ANNALES ACADEMIAE SCIENTIARUM FENNICAE

Series A

I. MATHEMATICA

516

FINITE POWER PROPERTY OF REGULAR LANGUAGES

BY

MATTI LINNA

HELSINKI 1972
SUOMALAINEN TIEDEAKATEMIA

doi:10.5186/aasfm.1972.516

ISBN 951–41–0056–5

Communicated 11 February 1972 by ARTO SALOMAA

KESKUSKIRJAPAINO
HELSINKI 1972

1. Introduction

A regular language L is said to possess the *finite power property* (*f.p.p.*) if and only if the set

$$\{L^i \mid i = 0, 1, 2, \ldots\}$$

is finite. In this paper, we consider the problem of finding an algorithm for deciding whether a given regular language possesses f.p.p. First the problem is solved in the case where L is a regular language over one letter. Next some special cases are studied. A language L $(\lambda \in L)$ accepted by a permutation automaton possesses f.p.p. If $L_{m'} = L_m \cup \{\lambda\}$, where $L_m \neq \emptyset$ is a minimum root, then $L_{m'}$ does not possess f.p.p. Some results concerning the case $L^* = W(V)$ are also obtained. Finally, an algorithm is given to determine whether there exists a word $P \in L^*$ such that $P^i \notin L^i$ for all $i = 1, 2, \ldots$ The last result may give a solution to the general problem. However, we have not been able to show this and the general problem remains open.

2. Preliminaries and notations

Let V be a finite non-empty *alphabet*. A *word* over V is denoted by P or Q and the *empty word* by λ. The *length* of P is denoted by $\lg(P)$. By definition, $\lg(\lambda) = 0$. Denote by $W(V)$ the set of all words over V. A *language* is any subset of $W(V)$. The *empty language* is denoted by $\emptyset$. In the following, we identify an element and its unit set to simplify notation: we may denote simply by P the language $\{P\}$ consisting of the word P. For any two languages L_1, L_2, $L_1 \cup L_2$, $L_1 \cap L_2$, $L_1 - L_2$ and L_1L_2 denote the *union, intersection, difference* and *catenation* of L_1 and L_2, and L^* denotes the *iteration* of L. *Regular expressions* considered are restricted (i.e., use only operators $\cup, \cdot, *$).

A language L is a *star language* if and only if (iff) there exists a language L_1 such that $L = L_1^*$. In that case L_1 is called a *root* of L.

A *finite deterministic automaton* is an ordered quintuple $A = (V, S, F, s_0, f)$, where V is an alphabet, S is a finite non-empty set of *states*,

$F \subseteq S$ is the set of *final states*, $s_0 \in S$ is the *initial state* and f is the *transition function*: $f : S \times V \to S$.

The domain of the transition function f is extended from $S \times V$ to $S \times W(V)$ in the usual way. Extend f further as follows: $f : 2^S \times 2^{W(V)} \to 2^S$, where for every $S_1 \subseteq S$ and $L \subseteq W(V)$

$$f(S_1, L) = \{s \in S | s = f(s_1, P) \text{ for some } s_1 \in S_1, P \in L\}.$$

The language $L(A)$ *accepted* by the automaton A is defined by

$$L(A) = \{P \in W(V) | f(s_0, P) \in F\}.$$

The *state graph* of an automaton A accepting the language L is denoted by $G_A(L)$. The nodes of $G_A(L)$ are the states of A and, for every pair $s, s' \in S$ such that $f(s, a) = s'$ for some $a \in V$, there is in $G_A(L)$ a directed branch leading from s to s' and labelled by a. Let A_0 be the *reduced automaton* accepting L. The corresponding state graph is denoted by $G_0(L)$.

