数理解析研究所講究録
第 666 巻 1988 年 225-234

Invariant sets for substitution

Taishin NISHIDA* and Youichi KOBUCHI**
西田泰伸　小渕洋一

* International Institute for Advanced Study of Social Information Science, Fujitsu Limited
** Department of Biophysics, Faculty of Science, Kyoto University

Introduction

Let F be a relation on a countable set X. Then F determines a function from 2^X to 2^X (again denoted by F) as follows:

For $Z \in 2^X$, $F(Z) = \{y \in X \mid \exists x \in Z, \ x\ F\ y\}$.

We can thus define an n-fold product F^n of F as follows:

F^0 is the identity function on 2^X,

$F^1 = F$, and

$F^{n+1} = F(F^n)$.

We shall use the following notations:

$F^* = \bigcup_{k \in \mathbf{N}} F^k$, $F^+ = F(F^*)$, and $F^{[n]} = \bigcup_{k \in [n]} F^k$,

where **N** denotes the set of non-negative integers and [n], the set {0, 1, ..., n-1} for any positive integer n. We shall not distinguish a singleton set {x} from an element x. Also, we refer to a point Z in 2^X as a subset $Z \subset X$ whenever it is appropriate.

A subset $Z \subset X$ is called <u>invariant</u> for F if it is a fixed point with respect to F, i.e., $F(Z) = Z$.

We introduce ascendability concepts with respect to the function F as follows. Let Z be a subset of X. An element $x \in Z$ is said to be ascendable in Z if there exists an infinite sequence $x_0=x, x_1, \ldots, x_n, \ldots$ (not necessarily distinct) in Z such that $x=x_0$ and $x_i \in F(x_{i+1})$ $(i \geq 0)$. Also, $x \in X$ is called ascendable if it is ascendable in some $Z \subset X$. A subset Z is called ascendable if every $x \in Z$ is ascendable in Z. Then it is shown that an invariant set Z is the F^+ image of some ascendable subset K, i.e., $Z = F^+(K)$ (Lemma 1.3).

Besides the above general characterization, we can give more detailed structure of invariant sets when F is defined by a substitution. Consider an element $x \in X$ called a repeatable point that satisfies $x \in F^+(x)$. It is obvious that for any repeatable point x, the set $F^+(x)$ is ascendable and $F^+(F^+(x)) = F^+(x)$ because $F^+(x) \subset F^+(F^+(x)) \subset F^+(x)$. Hence $F^+(x)$ is invariant. Then for any set S of repeatable points, the set $F^+(S)$ is also invariant. The converse is, however, not always the case. That is, in general, there is an ascendable element x such that there is no repeatable point z satisfying $x \in F^+(z)$.

The main result of this note is that if X is a free monoid over a finite set (or the set of all words over an alphabet) and F is a substitution on it, then for any ascendable element $x \in X$ there does exist a repeatable point z such that $x \in F^+(z)$ (Lemma 4.1). We also prove that any invariant set Z for a substitution is characterized as $Z = F^+(S)$ where S is a set of repeatable points (Theorem 4.3).

1. Invariant set for a multivalued mapping

In this section, we prove several properties of invariant sets and ascendable sets.

Lemma 1.1. A subset Z of X is ascendable if and only if $Z \subset F(Z)$.

Proof. If part : If $Z \subset F(Z)$ then for every $x \in Z$ there exists some $y \in Z$ such that $x \in F(y)$. This guarantees that x is ascendable in Z.

Only if part : Let $x \in Z$. Since x is ascendable in Z, there is $y \in Z$ such that $x \in F(y)$. Thus $x \in F(Z)$.

The following lemmas show the relations between invariant sets and ascendable sets.

Property 1.2. 1) $F(Z) = Z$ if and only if $F^+(Z) = Z$.

2) If Z is invariant, then it is ascendable.

3) If Z_1 and Z_2 are invariant, then so is $Z_1 \cup Z_2$.

Lemma 1.3. A subset Z of X is invariant if and only if $Z = F^+(K)$ for some ascendable subset K of X.

Proof. Only if part: Since $Z = F(Z) = F^+(Z)$ and Z is ascendable, let $K = Z$.

If part: Since K is ascendable, we have $K \subset F(K)$ by Lemma 1.1. This implies $K \subset F^2(K)$ ..., i.e., $K \subset F^+(K)$ and hence $F^+(K) = K \cup F^+(K)$. Then, $F(Z) = F(F^+(K)) = F(K \cup F^+(K)) = F^+(K) = Z$.

