

A POLYNOMIAL TIME ALGORITHM FOR LEFT [RIGHT] LOCAL TESTABILITY

A.N. Trahtman

Bar-Ilan University, Dep. of Math. and CS, 52900, Ramat Gan, Israel
email:trakht@macs.biu.ac.il

Abstract. A right [left] locally testable language S is a language with the property that for some nonnegative integer k two words u and v in alphabet S are equal in the semigroup if (1) the prefix and suffix of the words of length $k - 1$ coincide, (2) the set of segments of length k of the words as well as 3) the order of the first appearance of these segments in prefixes [suffixes] coincide.

We present necessary and sufficient condition for graph [semigroup] to be transition graph [semigroup] of the deterministic finite automaton that accepts right [left] locally testable language and necessary and sufficient condition for transition graph of the deterministic finite automaton with locally idempotent semigroup. We introduced polynomial time algorithms for the right [left] local testability problem for transition semigroup and transition graph of the deterministic finite automaton based on these conditions. Polynomial time algorithm verifies transition graph of automaton with locally idempotent transition semigroup.

Key words: *language, locally testable, deterministic finite automaton, algorithm, semigroup, graph*

AMS subject classification 20M07, 68Q25, 68Q45, 68Q68

1 Introduction

The concept of local testability was first introduced by McNaughton and Papert [12] and by Brzozowski and Simon [5]. This concept is connected with languages, finite automata and semigroups and has a wide spectrum of generalizations.

The necessary and sufficient condition for local testability were investigated for both transition graph and transition semigroups of the automaton [5], [10], [13], [16]. The polynomial time algorithms solve the problem of local testability for transition graph [10] and for transition semigroups of the automaton [13]. They are polynomial in terms of the size of the semigroup or in the sum of nodes and edges.

Right [left] local testability was introduced and studied by König [9] and by Garcia and Ruiz [7]. These papers use different definitions of the conception and we follow [7] here

Theorem 11 [7] *A finite semigroup S is right [left] locally testable iff it is locally idempotent and locally satisfies the identity $xyx = xy$ [$xyx = yx$].*

For conception of local idempotency see, for instance, [6]. The varieties of semigroups defined by considered identities are located not far from atoms in the structure of idempotent varieties [4].

We present in this work necessary and sufficient condition for right [left] local testability for transition graph of the DFA and for the local idempotency of the transition semigroup on the corresponding transition graph. We improve necessary and sufficient condition for right [left] local testability from [7] for transition semigroup. On the base of these results, we introduced a polynomial time algorithm for the right [left] local testability problem for transition semigroup and transition graph of the deterministic finite automaton and for checking the transition graph of the automaton with locally idempotent semigroup.

These algorithms are implemented in the package TESTAS. The package checks also whether or not a language given by its minimal automaton or by syntactic semigroup of the automaton is locally testable, threshold locally testable, strictly locally testable, or piecewise testable [2], [15].

2 Notation and definitions

Let Σ be an alphabet and let Σ^+ denote the free semigroup on Σ . If $w \in \Sigma^+$, let $|w|$ denote the length of w . Let k be a positive integer. Let $i_k(w)$ [$t_k(w)$] denote the prefix [suffix] of w of length k or w if $|w| < k$. Let $F_k(w)$ denote the set of segments of w of length k . A language L [a semigroup S] is called *right [left] k -testable* if there is an alphabet Σ [and a surjective morphism $\phi : \Sigma^+ \rightarrow S$] such that for all $u, v \in \Sigma^+$, if $i_{k-1}(u) = i_{k-1}(v)$, $t_{k-1}(u) = t_{k-1}(v)$, $F_k(u) = F_k(v)$ and the order of appearance of these segments in prefixes [suffixes] in the word coincide, then either both u and v are in L or neither is in L [$u\phi = v\phi$].

An automaton is *right [left] k -testable* if the automaton accepts a right [left] k -testable language.

A language L [a semigroup S , an automaton \mathbf{A}] is *right [left] locally testable* if it is right [left] k -testable for some k .

$|S|$ is the number of elements of the set S .

A semigroup S is called *semigroup of left [right] zeroes* if S satisfies the identity $xy = x$ [$xy = y$].

A semigroup S has a property ρ *locally* if for any idempotent $e \in S$ the subsemigroup eSe has the property ρ .

So a semigroup S is called *locally idempotent* if eSe is an idempotent subsemigroup for any idempotent $e \in S$.

A maximal strongly connected component of the graph will be denoted for brevity as *SCC*, a finite deterministic automaton will be denoted as *DFA*. A node from an *SCC* will be called for brevity as an *SCC – node*. *SCC*-node can be defined as a node that has a right unit in transition semigroup of the automaton.

$|Γ|$ denotes the number of nodes of the graph $Γ$.

$Γ^i$ denotes the direct product of i copies of the graph $Γ$. The edge $(\mathbf{p}_1, \dots, \mathbf{p}_n) \rightarrow (\mathbf{q}_1, \dots, \mathbf{q}_n)$ in $Γ^i$ is labelled by σ iff for each i the edge $\mathbf{p}_i \rightarrow \mathbf{q}_i$ in $Γ$ is labelled by σ .