Denote by $G_A^i(L), i = 1, 2, \ldots,$ the graph obtained from $G_A(L)$ by substituting every state s of $G_A(L)$ by s^i. An infinite graph $G_\infty(L)$ consists of an infinite sequence of the graphs G_A^i such that from the final states of $G_A^i(L), i = 1, 2, \ldots,$ there are directed branches labelled by λ to the initial state of $G_A^{i+1}(L)$. Subsets of the states of $G_A^i(L)$ are also marked by the upper index i. The only initial state of $G_\infty(L)$ is s_0^1 and every state s^i, where $i \geqq 1$ and $s \in F$, is a final state. The functions $f_i : 2^{S^k} \times 2^{W(V)} \to 2^{S^i}, k \geqq 1, i \geqq k,$ are defined as follows: for any $S_1 \subseteq S$ and $L \subseteq W(V)$,

$$\begin{aligned} f_i(S_1^k, L) = \{s^i \in S^i | \; & \text{There exist words } P_j, 1 \leqq j \leqq i - k + 1, \\ & \text{such that } P_1 P_2 \ldots P_{i-k+1} \in L, f(s_1, P_1) \in F \\ & \text{for some } s_1 \in S_1, f(s_0, P_j) \in F, 2 \leqq j \leqq i - k, \\ & \text{and } f(s_0, P_{i-k+1}) = s\} \end{aligned}$$

(i.e., $f_i(S_1^k, L)$ is the set of all states $s^i \in S^i$ such that there is a path leading from a state of S_1^k to the state s^i and labelled by a word belonging to L). In the following, the notation $f_i(S_1^k, L)$ often appears in the case where S_1^k and L consist of only one element. Then we write $f_i(s, P)$ instead of $f_i(\{s\}, \{P\})$. The function

$$f_\infty : 2^{S^k} \times 2^{W(V)} \to 2^{\bigcup_{i=k}^{\infty} S^i}$$

is defined by

$$f_\infty(S_1^k, L) = \bigcup_{i=k}^{\infty} f_i(S_1^k, L).$$

Define the operator B as follows: for any $S' \subseteq \bigcup_{i=1}^{\infty} S^i$,

$$B(S') = \{s \in S \mid s^i \in S' \text{ for some } i\}.$$

Obviously, the graph $G_\infty(L)$ accepts a word P iff $B(f_\infty(s_0^1, P)) \cap F \neq \emptyset$ and the language accepted by $G_\infty(L)$ is L^* or $L^* - \lambda$, depending on whether $\lambda \in L$ or $\lambda \notin L$.

Definition. A regular language L possesses the *finite power property* (*f.p.p.*) iff the set

$$\{L^i \mid i = 0, 1, 2, \ldots\}$$

is finite.

We consider the problem of finding an algorithm for determining whether a given regular language $L \subseteq W(V)$ possesses f.p.p.

3. One-letter case

In this section the f.p.p.-problem is solved in the case where the alphabet consists of one letter.

The first lemma holds also for all finite V's.

Lemma 1. *If $L \neq \lambda, \emptyset$ is a finite language or else $L \neq \emptyset$ and $\lambda \notin L$, then L does not possess f.p.p.*

Proof. In the first case,

$$\max\{\lg(P) \mid P \in L^{i-1}\} < \max\{\lg(Q) \mid Q \in L^i\}, \; i = 1, 2, \ldots$$

and, in the second,

$$\min\{\lg(P) \mid P \in L^{i-1}\} < \min\{\lg(Q) \mid Q \in L^i\}, \; i = 1, 2, \ldots$$

Thus, in both cases $L^i \neq L^j$ for all $i \neq j$.

Lemma 2. *Every regular language over the alphabet $\{a\}$ can be expressed in the form*

$$(1) \qquad (a^c)^*(a^{p_1} \cup \ldots \cup a^{p_m}) \cup (a^{q_1} \cup \ldots \cup a^{q_n}),$$

where c, p_i's and q_j's are integers such that $c \geqq 0$, $0 \leqq p_1 < p_2 < \ldots < p_m$ and $0 \leqq q_1 < q_2 < \ldots < q_n$.

Proof. Salomaa [2], pp. 130—131.

