factor of length 3, occuring more than once. The second is remarkable, since, according to Corollary 2, it would mean that φ is stable for minimal chains. Therefore, we propose the conjecture:

Conjecture 4.4. $\mathbf{C}_{\min}(\varphi^n(a))=19$, $n\geqslant 3$.

TABLE I

$C_r(\varphi^n(a))$ = Number of Chains of Length r for $\varphi^n(a)$

		Length													
n	$\lvert\varphi^n(a)\rvert$	1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	2	1													
2	4			5											
3	8					19	116	294							
4	16							19	342	?	?	?	?	?	?
5	32									19	?	?	?	?	?
6	64											19	?	?	?

Acknowledgments

Many improvements came from fruitful discussions with Jean Berstel, François Bergeron, and Christine Duboc. We are also indebted to Eduardo Dubuc, who produced an efficient program to compute word chains and tested the conjectures.

Received October 1988; accepted November 16, 1988

References

1. Berstel, J., and Brlek, S. (1987), On the length of word chains, *Inform. Process. Lett.* **26**, No. 1, 23–28.
2. Brlek, S. (1987), Enumeration of factors in the Thue–Morse word, *in* "Actes du Colloque de Combinatoire et Informatique de l'Université de Montréal, April 27th–May 2nd," *Discrete Appl. Math.*, in press.
3. Diwan, A. A. (1986), "A New Combinatorial Complexity Measure for Languages," Tata Institute, Bombay, India.
4. Knuth, D. E. (1981), "The Art of Computer Programming," Vol. 2, 2nd ed., Addison–Wesley, Reading, MA.
5. Lothaire, M. (1983), "Combinatorics on Words," Addison–Wesley, Reading, MA.