2. Substitution over a finite alphabet

As we stated in Introduction, our main concern is the invariant sets for a substitution over a finite alphabet. In this section we give some basic notations of substitutions.

Let Σ be a finite set, which is called an <u>alphabet</u>. An element of Σ is called a <u>letter</u>. The set of all words over Σ, including the empty word 1, is denoted by Σ^*.

A subsequence of a word s is called a sparse subword of s or, for short, a <u>subword</u> of s. The <u>length</u> of a word s is denoted by $|s|$. If V is any subset of Σ, $|s|_V$ denotes the number of occurrences of letters of V in s.

Definition. A relation F on Σ^* is said to be a substitution if it satisfies the following conditions.

i) $F(1)=1$,

ii) $F(a)\in \Sigma^*$ for every $a\in \Sigma$, and

iii) $F(w) = F(a_1)F(a_2)\ldots F(a_n)$ for every $w = a_1a_2\ldots a_n$ where $a_i\in \Sigma$ for $i=1,2,\ldots,n$.

Let F be a substitution on Σ^*, and let u and v be two words in Σ^* such that $|u| = \ell$. The word v is said to be a <u>descendant</u> of u if v belongs to $F^n(u)$ for some positive integer n. The <u>derivation</u> Δ from u to v is an ℓ-tuple of pairs $\Delta = ((x_1,s_1), (x_2,s_2), \ldots, (x_\ell,s_\ell))$ where $u = x_1\ldots x_\ell$ and $s_i\in F^n(x_i)$ for $i=1,2,\ldots,\ell$.

A substitution F on Σ^* is said to be <u>finite</u> (resp. <u>rational</u>, <u>context free</u>) if F(a) is a finite (resp. rational, context free) subset of Σ^* for every a in Σ.

We assume the reader to be familiar with the basic notions and results of rational and cotext free languages (see, for example. [1]).

3. Some technical results

In this section we establish some technical results, which will be useful in Section 4. Henceforth F will always denote a substitution on Σ^*, where Σ is a finite alphabet.

Repeatable points for a substitution are called repeatable words. We denote by P(F) the set of repeatable words for F, i.e., $P(F) = \{w \mid w \in F^+(w)\}$. We note that a repeatable word u has at least one derivation Δ from u to u. Let $u = x_1 x_2 \ldots x_\ell$ ($x_i \in \Sigma$, $i = 1,2,\ldots,\ell$) and $\Delta = ((x_1,s_1),(x_2,s_2), \ldots, (x_\ell,s_\ell))$ be a repeatable word and its derivation. Then u is said to be decomposed into $s_1 s_2 \ldots s_\ell$.

Many properties of the repeatable words have been studied in [2].

A letter a of Σ is said to be <u>vital</u> if 1 is not the descendant of a, i.e., $1 \notin F^+(a)$. The set of vital letters is denoted by V. The set of <u>non-vital</u> letters is denoted by N, i.e.. $N = \Sigma - V = \{a \mid 1 \in F^+(a)\}$. A letter a of Σ is said to be <u>cyclic</u> if $uav \in F^+(a)$ for some $uv \in N^*$. We denote by C the set of cyclic letters.

Lemma 3.1. There is a positive integer n dependent only on F such that for any word $u = a_1 \ldots a_\ell$ in C^* there exists a repeatable word w in $F^{[n]}(u)$ where $w = s_0 a_1 s_1 \ldots s_{\ell-1} a_\ell s_\ell$ for some $s_0 \ldots s_\ell \in N^*$.

Proof. For any cyclic letter a, there exists a positive integer k_a such that $uav \in F^{k_a}(a)$ for some $uv \in N^*$. Let K be the least common multiple of k_a for any $a \in C$. Let M be the minimum integer such that $1 \in F^M(b)$ for any $b \in N$. Let n be the least multiple of K that is larger than M, then $w = s_0 a_1 s_1 \ldots s_{\ell-1} a_\ell s_\ell$ is in $F^{[n]}(a_1 \ldots a_\ell)$ for some $s_0 \ldots s_\ell \in N^*$ and w is repeatable.