Theorem 1. *Let L be an infinite regular language over the alphabet $\{a\}$ and $\lambda \in L$. If a regular expression of the form (1) represents L, then*

$$L^* = L^{(m+n)(c+p_1)+c}.$$

Proof. Since L is infinite, we have $c > 0$ in (1). It suffices to show that $L^* \subseteq L^{(m+n)(c+p_1)+c}$. Thus, assume that $P \in L^*$. Then $\lg(P)$ can be expressed in the form

$$\lg(P) = x_0 c + \sum_{i=1}^{m} x_i p_i + \sum_{j=1}^{n} y_j q_j ,$$

where $x_i \geqq 0 , y_j \geqq 0 , 0 \leqq i \leqq m , 1 \leqq j \leqq n ,$ are integers, and if $x_0 > 0$ and $p_1 > 0$, then at least one x_i is positive for some $i > 0$. Now, there exist integers $k_i \geqq 0 , h_j \geqq 0 . 1 \leqq i \leqq m , 1 \leqq j \leqq n ,$ such that

$$\lg(P) = x_0 c + \sum_{i=1}^{m} [k_i(c+p_1) + x'_i]p_i + \sum_{j=1}^{n} [h_j(c+p_1) + y'_j]q_j ,$$

where $0 \leqq x'_i < c + p_1 , 0 \leqq y'_j < c + p_1 . 1 \leqq i \leqq m , 1 \leqq j \leqq$ n. Denote

$$r = \sum_{i=1}^{m} k_i p_i + \sum_{j=1}^{n} h_j q_j .$$

If $r = 0$, then we conclude that

$$P \in L^{x_1 + \ldots + x_m + y_1 + \ldots + y_n} \subseteq L^{(m+n)(c+p_1)} .$$

Let $r > 0$. Then

$$\lg(P) = (x_0 + r)c + rp_1 + \sum_{i=1}^{m} x'_i p_i + \sum_{j=1}^{n} y'_j q_j$$

and since there exist integers $k \geqq 0$ and $0 < r' \leqq c$ such that $rp_1 = (kc + r')p_1$, we obtain

$$\lg(P) = (x_0 + r + kp_1)c + r'p_1 + \sum_{i=1}^{m} x'_i p_i + \sum_{j=1}^{n} y'_j q_j .$$

Therefore,

$$P \in L^{x'_1 + \ldots + x'_m + y'_1 + \ldots + y'_n + r'} \subseteq L^{(m+n)(c+p_1)+c} .$$

which completes the proof.

Lemma 1 and Theorem 1 give necessary and sufficient conditions for a regular language L over $\{a\}$ to possess f.p.p.

There is an algorithm to convert a regular expression representing a language L over $\{a\}$ into the form (1). We can algorithmically also test whether two regular expressions represent the same language. Theorem 1 gives one number i such that $L^i = L^*$. Hence, there is an algorithm for finding the number $\min \{i | L^i = L^*\}$, since it suffices to test only a finite number of equations between regular expressions.

4. Some special cases

Let L be an infinite language over V and $\lambda \in L$. Obviously, $L^{i-1} \subseteq L^i , i = 1 , 2 , \ldots ,$ and if $P \in L^* . \lg(P) = k$. then $P \in L^k$.

Theorem 2. *If a language* L, $\lambda \in L$, *possesses f.p.p.* (*respectively does not possess f.p.p.*) *and a language* L_1 *satisfies the conditions* (i) $\lambda \in L_1$, (ii) $L_1^* = L^*$ *and* (iii) $L - L_1$ (*respectively* $L_1 - L$) *is finite, then* L_1 *possesses f.p.p.* (*respectively does not possess f.p.p.*).

Proof. Assume first that L possesses f.p.p. This implies the existence of an integer k such that $L^k = L^*$. Let

$$k_1 = \max \{\lg(P) | P \in L - L_1\} .$$

Since the case $L - L_1 = \emptyset$ is trivial, we may assume that $L - L_1 \neq \emptyset$. Hence, $k_1 > 0$. Since, by (ii), $L - L_1 \subseteq L_1^*$, we obtain $L - L_1 \subseteq L_1^{k_1}$ and, consequently, $L \subseteq L_1^{k_1}$. Therefore, $L_1^{kk_1} = L_1^*$ and L_1 possesses f.p.p. Assume now that L does not possess f.p.p. and denote

$$k_2 = \max \{\lg(P) | P \in L_1 - L\} .$$

Then, similarly as above, we can show that $L_1 \subseteq L^{k_2}$. Hence, L_1 does not possess f.p.p.

Next we give an example of languages possessing f.p.p.

Definition. An automaton $A = (V, S, F, s_0, f)$ is called a *permutation automaton* iff, for every $a \in V$ and $s, s' \in S$, $f(s, a) = f(s', a)$ implies that $s = s'$.