The graph with only trivial SCC (loops) will be called *acyclic*.

If an edge $\mathbf{p} \rightarrow \mathbf{q}$ is labelled by σ then let us denote the node \mathbf{q} as $\mathbf{p}\sigma$.

We shall write $\mathbf{p} \succeq \mathbf{q}$ if the node \mathbf{q} is reachable from the node \mathbf{p} or $\mathbf{p} = \mathbf{q}$ ($\mathbf{p} \succ \mathbf{q}$ for distinct \mathbf{p}, \mathbf{q}).

In the case $\mathbf{p} \succeq \mathbf{q}$ and $\mathbf{q} \succeq \mathbf{p}$ we write $\mathbf{p} \sim \mathbf{q}$ (that is \mathbf{p} and \mathbf{q} belong to one SCC or $\mathbf{p} = \mathbf{q}$).

3 Transition graph of deterministic finite automaton

3.1 Graph of DFA with locally idempotent transition semigroup

Lemma 31 *Let S be the transition semigroup of a deterministic finite automaton and let $Γ$ be its transition graph. Let us suppose that for three distinct nodes $\mathbf{p}, \mathbf{q}, \mathbf{r}$ from $Γ$ the node $(\mathbf{p}, \mathbf{q}, \mathbf{r})$ in $Γ^3$ is SCC-node, and $(\mathbf{p}, \mathbf{q}) \succ (\mathbf{q}, \mathbf{r})$ in $Γ^2$.*

Then S is not locally idempotent.

Proof. Let us suppose that for the nodes $\mathbf{p}, \mathbf{q}, \mathbf{r}$ from $Γ$ the conditions of lemma hold. Therefore the nodes $\mathbf{p}, \mathbf{q}, \mathbf{r}$ have a right unit $e = e^2$, whence $\mathbf{p}e = \mathbf{p}$, $\mathbf{q}e = \mathbf{q}$, $\mathbf{r}e = \mathbf{r}$. In view $(\mathbf{p}, \mathbf{q}) \succ (\mathbf{q}, \mathbf{r})$, there exists an element $s \in S$ such that $\mathbf{p}s = \mathbf{q}$ and $\mathbf{q}s = \mathbf{r}$. Therefore $\mathbf{p}ese = \mathbf{q}$ and $\mathbf{q}ese = \mathbf{r}$, whence $\mathbf{p}(ese)^2 = \mathbf{r} \neq \mathbf{q} = \mathbf{p}ese$. So $\mathbf{p}(ese)^2 \neq \mathbf{p}ese$ and $(ese)^2 \neq ese$. Semigroup eSe is not an idempotent semigroup and therefore S is not locally idempotent.

Lemma 32 *Let S be the locally idempotent transition semigroup of a deterministic finite automaton and let $Γ$ be its transition graph.*

For any SCC-node $(\mathbf{p}, \mathbf{q}) \in Γ^2$ and $s \in S$ from $\mathbf{p}s \succeq \mathbf{q}$ follows $\mathbf{q}s \succeq \mathbf{q}$.

Proof. Let us consider SCC-node (\mathbf{p}, \mathbf{q}) from $Γ^2$ such that $\mathbf{p}s \succeq \mathbf{q}$. The node (\mathbf{p}, \mathbf{q}) has a right unit $e = e^2$, so $\mathbf{p}e = \mathbf{p}$, $\mathbf{q}e = \mathbf{q}$. For some $b \in S$ we have $\mathbf{p}sb = \mathbf{q}$. We can assume $s = es$, $b = be$. $esbe = (esbe)^2$ in locally idempotent semigroup S . Therefore $\mathbf{q} = \mathbf{p}esbe = \mathbf{p}(esbe)^2 = \mathbf{q}esbe = \mathbf{q}sbe$. Thus we have $\mathbf{q}s \succeq \mathbf{q}$.

Lemma implies

Corollary 33 *Let S be the locally idempotent transition semigroup of a deterministic finite automaton and let $Γ$ be its transition graph.*

Let us suppose that in $Γ^2$ we have $(\mathbf{p}, \mathbf{q}) \succ (\mathbf{q}, \mathbf{r})$ and the node (\mathbf{p}, \mathbf{q}) is an SCC-node. Then $\mathbf{r} \sim \mathbf{q}$.

Lemma 34 *Let S be transition semigroup of a deterministic finite automaton and suppose that in $Γ^2$ we have $(\mathbf{p}, \mathbf{q}) \succ (\mathbf{q}, \mathbf{p})$ for two distinct nodes \mathbf{p}, \mathbf{q} .*

Then S is not locally idempotent.