Let $w \neq 1$ be ascendable and let $\sigma = (w_0, w_1, \ldots, w_n, \ldots)$ be an ascending sequence of w, where $w_0 = w$. A <u>derivation trunk</u> of is a sequence of subwords u_i of w_i $(i = 0,1,\ldots)$ which is defined inductively by:

i) $u_0 = w_0$.

ii) Let $\Delta = ((a_1,s_1), \ldots, (a_\ell,s_\ell))$ be a derivation from w_n to w_{n-1}, i.e., $w_n = a_1\ldots a_\ell$ $(a_i \in \Sigma)$ and $w_{n-1} = s_1\ldots s_\ell$ $(s_i \in \Sigma^*)$. Assume that $u_{n-1} = b_1\ldots b_k$ is (inductively) given. Then we have $w_{n-1} = t_0b_1t_1\ldots t_{k-1}b_kt_k$ for some $t_0\ldots t_k \in \Sigma^*$. Let $s_{d_1}, \ldots, s_{d_m}$ be subwords of w_{n-1} which contain at least one b_i's, i.e., for some $j \geq 1$, $s_{d_i} = t'_{f_i}b_{f_i+1}t_{f_i+1}\ldots b_{f_i+j}t'_{f_i+j}$ where t'_{f_i} is a suffix of t_{f_i} and t'_{f_i+j} is a prefix of t_{f_i+j} (see Figure). Then u_n is defined as $u_n = a_{d_1}\ldots a_{d_m}$.

In the remaining of this section, let $w \neq 1$ be an ascending word, $\sigma = (w_0, w_1, \ldots)$ be the ascending sequence of w, and $(u_0, u_1, \ldots)$ be a derivation trunk of σ. Then we have the following properties and lemmas.

Property 3.2. i) $|u_{n-1}| \geq |u_n|$ and $|u_n| > 0$ for any $n > 0$.
ii) w_0 is in $F^n(u_n)$ for any $n \geq 0$.

Property 3.3. There exists a positive integer M such that $|u_M| = |u_{M+i}|$ for any non-negative integer i.

Lemma 3.4. If $u_n = b_1\ldots b_k$, then $w_n = t_0b_1t_1\ldots t_{k-1}b_kt_k$ for some $t_0\ldots t_k \in N^*$.

Proof. We prove this lemma by induction on n. Since $u_0 = w_0$, the lemma holds for $n = 0$. Assume that it is true for some $n > 0$. i.e., $u_n = b_1\ldots b_k$ and $w_n = t_0b_1t_1\ldots t_{k-1}b_kt_k$ for some $t_0\ldots t_k \in N^*$.

Let $w_{n+1} = a_1 \ldots a_\ell$ and $u_{n+1} = a_{d_1} \ldots a_{d_m}$. Let $\Delta = ((a_1, s_1), \ldots, (a\ ,s\ ))$ be the derivation from w_{n+1} to w_n. If $d_j < i < d_{j+1}$ for some j $(1 \leq j < m)$, $i < d_1$, or $d_m < i$, then s_i is a subword of t_p for some p. Since t_p is in N^*, a_i is non-vital. Therefore we have $w_{n+1} = v_0 a_{d_1} v_1 \ldots v_{m-1} a_{d_m} v_m$ for some $v_0 \ldots v_m$ in N^*.

Lemma 3.5. If $u_n = u_{n'}$ for some $n \neq n'$, then u_n is in C^+.

Proof. Assume that $n > n'$. Let $u_n = a_1 \ldots a_\ell$. Then $w_{n'}$ is decomposed into $s_1 a_1 t_1 \ldots s_\ell a_\ell t_\ell$ such that $s_i' a_i t_i' \in F^{n-n'}(a_i)$ where s_i' is a suffix of s_i and t_i' is a prefix of t_i for $i = 1, \ldots, \ell$. Hence a_i is cyclic because $s_i' t_i'$ is in N^* for $i = 1, \ldots, \ell$ from Lemma 3.4.

4. Main theorems

In this section, we first establish the following lemmas, which state close relations between the ascendable words and the repeatable words.

Lemma 4.1. If a word x is ascendable for a substitution F, then there exists a repeatable word v such that $x \in F^+(v)$.