Theorem 3. *A language* L, *where* $\lambda \in L$, *accepted by a permutation automaton possesses f.p.p. More specifically, if* L *is accepted by* $A = (V, S, F, s_0, f)$, *where* $\# \bar{F} = k$, *then* $L^{k+1} = L^*$.

Proof. Assume the contrary: There is a word P such that $P \notin L^q$ but $P \in L^{q+1}$ for some $q > k$.

Let $G_A(L)$ be the state graph of A. Since $\lambda \in L$, we have $s_0 \in F$. Consider the infinite graph $G_\infty(L)$ corresponding to $G_A(L)$. Clearly, there exists an initial subword P_1 of P such that if $P_1' \neq P_1$ is an arbitrary initial subword of P_1, then $B(f_1(s_0^1, P_1')) \in \{s_0\} \cup \bar{F}$ and $B(f_1(s_0^1, P_1)) \in F - \{s_0\}$. Consequently, $B(f_\infty(s_0^1, P_1')) = B(f_1(s_0^1, P_1'))$ and $B(f_\infty(s_0^1, P_1)) = B(f_2(s_0^1, P_1)) = B(f_1(s_0^1, P_1)) \cup \{s_0\}$. Since $G_A(L)$ is the state graph of a permutation automaton, we have $\# (f_2(s_0^1, P')) \geqq 2$ for an arbitrary initial subword P' of P such that $\lg(P') \geqq \lg(P_1)$. Further, there exists an initial subword $P_2 = P_1 P_2'$ such that if P_2'' is an initial subword of P_2 and $\lg(P_1) \leqq \lg(P_2'') < \lg(P_2)$, then $s_0 \in B(f_2(s_0^1, P_2''))$ or $B(f_2(s_0^1, P_2'')) \cap (F - \{s_0\}) = \emptyset$ and $s_0 \notin B(f_2(s_0^1, P_2))$ and $B(f_2(s_0^1, P_2)) \cap (F - \{s_0\}) \neq \emptyset$. Consequently, $B(f_\infty(s_0^1, P_2'')) = B(f_2(s_0^1, P_2''))$ and $B(f_\infty(s_0^1, P_2)) = B(f_3(s_0^1, P_2)) = B(f_2(s_0^1, P_2)) \cup \{s_0\}$. Since $G_A(L)$ is the state graph of a permutation automaton, we have $\#(f_3(s_0^1, P_2'')) \geqq 3$ for an arbitrary initial subword P'' od P such that $\lg(P'') \geqq \lg(P_2)$.

By induction we obtain: If Q is an initial subword of P and $B(f_i(s_0^1, Q))$, $i \leqq q$, is properly included in $B(f_{i+1}(s_0^1, Q))$, then

$\#(f_i(s_0^1, Q)) \geqq i$. Since $P \notin L^q$ but $P \in L^{q+1}$, we conclude that $B(f_q(s_0^1, P))$ is properly included in $B(f_{q+1}(s_0^1, P))$. Hence, $\#(f_q(s_0^1, P)) \geqq q > k$. By the assumption $k = \#\bar{F}$, we obtain $B(f_q(s_0^1, P)) \cap F \neq \emptyset$. This implies that $P \in L^q$, which is a contradiction.

Next we consider the minimum root of a regular language. The following lemma is found in Brzozowski [1], p. 469.

Lemma 3. *If L is a star language there exists a unique root*

$$L_m = (L - \lambda) - (L - \lambda)^2 \tag{2}$$

of L contained in every other root of L. L_m is called the minimum root of L.

If L is regular, we obtain from (2) that L_m is regular, too.