Proof. We have $\mathbf{ps} = \mathbf{q}$ and $\mathbf{qs} = \mathbf{p}$ for some $s \in S$. So $\mathbf{ps}^2 = \mathbf{p} \neq \mathbf{ps} = \mathbf{q}$ and $\mathbf{p} = \mathbf{ps}^{2n} \neq \mathbf{ps}^{2n-1} = \mathbf{q}$. Therefore $s^{2n} \neq s^{2n-1}$ for any integer n because of $\mathbf{p} \neq \mathbf{q}$. Finite semigroup S contains therefore non-trivial subgroup, whence S is not locally idempotent.

Let us formulate the necessary and sufficient conditions for graph to be transition graph of DFA with locally idempotent transition semigroup.

Theorem 35 *Transition semigroup S of a deterministic finite automaton is locally idempotent iff*

1. $(\mathbf{p}, \mathbf{q}) \not\sim (\mathbf{q}, \mathbf{p})$ in Γ^2 for any two distinct nodes \mathbf{p}, \mathbf{q} ,
2. for any SCC -node $(\mathbf{p}, \mathbf{q}) \in \Gamma^2$ and $s \in S$ from $\mathbf{ps} \succeq \mathbf{q}$ follows $\mathbf{qs} \succeq \mathbf{p}$ and
3. for any SCC -node $(\mathbf{p}, \mathbf{q}, \mathbf{r})$ of Γ^3 with distinct components holds $(\mathbf{p}, \mathbf{q}) \not\sim (\mathbf{q}, \mathbf{r})$ in Γ^2 .

Proof. If S is locally idempotent then the condition 1 follows from lemma 34, condition 2 follows from lemma 32, condition 3 follows from lemma 31.

Suppose now that S is not locally idempotent. Then for some node \mathbf{p} from Γ , idempotent e and element s from S we have $\mathbf{p}(ese)^2 \neq \mathbf{p}ese$. Hence $\mathbf{pe} \neq \mathbf{p}ese$ and at least one of two nodes $\mathbf{p}(ese)^2, \mathbf{p}ese$ exists. If exists the node $\mathbf{p}(ese)^2$ then the node $\mathbf{p}ese$ exists too. So $\mathbf{p}ese$ exists anyway. Therefore \mathbf{pe} exists too and from $(\mathbf{pe}, \mathbf{p}ese)ese = (\mathbf{p}ese, \mathbf{p}(ese)^2)$ in view of condition 2 follows $\mathbf{p}(ese)^2 \succ \mathbf{p}ese$, whence the node $\mathbf{p}(ese)^2$ exists.

The node $(\mathbf{pe}, \mathbf{p}ese, \mathbf{p}(ese)^2)$ is an SCC -node of Γ^3 because all components of the node have common right unit e . Let us notice that $\mathbf{p}(ese)^2 \neq \mathbf{p}ese$ and $\mathbf{pe} \neq \mathbf{p}ese$. We have $(\mathbf{pe}, \mathbf{p}ese) \succ (\mathbf{p}ese, \mathbf{p}(ese)^2)$. In the case $\mathbf{pe} = \mathbf{p}(ese)^2$ we have contradiction with condition 1, in opposite case we have contradiction with condition 3.

3.2 Right local testability

Theorem 36 *Let S be transition semigroup of deterministic finite automaton with state transition graph Γ . Then S is right locally testable iff*

1. for any SCC -node (\mathbf{p}, \mathbf{q}) from Γ^2 such that $\mathbf{p} \sim \mathbf{q}$ holds $\mathbf{p} = \mathbf{q}$.
2. for any SCC -node $(\mathbf{p}, \mathbf{q}) \in \Gamma^2$ and $s \in S$ from $\mathbf{ps} \succeq \mathbf{q}$ follows $\mathbf{qs} \succeq \mathbf{p}$.

Proof. Suppose semigroup S is right locally testable.

Condition 1. Let (\mathbf{p}, \mathbf{q}) be an SCC -node with distinct components. Then for some idempotent $e \in S$ holds $(\mathbf{p}, \mathbf{q})e = (\mathbf{p}, \mathbf{q})$. If $\mathbf{p} \sim \mathbf{q}$ then for some $a, b \in S$ holds $\mathbf{qa} = \mathbf{p}$ and $\mathbf{pb} = \mathbf{q}$, whence $\mathbf{qea} = \mathbf{p}$ and $\mathbf{pbe} = \mathbf{q}$. So $\mathbf{qaebe} = \mathbf{q}$ and $\mathbf{pebe} = \mathbf{p}$. Semigroup S is right locally testable and therefore the subsemigroup eSe satisfies identity $xyx = xy$ [7]. Consequently, $\mathbf{q} = \mathbf{qaebe} = \mathbf{qaebeae} = \mathbf{pebe} = \mathbf{p}$.

Condition 2 follows from lemma 32 because right locally testable semigroup S is locally idempotent.

Suppose now that both conditions of the theorem are valid. Let us begin from the local idempotency of S .

