Large Aperiodic Semigroups*

Janusz Brzozowski[1] and Marek Szykuła[2]

[1] David R. Cheriton School of Computer Science, University of Waterloo,
Waterloo, ON, Canada N2L 3G1
{brzozo@uwaterloo.ca}
[2] Institute of Computer Science, University of Wrocław,
Joliot-Curie 15, PL-50-383 Wrocław, Poland
{msz@cs.uni.wroc.pl}

Abstract. The syntactic complexity of a regular language is the size of its syntactic semigroup. This semigroup is isomorphic to the transition semigroup of a minimal deterministic finite automaton accepting the language, that is, to the semigroup generated by transformations induced by non-empty words on the set of states of the automaton. In this paper we search for the largest syntactic semigroup of a star-free language having n left quotients; equivalently, we look for the largest transition semigroup of an aperiodic finite automaton with n states.

We introduce two new aperiodic transition semigroups. The first is generated by transformations that change only one state; we call such transformations and resulting semigroups *unitary*. In particular, we study *complete* unitary semigroups which have a special structure, and we show that each maximal unitary semigroup is complete. For $n \geqslant 4$ there exists a complete unitary semigroup that is larger than any aperiodic semigroup known to date.

We then present even larger aperiodic semigroups, generated by transformations that map a non-empty subset of states to a single state; we call such transformations and semigroups *semiconstant*. In particular, we examine semiconstant *tree* semigroups which have a structure based on full binary trees. The semiconstant tree semigroups are at present the best candidates for largest aperiodic semigroups.

We also prove that $2^n - 1$ is an upper bound on the state complexity of reversal of star-free languages, and resolve an open problem about a special case of state complexity of concatenation of star-free languages.

Keywords: aperiodic, monotonic, nearly monotonic, partially monotonic, semiconstant, transition semigroup, star-free language, syntactic complexity, unitary

1 Introduction

The *state complexity* of a regular language is the number of states in a complete minimal deterministic finite automaton (DFA) accepting the language [17]. An

---

equivalent notion is that of *quotient complexity,* which is the number of left quotients of the language [1]; we prefer quotient complexity since it is a language-theoretic notion. The usual measure of complexity of an operation on regular languages [1, 17] is the quotient complexity of the result of the operation as a function of the quotient complexities of the operands. This measure has some serious disadvantages, however. For example, as shown in [7], in the class of star-free languages all common operations have the same quotient complexity as they do in the class of arbitrary regular languages[3]. Thus quotient complexity fails to differentiate between the very special class of star-free languages and the class of all regular languages.

It has been suggested that other measures of complexity may also be useful [2], in particular, the *syntactic complexity* of a regular language which is the cardinality of its syntactic semigroup [15]. This is the same as the cardinality of the *transition semigroup* of a minimal DFA accepting the language, and it is this latter representation that we use here. The transition semigroup is the set of all transformations induced by non-empty words on the set of states of the DFA. The *syntactic complexity of a class* of languages is the size of the largest syntactic semigroups of languages in that class as a function of the quotient complexities of the languages. Since the syntactic complexity of star-free languages is considerably smaller than that of regular languages, this measure succeeds in distinguishing the two classes.

The class of *star-free* languages is the smallest class obtained from finite languages using only boolean operations and concatenation, but no star. By Schützenberger's theorem [16] we know that a language is star-free if and only if the transition semigroup of its minimal DFA is *aperiodic*, meaning that it contains no non-trivial subgroups. Equivalently, a transition semigroup is aperiodic if and only if no word over the alphabet of the DFA can induce a non-trivial permutation of any subset of two or more states. Star-free languages and the DFAs that accept them were studied by McNaughton and Papert in 1971 [14].

Two aperiodic semigroups, monotonic and partially monotonic, were studied by Gomes and Howie [10]. Their results were adapted to finite automata in [6], where nearly monotonic semigroups were also introduced; they are larger than the partially monotonic ones and were the largest aperiodic semigroups known to date for $n \leqslant 7$. For $n \geqslant 8$ the largest aperiodic semigroups known to date were those generated by DFAs accepting $\mathcal{R}$-trivial languages [5]. The syntactic complexity of $\mathcal{R}$-trivial languages is $n!$. As to aperiodic semigroups, tight upper bounds on their size were known only for $n \leqslant 3$.