Theorem 4. *If a regular language $L_m \neq \emptyset$ is a minimum root, then the language $L_{m'} = L_m \cup \lambda$ does not possess f.p.p.*

Proof. By (2), $L_m \neq \lambda$. In case $L_{m'}$ is finite the assertion follows by Lemma 1. Now let $L_{m'}$ be infinite. Assume the contrary: There is an integer $k \geqq 0$ such that $L_{m'}^k = L_{m'}^*$. Let $P \neq \lambda$ be a word belonging to $L_{m'}$. Consider words

$$P_2 P^i P_3 \in L_{m'}, \tag{3}$$

for which there exist words P_1, P_4 and integers $j_1 \geqq 0, j_2 \geqq 0$ such that $P^{j_1}P_1, P_4P^{j_2} \in L_{m'}^*$ and $P_1P_2 = P$ or $= \lambda$ and $P_3P_4 = P$ or $= \lambda$ and, furthermore, $\lg(P_2), \lg(P_3) < \lg(P)$. We claim that there is only a finite number of words of the form (3). Assume the contrary. Since the set $\{P' | \lg(P') < \lg(P)\}$ is finite, there exist words P_2 and P_3, which appear in infinitely many words of the form (3). Thus, there is an infinite number of words of the form $P^{j_1}P_1P_2P^iP_3P_4P^{j_2}$, where j_1 and j_2 are fixed and $P^{j_1}P_1, P_4P^{j_2} \in L_{m'}^*$ and $P_1P_2 = P$ or $= \lambda$ and $P_3P_4 = P$ or $= \lambda$ and, furthermore, $P_2P^iP_3 \in L_{m'}$ for infinitely many values of i. From these values of i we can choose i_1 and i_2 such that

$$\lg(P^{i_2 - i_1}) \geqq \lg(P^{i_1}P_3P_4P^{j_1+j_2}P_1P_2P^{i_1}).$$

This implies that

$$P_2P^{i_2}P_3 = P_2P^{i_1}P_3P_4P^{j_2}P^rP^{j_1}P_1P_2P^{i_1}P_3 \in L_{m'},$$

where $r \geqq 0$. Since $P_2P^{i_1}P_3, P_4P^{j_2}, P^r$ and $P^{j_1}P_1$ belong to $L_{m'}^*$ and L_m is a minimum root, we have a contradiction.

Now define $s = \max\{\lg(Q) | Q \text{ is of the form } (3)\}$. Then the word $P^{ks+1} \in L_{m'}^*$ but $P^{ks+1} \notin L_{m'}^k$. This is a contradiction and the proof is completed.

In the following, let $L^* = W(V)$. Then $a \in L$ for all $a \in V$. Thus, if $G_A(L)$ is the state graph of L, then $f(s_0, a) \in F$ for all $a \in V$ and for every word $P \in W(V)$ there is a path in $G_\infty(L)$ from s_0^1 to some final states of $G_\infty(L)$ labelled by P. Furthermore, $\lg(P) \leqq q$ implies that $P \in L^{q_1}$ for some $q_1 \leqq q$.

Theorem 5. *Let* $L^* = W(V)$ *and* $\lambda \in L$. *If in* $G_0(L)$, $\# \bar{F} = k$ *and there is no cycle in the subgraph consisting of the states of* $\bar{F}$ *in* $G_0(L)$, *then* $L^{k+1} = L^*$.

Proof. Consider a word $P \in W(V)$, $\lg(P) > k$. We can write $P = P_1P_2$, where $\lg(P_2) = k$. If $f(s_0, P_1) \in F$, then clearly $P = P_1P_2 \in L^{k+1}$. Now assume that $f(s_0, P_1) \notin F$. The length of the longest word leading from the state $f(s_0, P_1)$ to some state of $\bar{F}$ such that every intermediate state belongs to $\bar{F}$ is at most $k-1$. Hence, there exist words P_3 and P_4 such that $P_2 = P_3P_4$ and $P_1P_3 \in L$. Since $\lg(P_4) < k$, we have $P = P_1P_3P_4 \in L^{k+1}$.

Theorem 6. *Let* $L^* = W(V)$, $\lambda \in L$ *and, in* $G_0(L)$, $\bar{F} = \{s_n\}$. *If the number of all different non-empty subsets of* F *is* k, *then* L *possesses f.p.p. iff* $L^{2k+1} = L^*$.