If the identity $x^2 = x$ is not valid in eSe for some idempotent e then for some node $\mathbf{v} \in \Gamma$ and some element $a \in S$ we have $\mathbf{veae} \neq \mathbf{veaeae}$. At least one of two considered nodes exists. In view of $\mathbf{ve} \succeq \mathbf{veae} \succeq \mathbf{veaeae}$ the nodes \mathbf{veae} , \mathbf{ve} exist. Let us denote $\mathbf{p} = \mathbf{ve}$, $\mathbf{q} = \mathbf{veae}$. Therefore (\mathbf{p}, \mathbf{q}) is an *SCC*-node. Notice that $\mathbf{peae} \succeq \mathbf{q}$. Hence, by condition 2, $\mathbf{qae} \succeq \mathbf{q}$. Now, by condition 1, in view of $\mathbf{q} \succeq \mathbf{qae}$, we have $\mathbf{qae} = \mathbf{q}$. So $\mathbf{veae} = \mathbf{veaeae}$ in spite of our assumption.

Thus the transition semigroup S is locally idempotent.

If the identity $xyx = xy$ [7] is not valid in eSe then for some node $\mathbf{v} \in \Gamma$, some idempotent e and elements $a, b \in S$ holds $\mathbf{vaebe} \neq \mathbf{vaebeae}$. So the node \mathbf{vaebe} exists. Let us denote $\mathbf{p} = \mathbf{vaebe}$. S is locally idempotent and therefore $\mathbf{p} = \mathbf{vaebeaebe}$. Consequently, the node $\mathbf{q} = \mathbf{vaebeae}$ exists too. We have $\mathbf{p} \neq \mathbf{q}$. The node $(\mathbf{vaebe}, \mathbf{vaebeae}) = (\mathbf{p}, \mathbf{q})$ is an *SCC*-node from Γ^2 . It is clear that $\mathbf{p} = \mathbf{vaebe} \succeq \mathbf{vaebeae} = \mathbf{q}$. Then $\mathbf{q} = \mathbf{vaebeae} \succeq \mathbf{vaebeaebe} = \mathbf{vaebe} = \mathbf{p}$. So $\mathbf{p} \sim \mathbf{q}$ and $\mathbf{p} \neq \mathbf{q}$ in spite of the condition 1.

3.3 Left local testability

Lemma 37 *Let reduced DFA \mathbf{A} with state transition graph Γ and transition semigroup S be left locally testable. Suppose that for *SCC*-node (\mathbf{p}, \mathbf{q}) of Γ^2 holds $\mathbf{p} \succeq \mathbf{q}$.*

Then for any $s \in S$ holds $\mathbf{ps} \succeq \mathbf{q}$ iff $\mathbf{qs} \succeq \mathbf{q}$.

Proof. Suppose \mathbf{A} is left locally testable. Then the transition semigroup S of the automaton is finite, aperiodic and for any idempotent $e \in S$ the subsemigroup eSe is idempotent [7].

For some $a, e = e^2 \in S$ holds $\mathbf{pa} = \mathbf{q}$, $(\mathbf{p}, \mathbf{q})e = (\mathbf{p}, \mathbf{q})$. So we have $\mathbf{pes} = \mathbf{ps}$ and $\mathbf{qes} = \mathbf{qs}$.

If we assume that $\mathbf{ps} \succeq \mathbf{q}$, then for some b from S holds $\mathbf{psb} = \mathbf{q}$, whence $\mathbf{pesbe} = \mathbf{q}$. In idempotent subsemigroup eSe we have $esbe = (esbe)^2$. Therefore $\mathbf{qesbe} = \mathbf{p}(esbe)^2 = \mathbf{pesbe} = \mathbf{q}$ and $\mathbf{qes} = \mathbf{qs} \succeq \mathbf{q}$.

If we assume now that $\mathbf{qs} \succeq \mathbf{q}$, then for some $d \in S$ holds $\mathbf{qsde} = \mathbf{q}$. For some $a \in S$ holds $\mathbf{pa} = \mathbf{q}$ because of $\mathbf{p} \succeq \mathbf{q}$. So $\mathbf{qsde} = \mathbf{qesde} = \mathbf{q}$ and $\mathbf{peaesde} = \mathbf{q}$. The subsemigroup eSe satisfies identity $xyx = yx$, therefore $\mathbf{eaesde} = \mathbf{esdeaesde}$. So $\mathbf{q} = \mathbf{peaesde} = \mathbf{pesdeaesde}$. Hence, $\mathbf{pes} = \mathbf{ps} \succeq \mathbf{q}$.