The following are the main contributions of this paper:

1. Using the method of [13], we have enumerated all aperiodic semigroups for $n = 4$, and we have shown that the maximal aperiodic semigroup has size 47, while the maximal nearly monotonic semigroup has size 41. Although this may seem like an insignificant result, it provided us with strong motivation to search for larger semigroups.

---

[3] Two small exceptions are discussed in Section 6.

The number of aperiodic transformations is $(n + 1)^{n-1}$. For large n the number of aperiodic semigroups is very large, and so it is difficult to check them all.

2. We studied semigroups generated by transformations that change only one state; we call such transformations and semigroups *unitary*. We characterized unitary semigroups and computed their maximal sizes up to $n = 1,000$. There are $n(n - 1)$ unitary transformations. For $n \geqslant 4$ the maximal unitary semigroups are larger than the maximal nearly monotonic ones and also larger than any previously known aperiodic semigroup.

3. For each n we found a set of DFAs whose inputs induce *semiconstant tree transformations* – transformations that send a non-empty subset of the set of all states to a single state, and have a structure based on full binary trees. For $n \geqslant 4$, there is a semiconstant tree semigroup larger than the largest complete unitary semigroup. We computed the maximal size of these transition semigroups up to $n = 500$. The total number of semiconstant transformations is $(2^{n-1} - 1)n$.

4. We derived formulas for the sizes of complete unitary and semiconstant tree semigroups. We also provided recursive formulas characterizing the maximal complete unitary and semiconstant tree semigroups; these formulas lead to efficient algorithms for computing the forms and sizes of such semigroups.

5. We proved that the quotient complexity of the reverse of a star-free language with quotient complexity n is at most $2^n - 1$.

6. We resolved an open problem about a special case of quotient complexity of product (catenation, concatenation) of star-free languages K and L, when the quotient complexities of K and L are $m \geqslant 2$ and 2, respectively: we proved that $3m - 2$ is a tight upper bound.

Our results about aperiodic semigroups are summarized in Tables 1 and 2 for small values of n. Transformation **1** is the identity; it can be added to unitary and semiconstant transformations without affecting aperiodicity.

Additional information about the classes of semigroups in Tables 1 and 2 will be given later. The classes are listed in the order of increasing size when n is large. The number in boldface shows the value of n for which the size of a given semigroup exceeds the sizes of all of the preceding ones. For example, the largest semigroups of finite languages exceed the preceding semigroups for $n \geqslant 12$.

There are two more classes of syntactic semigroups that have the same complexity as the semigroups of finite languages: those of cofinite and reverse definite languages. The tight upper bound $\lfloor e \cdot (n-1)! \rfloor$ for $\mathcal{J}$-trivial languages ([5]) is also a lower bound for definite languages ([6]). An upper bound of $n((n-1)! - (n-3)!)$ has been shown to hold [12] for definite and generalized definite languages [9], but it is not known whether this bound is tight.

The asymptotic behaviour of the size $e(n)$ of partially monotonic semigroups is $A \frac{B^{2n-1}}{\sqrt{n}}$, where A and B are constants [6]. For nearly monotonic semigroups the size is $e(n) + n - 1$.

Table 1. Large aperiodic semigroups.

$n:$	1	2	3	4	5	6	7	8
Monotonic $\binom{2n-1}{n}$	1	3	10	35	126	462	1,716	6,435
Part. mon. $e(n)$	−	2	8	**38**	192	1,002	5,336	28,814
Near. mon. $e(n)+n-1$	−	3	**10**	41	196	1,007	5,342	28,821
Finite $(n-1)!$	1	1	2	6	24	120	720	5,040
$\mathcal{J}$-trivial $\lfloor e\cdot(n-1)!\rfloor$	1	2	5	16	65	326	1,957	13,700
$\mathcal{R}$-trivial $n!$	1	2	6	24	120	720	5,040	**40,320**
Complete unitary with **1**	−	3	10	**45**	270	1,737	13,280	121,500
Semiconstant tree with **1**	−	3	10	**47**	273	1,849	14,270	126,123
Aperiodic	1	3	10	47	?	?	?	?