Proof. If $L^{2k+1} = L^*$, then clearly L possesses f.p.p. Conversely, let L possess f.p.p. Assume the contrary: There is a word P such that $P \notin L^{q-1}$ but $P \in L^q$ for some $q > 2k+1$. Consider the infinite graph $G_\infty(L)$ corresponding to the graph $G_0(L)$. Obviously, there exist words P_1 and P_2 such that $P = P_1P_2$ and P_1 is the shortest word leading to the state s_n such that in P_2 there is no letter leading out from the state s_n. Let $f_2(s_0^1, P_1) \cap F^2 = S_1^2$. Obviously, $\# S_1^2 \geqq 1$ and hence $s_0^3 \in f_3(s_0^1, P_1)$. Now, there exists an initial subword P_2' of P_2 such that if $P_2'' \neq P_2'$ is an initial subword of P_2', then $f_2(S_1^2, P_2'') \cap F^2 \neq \emptyset$ and $f_2(S_1^2, P_2') = \{s_n\}$. Since $s_0^3 \in f_3(S_1^2, P_2'')$, we have $B(f_\infty(S_1^2, P_2'')) = B(f_2(S_1^2, P_2'') \cup f_3(S_1^2, P_2''))$, Furthermore, $B(f_\infty(S_1^2, P_2')) \cap F = B(f_3(S_1^2, P_2') \cup f_4(S_1^2, P_2')) \cap F$.

By induction we obtain: If P_3 is an arbitrary initial subword of P_2, then there exists an integer i such that

$$B(f_j(S_1^2, P_3)) = \{s_n\}, \ 2 \leqq j \leqq i-1, \tag{4}$$

$$B(f_\infty(S_1^2, P_3)) = B(f_i(S_1^2, P_3) \cup f_{i+1}(S_1^2, P_3)). \tag{5}$$

Since $P \notin L^{q-1}$ but $P \in L^q$, there exist words Q_i, Q_i', $i = 1, 2, \ldots, q-1$, such that $P = P_1Q_iQ_i'$ and $P_1Q_i \notin L^i$, $P_1Q_i \in L^{i+1}$ and $\lg(Q_i) < \lg(Q_{i+1})$. Denote $S_2 = S_1 \cup \{s_0\}$. Consider the sets $B(f_\infty(S_1^2, Q_i)) \cap F$, $i = 1, 2, \ldots, q-1$. Since $q-1 > 2k$, some set appears at least three times. Thus, by (4) and (5), there exist $S_3 \subseteq S$, where $s_0, s_n \in S_3$, and a subword Q of P_2 such that $B(f_\infty(s_n^1, Q)) = \{s_n\}$, $B(f_\infty(S_3^1, Q)) \subseteq S_3$ and $f(S_3, Q) = \{s_n\}$. Therefore, $Q^i \notin L^i$ but $Q^i \in L^*$ for $i = 1, 2, \ldots$, which implies that L does not possess f.p.p. This is a contradiction completing the proof.

5. The main result

Definition. Let S_1 and S_2 be subsets of S in $G_0(L)$. Then define

$$L^1_{S_1S_2} = \{P \in W(V) | f(s_1, P) = s_2, s_1 \in S_1, s_2 \in S_2\},$$

$$L^\infty_{S_1S_2} = \{P \in W(V) | B(f_\infty(S_1^1, P)) \subseteq S_2\}.$$

Lemma 4. *The language* $L^\infty_{S_1S_2}$ *is regular.*

Proof. It is a well-known fact that $L^1_{S_1S_2}$ is regular. Obviously,

$$L^\infty_{S_1S_2} = (L^1_{S_1S_2} \cup L^1_{S_1F}L^*L^1_{s_0S_2}) - (L^1_{S_1\bar{S}_2} \cup L^1_{S_1F}L^*L^1_{s_0\bar{S}_2}). \tag{6}$$

Hence, $L^\infty_{S_1S_2}$ is regular, too.