Lemma 38 *Let reduced DFA \mathbf{A} with state transition graph Γ be left locally testable.*

*If the node $(\mathbf{p}, \mathbf{q}, \mathbf{r})$ is an *SCC*-node of Γ^3 , $(\mathbf{p}, \mathbf{r}) \succeq (\mathbf{q}, \mathbf{r})$ and $(\mathbf{p}, \mathbf{q}) \succeq (\mathbf{r}, \mathbf{q})$ in Γ^2 , then $\mathbf{r} = \mathbf{q}$.*

$$\begin{array}{c} \mathbf{p} \\ \circ \\ \mathbf{q} \\ \circ \\ \mathbf{r} \\ \circ \\ e \end{array} \quad \begin{array}{c} \mathbf{p} \\ \circ \\ \mathbf{r} \\ \circ \end{array} \succeq \begin{array}{c} \mathbf{q} \\ \circ \\ \mathbf{r} \\ \circ \end{array} \quad \text{and} \quad \begin{array}{c} \mathbf{p} \\ \circ \\ \mathbf{q} \\ \circ \end{array} \succeq \begin{array}{c} \mathbf{r} \\ \circ \\ \mathbf{q} \\ \circ \end{array} \quad \longrightarrow \quad \mathbf{q} = \mathbf{r}$$

Proof. Suppose \mathbf{A} is left locally testable. Then the transition semigroup S of the automaton is finite, aperiodic and for any idempotent $e \in S$ the subsemigroup eSe is idempotent [7].

Let us consider the nodes $\mathbf{p}, \mathbf{q}, \mathbf{r}$ from Γ such that the conditions of lemma are valid for them. From $(\mathbf{p}, \mathbf{r}) \succeq (\mathbf{q}, \mathbf{r})$ and $(\mathbf{p}, \mathbf{q}) \succeq (\mathbf{r}, \mathbf{q})$ follows $(\mathbf{p}, \mathbf{r})s = (\mathbf{q}, \mathbf{r})$ and $(\mathbf{p}, \mathbf{q})t = (\mathbf{r}, \mathbf{q})$ for some $s, t \in S$ and $(\mathbf{p}, \mathbf{q}, \mathbf{r})e = (\mathbf{p}, \mathbf{q}, \mathbf{r})$, for some idempotents $e \in S$. We can take s, t from eSe . Therefore

$$ese = s, ete = t, s^2 = s, t^2 = t$$

So $\mathbf{p}s = \mathbf{q}$, $\mathbf{r}s = \mathbf{r}$, $\mathbf{p}t = \mathbf{r}$, $\mathbf{q}t = \mathbf{q}$. Let us notice that $\mathbf{q}s = \mathbf{p}s^2 = \mathbf{p}s = \mathbf{q}$. Analogously, $\mathbf{r}t = \mathbf{r}$.

We have $\mathbf{p}sts = \mathbf{q}ts = \mathbf{q}s = \mathbf{q}$. Then $\mathbf{p}ts = \mathbf{r}s = \mathbf{r}$. The identity $xyx = yx$ is valid in subsemigroup eSe , whence $\mathbf{q} = \mathbf{p}sts = \mathbf{p}ts = \mathbf{r}$.

Let us formulate the necessary and sufficient conditions for graph to be transition graph of DFA with left locally testable transition semigroup.

Theorem 39 *Let S be transition semigroup of a deterministic finite automaton with state transition graph Γ .*

Then S is left locally testable iff

1. *S is locally idempotent,*
2. *for any SCC-node (\mathbf{p}, \mathbf{q}) of Γ^2 such that $\mathbf{p} \succeq \mathbf{q}$ and for any $s \in S$ we have $\mathbf{p}s \succeq \mathbf{q}$ iff $\mathbf{q}s \succeq \mathbf{q}$ and*
3. *If for arbitrary nodes $\mathbf{p}, \mathbf{q}, \mathbf{r} \in \Gamma$ the node $(\mathbf{p}, \mathbf{q}, \mathbf{r})$ is SCC-node of Γ^3 , $(\mathbf{p}, \mathbf{r}) \succeq (\mathbf{q}, \mathbf{r})$ and $(\mathbf{p}, \mathbf{q}) \succeq (\mathbf{r}, \mathbf{q})$ in Γ^2 , then $\mathbf{r} = \mathbf{q}$.*

Proof. Suppose semigroup S is left locally testable. Then S is locally idempotent [7]. Second and third conditions of our theorem follow from lemmas 37 and 38, correspondingly.

Suppose now that the conditions of the theorem are valid but for an arbitrary node \mathbf{p} , an arbitrary idempotent $e \in S$ and two elements $s, t \in eSe$ holds $\mathbf{p}sts \neq \mathbf{p}ts$. By condition 1,

$$s^2 = s, t^2 = t, tsts = ts, stst = st, tssts = ts$$

At least one of two nodes $\mathbf{p}sts = \mathbf{q}$ and $\mathbf{p}ts = \mathbf{r}$ exists. Therefore $\mathbf{p}e$ exists too. We have $(\mathbf{p}e, \mathbf{p}ts)sts = (\mathbf{p}sts, \mathbf{p}ts)$. Therefore the existence of the node $\mathbf{p}ts = \mathbf{r}$ implies by condition 2 the existence of the node $\mathbf{p}sts = \mathbf{q}$. Analogously, from $(\mathbf{p}e, \mathbf{p}sts)ts = (\mathbf{p}ts, \mathbf{p}sts)$ and existence of the node $\mathbf{p}sts = \mathbf{q}$ follows by condition 2 the existence of the node $\mathbf{p}ts = \mathbf{r}$.