Proof. If $x = 1$, then x is in $F^+(1)$ and 1 is repeatable for any F. Then, assume that $x \neq 1$. Let $\sigma = (x_0, x_1, \ldots)$ be an ascending sequence of x and $(u_0, u_1, \ldots)$ be a corresponding derivation trunk of σ. By Property 3.3, there is a pair u_n and $u_{n'}$ $(n \neq n')$ in the derivation trunk such that $u_n = u_{n'}$. Then $u_n = b_1 \ldots b_\ell$ is in C^+ from Lemma 3.5. Let $v = s_0 b_1 s_1 \ldots s_{\ell-1} b_\ell s_\ell$ be the repeatable word in $F^+(u_n)$ whose existence was proved in Lemma 3.1. By Property 3.2 ii), x is in $F^n(b_1 \ldots b_\ell)$. And we can assume that n is greater than the least integer M such that $1 \in F^M(s_0 \ldots s_\ell)$. Therefore we have

$x \in F^+(v)$.

Lemma 4.2. If a subset X of Σ^* is ascendable for a substitution F, then there exists a subset W of P(F) such that $F^+(X) = F^+(W)$.

Proof. For an ascendable word x, let p(x) be the repeatable word whose existence is ensured by Lemma 4.1, i.e., $v = p(x) \in P(F)$ and $x \in F^+(v)$. Let $W = \{p(x) | x \in X\}$. Then we will show that $F^+(X) = F^+(W)$.

First we show that $F^+(X) \subset F^+(W)$. Let u be a word in $F^+(x)$ for some x in X. Then u is in $F^+(W)$ since $x \in F^+(p(x)) \subset F^+(W)$.

Next we show that $F^+(X) \supset F^+(W)$. Let u be a word in $F^+(v)$ for some v in W. By the definition of W, there is a word x in X such that $v = p(x)$. That is, there is a word u_n in the derivation trunk of the ascending sequence $\sigma = (x_0, x_1, \ldots)$ of x such that $v \in F^+(u_n)$ from the proof of the above lemma. Let x_n be the word in σ which corresponds to u_n. Since the letters contained in x_n which do not occur in u_n are non-vital, we have $v \in F^+(x_n)$. Because X is ascendable, we have $x_n \in X$ and hence the lemma follows immediately.

Then we prove the main theorem.

Theorem 4.3. A subset X of Σ^* is invariant for F if and only if $X = F^+(S)$ for some $S \subset P(F)$.

Proof. If part: For any subset S of P(F), $F^+(S)$ is obviously ascendable. Then $F^+(F^+(S)) = F^+(S) = X$ is invariant by Lemma 1.3.

Only if part: If X is invariant set, then there is an ascendable set Y such that $X = F^+(Y)$. By Lemma 4.2, there exists $W \subset P(F)$ such that $F^+(Y) = F^+(W) = X$.

A subset $Z \subset X$ is said to be <u>maximum</u> <u>invariant</u> for F if Z is invariant and there is no invariant subset $Z' \subset X$ such that $Z \subsetneq Z'$. We denote the maximum invariant set for F by I(F).

Corollary 4.4. The maximum invariant set for a substitution F is the image of the set of all repeatable words by the substitution, i.e..

$$I(F) = F^+(P(F)).$$

References

[1] Hopcroft, J. E. & Ullman, J. D., (1979) Introduction to automata theorey, languages, and computation, Addison-Wesley, Menlo Park.

[2] Nishida, T. & Kobuchi, Y., (1987) Repeatable words for substitution, Theoretical Computer Science, 53, 319-333.

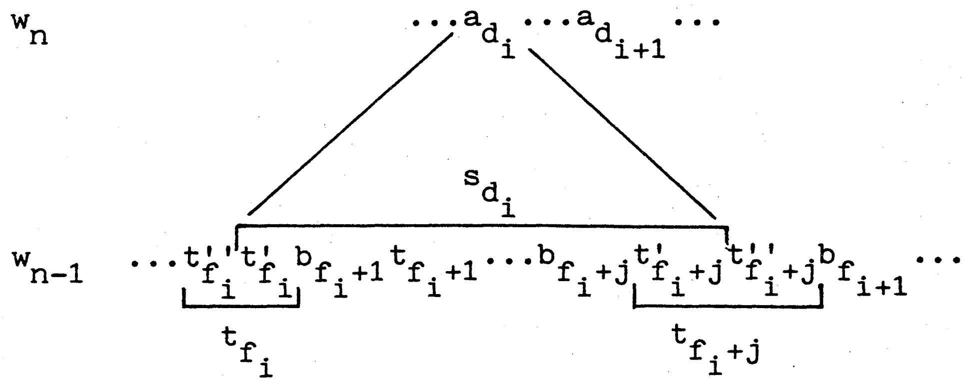

Figure. Derivation from w_n to w_{n-1}, where $f_{i+1} = f_i+j+1$.