Theorem 7. *Let* L *be a regular language,* $\lambda \in L$, *and in* $G_0(L)$, $\# S = n + 1$. *There exists a word* $Q \in L^*$ *such that* $Q^i \notin L^i, i = 1, 2, \ldots,$ *iff there exist* $S_1 \subseteq S$, *where* $s_0 \in S_1$, *and* $S_2 \subseteq \bar{F}$ *such that*

$$L_1 = (L^\infty_{S_1S_1} \cap L^\infty_{S_2S_2} \cap L^*) - L^1_{S_1\bar{S}_2} \neq \emptyset. \tag{7}$$

Proof. Assume first that $L_1 \neq \emptyset$. Let $P \in L_1$. This implies that $P \notin L$ and hence $P \neq \lambda$. By (7), $f_1(s_0^1, P) \in S_2^1$ and $f_2(s_0^1, P) \subseteq S_1^2$. Similarly, $f_2(s_0^1, P^2) \subseteq S_2^2$ and $f_3(s_0^1, P^2) \subseteq S_1^3$. We can generally verify that for all $j \leqq i, f_j(s_0^1, P^i) \subseteq S_2^j$ and $f_{i+1}(s_0^1, P^i) \subseteq S_1^{i+1}$. Therefore, $P^i \notin L^i, i = 1, 2, \ldots$

Assume, conversely, that $P \in L^*$ but $P^i \notin L^i, i = 1, 2, \ldots$ Let

$$S' = \bigcup_{i=0}^{\infty} B(f_\infty(s_0^1, P^i))$$

and choose

$$S_2 = \{s \in S' | (\bigcup_{i=1}^{\infty} B(f_\infty(s^1, P^i))) \cap F = \emptyset\}.$$

We claim that $S_2 \neq \emptyset$. Consider, in $G_\infty(L)$, the states $f_1(s_0^1, P)$, $f_1(s_0^1, P^2), \ldots, f_1(s_0^1, P^{n+1})$. Since $\# S = n + 1$, there exist integers i_1 and i_2 such that $1 \leqq i_1 < i_2 \leqq n + 2$ and $f(s_0, P^{i_1}) = f(s_0, P^{i_2})$. The states $f(s_0, P^i), i_1 \leqq i \leqq i_2$, belong to the set S_2 for otherwise the condition $P^i \notin L^i, i = 1, 2, \ldots,$ does not hold. Thus $S_2 \neq \emptyset$.

Since the number of different subsets of the set S' is finite, there exist positive integers k_1 and k_2 such that $k_2 - k_1 \geqq n + 2$ and

$$B(f_\infty(s_0^1, P^{k_1})) = B(f_\infty(s_0^1, P^{k_2})).$$

Choose $S_1 = B(f_\infty(s_0^1, P^{k_1}))$ and $Q = P^{k_2 - k_1}$. Since $P^{k_1} \in L^*$, then also $s_0 \in S_1$.

From the considerations above it follows that

$$P^{k_2-k_1} \in L^{\infty}_{S_1S_1} \cap L^{\infty}_{S_2S_2} \cap L^* .$$

Assume now that $s \in S_1$. Consider the states $f(s, P), f(s, P^2), \ldots, f(s, P^{n+2}), \ldots, f(s, P^{k_2-k_1})$. Since $\# S = n + 1$, there exist integers i_1 and i_2 such that $1 \leqq i_1 < i_2 \leqq n + 2$ and $f(s, P^{i_1}) = f(s, P^{i_2})$. The states $f(s, P^i)$, $i_1 \leqq i \leqq k_2 - k_1$, belong to the set S_2 for otherwise the condition $P^i \notin L^i$, $i = 1, 2, \ldots,$ does not hold. Thus $P^{k_2-k_1} \notin L^1_{S_1\bar{S}_2}$, which implies that $P^{k_2-k_1} \in L_1$. This completes the proof.

It is a well-known fact that there is an algorithm for constructing a regular expression representing the language $L^1_{S_1S_2}$. Hence, by (6), we can algorithmically construct a regular expression representing the language $L^{\infty}_{S_1S_2}$ and test whether in (7) $L_1 \neq \emptyset$. If the answer to the following problem is yes, then Theorem 7 solves the f.p.p.-problem.

Problem. Let L, where $\lambda \in L$, be a regular language not possessing f.p.p. Does there always exist a word $P \in L^*$ such that $P^i \notin L^i$ for all $i = 1, 2, \ldots$?

For instance, in cases like Theorems 4 and 6 the answer is yes.

University of Turku
Turku, Finland

References

[1] BRZOZOWSKI, J. A.: Roots of star events, J. Assoc. Comput. Mach. **14**, 1967, 466—477.

[2] SALOMAA, A.: Theory of Automata, Pergamon Press, 1969.

Printed September 1972