The node $(\mathbf{p}e, \mathbf{q}, \mathbf{r})$ is an SCC-node because all his components have common right unit e . We have $(\mathbf{p}, \mathbf{r})sts = (\mathbf{p}sts, \mathbf{p}sts) = (\mathbf{q}, \mathbf{p}ts) = (\mathbf{q}, \mathbf{r})$. Analogously, $(\mathbf{p}, \mathbf{q})ts = (\mathbf{p}ts, \mathbf{p}sts) = (\mathbf{r}, \mathbf{p}sts) = (\mathbf{r}, \mathbf{q})$. Thus,

$$(\mathbf{p}e, \mathbf{r}) \succ (\mathbf{q}, \mathbf{r}), (\mathbf{p}e, \mathbf{q}) \succ (\mathbf{r}, \mathbf{q})$$

Now by the third condition of the theorem, $\mathbf{r} = \mathbf{q}$. Therefore $\mathbf{p}sts = \mathbf{p}ts$. The node \mathbf{p} is an arbitrary node, whence $sts = ts$ for every two elements $s, t \in eSe$. Consequently, the subsemigroup eSe satisfies identity $xyx = yx$. Thus the semigroup S is left locally testable.

4 Semigroups

Lemma 41 *Let S be a finite locally idempotent semigroup. The following two conditions are equivalent in S :*

- a) *S satisfies locally the identity $xyx = xy$ (S is right locally testable).*
- b) *No two distinct idempotents e, i from S such that $ie = e, ei = i$ have a common right unit in S . That is, there is no idempotent $f \in S$ such that $e = ef$ and $i = if$.*

Proof. Suppose the identity $xy = xyx$ is valid in subsemigroup uSu for any idempotent u and for some idempotents e, i in S we have $ie = e, ei = i$. Suppose f is a common right unit of e, i . The identity $xyx = xy$ in fSf and equality $ei = i$ imply $i = ei = efefif = efefife = eie = e$. Thus the idempotents e, i are not distinct.

Suppose now that uSu does not satisfy the identity $xyx = xy$ for some idempotent u . Notice that uSu is an idempotent semigroup. So for some a, b of S , $uaubua \neq uaubu$. For two distinct idempotents $i = uaubua$ and $e = uaubu$ with common right unit u we have $ie = uaubuauba = uaubua = uaubu = e$ and $ei = uaubuauba = uaubua = i$.

So two distinct idempotents e, i from S such that $ie = e, ei = i$ have a common right unit u in S .

The following lemma is proved analogously:

Lemma 42 *Let S be a finite locally idempotent semigroup. The following two conditions are equivalent in S :*

- a) *S satisfies locally the identity $xyx = yx$ (S is left locally testable).*
- b) *No two distinct idempotents e, i from S such that $ie = i, ei = e$ have a common left unit in S . That is, there is no idempotent $f \in S$ such that $e = fe$ and $i = fi$.*

Recall that a semigroup A is a right [left] zero semigroup if A satisfies the identity $xy = y[xy = x]$. A right [left] locally testable semigroup is locally idempotent [7]. Then from the last two lemmas follows

Theorem 43 *A finite semigroup S is right [left] locally testable iff S is locally idempotent and no two distinct idempotents e, i from right [left] zero subsemigroup have a common right [left] unit in S .*

5 An algorithm for semigroup

The following proposition is useful for the algorithm.

Lemma 51 [13] *Let E be the set of idempotents of a semigroup S of size n represented as an ordered list. Then there exists an algorithm of order n^2 that reorders the list so that the maximal left [right] zero subsemigroups of S appear consecutively in the list.*

1. *Testing whether a finite semigroup S is right [left] locally testable.*

Suppose $|S| = k$. We begin by finding the set of idempotents E . This is a linear time algorithm. Then let us verify local idempotency. For every $e \in E$ and every $s \in S$ let us check condition $ese = (ese)^2$. If the condition does not hold for some pair, the semigroup is not locally idempotent and therefore not right locally testable (theorem 43). This takes $O(k^2)$ steps.

Now we reorder E according to lemma 51 in a chain such that the subsemigroups of right [left] zeroes form intervals in this chain. We note the bounds of these intervals. We find for each element e of E the first element i in the chain such that e is a right [left] unit for i . Then we find in the chain the next element j with the same unit e . If i and j belong to the same subsemigroup of right [left] zeroes we conclude that S is not right [left] testable (Lemma 41) and stop the process. If they are in different right [left] zero semigroups, we replace i by j and continue the process of finding a new j . This takes $O(k^2)$ steps.

Finding the maximal subsemigroup of right [left] zeroes containing a given idempotent needs k steps. So for to reorder E we need at most k^2 steps. The time and the space complexity of the algorithm is $O(k^2)$.

6 Graph algorithms

Let n be the sum of the nodes and edges of Γ . The first-depth search ([1], [10] or [15]) will be used for SCC search, for reachability table for triples and for checking condition 2 of theorems 35 and 36.

Table of reachability for triples

Suppose SCC of Γ , Γ^3 and the table of reachability are known. For every SCC -node \mathbf{q} of the graph Γ let us form by help of the first-depth search on Γ^2 the following relation L [I] on Γ : $\mathbf{p}L\mathbf{r}$ if $(\mathbf{p}, \mathbf{q}) \succeq (\mathbf{r}, \mathbf{q})$ $[\mathbf{p}I\mathbf{r}$ if $(\mathbf{p}, \mathbf{q}) \succeq (\mathbf{q}, \mathbf{r})]$. For every node (\mathbf{p}, \mathbf{q}) we form set of nodes \mathbf{r} such that $\mathbf{p}L\mathbf{r}$ $[\mathbf{p}I\mathbf{r}]$. We use an auxiliary array for this aim: for every node (\mathbf{p}, \mathbf{q}) and for every node \mathbf{s} , we form set of pointers to nearest successors (\mathbf{t}, \mathbf{s}) $[(\mathbf{s}, \mathbf{t})]$ of (\mathbf{p}, \mathbf{q}) .

If $(\mathbf{p}, \mathbf{q}, \mathbf{r})$ is an SCC -node with distinct components and $\mathbf{p}L\mathbf{r}$ $[\mathbf{p}I\mathbf{r}]$ then we add the triple $(\mathbf{p}, \mathbf{q}, \mathbf{r})$ to the set $Left$ $[LocId]$. ($O(n^3)$ time and space complexity).

6.1 Graph of automaton with locally idempotent transition semigroup

The algorithm is based on the theorem 35. Let us recognize the reachability on the graph Γ and form the table of reachability for all pairs of Γ . The time required for this step is $O(|\Gamma|^2)$.

We find graph Γ^2 and all SCC of the graph ($O(n^2)$ time complexity). If the nodes (\mathbf{p}, \mathbf{q}) and (\mathbf{q}, \mathbf{p}) belong to common SCC then the transition semigroup is not locally idempotent (condition 1).

For check the condition 2 of the theorem let us add to the graph Γ^2 new node $(\mathbf{0}, \mathbf{0})$ with edges from this node to every SCC -node (\mathbf{p}, \mathbf{q}) from Γ^2 such that $\mathbf{p} \succeq \mathbf{q}$. Let us consider first-depth search from the node $(\mathbf{0}, \mathbf{0})$ (the unique starting point of any path).

Let us fix the node \mathbf{q} after going through the edge $(\mathbf{0}, \mathbf{0}) \rightarrow (\mathbf{p}, \mathbf{q})$. We do not visit edges $(\mathbf{r}, \mathbf{s}) \rightarrow (\mathbf{r}, \mathbf{s})\sigma$ such that $\mathbf{r}\sigma \not\succeq \mathbf{s}$. In the case that for the node (\mathbf{r}, \mathbf{s}) from two conditions $\mathbf{r}\sigma \succeq \mathbf{q}$ and $\mathbf{s}\sigma \succeq \mathbf{q}$ only the first is valid the condition 2 does not hold, the transition semigroup is not locally idempotent and the algorithm stops.

Let us find graph Γ^3 , all SCC of the graph Γ^3 and mark all SCC -nodes with three distinct components such that the first component is ancestor of two others. ($O(n^3)$ time complexity).

Let us go to the condition 3 of the theorem 35. We form a table of triples *LocId* (see algorithm for table of reachability above). If some SCC -node $(\mathbf{p}, \mathbf{q}, \mathbf{r})$ from Γ^3 with distinct components belongs to *LocId* then the condition 3 does not hold and the semigroup is not locally idempotent.

The whole time and space complexity of the algorithm is $O(n^3)$.

6.2 Right local testability of DFA

The algorithm is based on the theorem 36. Let us form a table of reachability of the graph Γ , find all SCC of Γ , Γ^2 and all SCC -nodes of Γ^2 . ($O(n^2)$ time complexity).

Let us verify the condition 1 of the theorem. For every SCC -node (\mathbf{p}, \mathbf{q}) ($\mathbf{p} \neq \mathbf{q}$) from Γ^2 let us check the condition $\mathbf{p} \sim \mathbf{q}$. If the condition holds the automaton is not right locally testable. ($O(n^2)$ time complexity).

For check the condition 2 of the theorem let us add to the graph Γ^2 new node $(\mathbf{0}, \mathbf{0})$ with edges from this node to every SCC -node (\mathbf{p}, \mathbf{q}) from Γ^2 such that $\mathbf{p} \succeq \mathbf{q}$. Let us consider first-depth search from the node $(\mathbf{0}, \mathbf{0})$ (the unique begin of any path).

Let us fix the node \mathbf{q} after going through the edge $(\mathbf{0}, \mathbf{0}) \rightarrow (\mathbf{p}, \mathbf{q})$. We do not visit edges $(\mathbf{r}, \mathbf{s}) \rightarrow (\mathbf{r}, \mathbf{s})\sigma$ such that $\mathbf{r}\sigma \not\succeq \mathbf{s}$. In the case that for the node (\mathbf{r}, \mathbf{s}) from two conditions $\mathbf{r}\sigma \succeq \mathbf{q}$ and $\mathbf{s}\sigma \succeq \mathbf{q}$ only the first is valid the algorithm stops and the condition 2 does not hold. The automaton is not right locally testable in this case. ($O(n^2)$ time complexity).

The whole time and space complexity of the algorithm is $O(n^2)$.

6.3 Left local testability of DFA

The algorithm is based on the theorem 39. Let us form a table of reachability on the graph Γ and find all SCC of Γ . Let us find Γ^2 and all SCC of Γ^2 . ($O(n^2)$ time complexity).

Let us check the local idempotency ($O(n^3)$ time complexity).

For check the condition 2 of the theorem let us add to the graph Γ^2 new node $(\mathbf{0}, \mathbf{0})$ with edges from this node to every *SCC*-node (\mathbf{p}, \mathbf{q}) from Γ^2 such that $\mathbf{p} \succeq \mathbf{q}$. Let us consider first-depth search from the node $(\mathbf{0}, \mathbf{0})$.

We do not visit edges $(\mathbf{r}, \mathbf{s}) \rightarrow (\mathbf{r}, \mathbf{s})\sigma$ such that $\mathbf{r}\sigma \not\succeq \mathbf{s}$ and $\mathbf{s}\sigma \not\succeq \mathbf{s}$. In the case that for the node (\mathbf{r}, \mathbf{s}) from two conditions $\mathbf{r}\sigma \succeq \mathbf{s}$ and $\mathbf{s}\sigma \succeq \mathbf{s}$ only one is valid the algorithm stops and the condition 2 does not hold.

Condition 3 of the theorem 39. Let us find Γ^3 and all *SCC*-nodes of Γ^3 ($O(n^3)$ time complexity).

Let us recognize the relation \succ on the graph Γ^2 and find set *Left* of triples $\mathbf{p}, \mathbf{q}, \mathbf{r}$ such that $(\mathbf{p}, \mathbf{q}) \succ (\mathbf{r}, \mathbf{q})$ (see algorithm for table of reachability above).

If for some *SCC*-node $(\mathbf{p}, \mathbf{u}, \mathbf{v})$ of Γ^3 both triples $(\mathbf{p}, \mathbf{u}, \mathbf{v})$ and $(\mathbf{p}, \mathbf{v}, \mathbf{u})$ belong to the set then the condition 3 does not hold, the automaton is not left locally testable and the algorithm stops.

The whole time and space complexity of the algorithm is $O(n^3)$.

References

1. A. Aho, J. Hopcroft, J. Ulman, The Design and Analysis of Computer Algorithms, Addison-Wesley, 1974.
2. D. Belostotski, D. Kravtsov, A. Shemshurenko, M. Sobol, A.N. Trahtman, Sh. Yakov, A package for checking some kinds of testability. 6-th Int. Conf. on Impl. and Appl. of Automata, CIAA2001, Pretoria, 2001.
3. J.-C. Birget, Strict local testability of the finite control of two-way automata and of regular picture description languages, *J. of Alg. Comp.* 1, **2**(1991), 161-175.
4. A.P. Biryukov, Varieties of idempotent semigroups, *Algebra i logika*, 9, 3(1970), 255-273.
5. J.A. Brzozowski, I. Simon, Characterizations of locally testable events, *Discrete Math.* 4, (1973), 243-271.
6. J.C. Costa, Free profinite R-trivial, locally idempotent and locally commutative semigroups. *Sem. Forum*, 58, 3(1999), 423-444.
7. P. Garcia, J. Ruiz, Right and left locally testable languages, *Theoret. Comput. Sci.*, **246**(2000), 253-264.
8. T. Head, Formal languages theory and DNA: an analysis of the generative capacity of specific recombinant behaviors, *Bull. Math. Biol.* **49**(1987), 4, 739-757.
9. R. König, Reduction algorithm for some classes of aperiodic monoids, *R.A.I.R.O. Theor. Inform.*, 19, **3**(1985), 233-260.
10. S. Kim, R. McNaughton, R. McCloskey, A polynomial time algorithm for the local testability problem of deterministic finite automata, *IEEE Trans. Comput.* **40**(1991) N10, 1087-1093.
11. Lallement, G., *Semigroups and Combinatorial Applications*, Wiley, N.Y., 1979.
12. R. McNaughton, S. Papert, *Counter-free automata* M.I.T. Press. Mass., 1971.
13. A.N. Trahtman, A polynomial time algorithm for local testability and its level. *Int. J. of Algebra and Comp.*, vol. 9, 1(1998), 31-39.
14. A.N. Trahtman, Identities of locally testable semigroups. *Comm. in Algebra*, v. 27, 11(1999), 5405-5412.
15. A.N. Trahtman, Piecewise and local threshold testability of DFA. *Lect. Notes in Comp. Sci.*, 2138(2001), 347-358.
16. Y. Zalcstein, Locally testable language, *J. Comp. System Sci.* **6**(1972), 151-167