Table 2. Large aperiodic semigroups continued.

$n:$	9	10	11	12	13
Monotonic	24,310	92,378	352,716	1,352,078	5,200,300
Part. mon.	157,184	864,146	4,780,008	26,572,086	148,321,344
Near. mon.	157,192	864,155	4,780,018	26,572,097	148,321,352
Finite	40,320	362,880	3,628,800	**39,916,800**	479,001,600
$\mathcal{J}$-trivial	109,601	**986,410**	9,864,101	108,505,112	1,302,061,345
$\mathcal{R}$-trivial	362,880	3,628,800	39,916,800	479,001,600	6,227,020,800
Comp. unit., **1**	1,231,200	12,994,020	151,817,274	2,041,564,499	29,351,808,000
Sc. tree, **1**	1,269,116	14,001,630	169,410,933	2,224,759,334	31,405,982,420
Aperiodic	?	?	?	?	?

The remainder of the paper is structured as follows. Section 2 presents our terminology and notation. Our large aperiodic semigroups are defined in Section 3. The special case of unitary semigroups is then considered in Section 4, and semiconstant tree semigroups are the topic of Section 5. Section 6 contains the new results about reversal and product. Section 7 concludes the paper.

2 Terminology and Notation

Let Σ be a finite alphabet. The elements of Σ are *letters* and the elements of Σ^* are *words*, where Σ^* is the free monoid generated by Σ. The empty word

is denoted by ε, and the set of all non-empty words is Σ^+, the free semigroup generated by Σ. A *language* is any subset of Σ^*.

Suppose $n \geqslant 1$. Without loss of generality we assume that our basic set under consideration is $Q = \{0, 1, \ldots, n-1\}$. A *deterministic finite automaton (DFA)* is a quintuple $\mathcal{D} = (Q, \Sigma, \delta, 0, F)$, where Q is a finite non-empty set of *states*, Σ is a finite non-empty *alphabet*, $\delta\colon Q \times \Sigma \to Q$ is the *transition function*, $0 \in Q$ is the *initial state*, and $F \subseteq Q$ is the set of *final states*. We extend δ to $Q \times \Sigma^*$ and to $2^Q \times \Sigma^*$ in the usual way. A DFA $\mathcal{D}$ *accepts* a word $w \in \Sigma^*$ if $\delta(0, w) \in F$. The *language accepted* by $\mathcal{D}$ is $L(\mathcal{D}) = \{w \in \Sigma^* \mid \delta(0, w) \in F\}$.

By the *language of a state* q of $\mathcal{D}$ we mean the language $L_q(\mathcal{D})$ accepted by the DFA $(Q, \Sigma, \delta, q, F)$. A state is *empty* (also called *dead* or a *sink*) if its language is empty. Two states p and q of $\mathcal{D}$ are *equivalent* if $L_p(\mathcal{D}) = L_q(\mathcal{D})$. Otherwise, states p and q are *distinguishable*. A state q is *reachable* if there exists a word $w \in \Sigma^*$ such that $\delta(0, w) = q$. A DFA is *minimal* if all its states are reachable and pairwise distinguishable.

A *transformation* of Q is a mapping of Q into itself. Let t be a transformation of Q; then qt is the *image* of $q \in Q$ under t. If P is a subset of Q, then $Pt = \{qt \mid q \in P\}$. An arbitrary transformation can be written in the form

$$t = \begin{pmatrix} 0 & 1 & \cdots & n-2 & n-1 \\ p_0 & p_1 & \cdots & p_{n-2} & p_{n-1} \end{pmatrix},$$

where $p_q = qt$ for $q \in Q$. We also use $t = [p_0, \ldots, p_{n-1}]$ as a simplified notation. The *composition* of two transformations t_1 and t_2 of Q is a transformation $t_1 \circ t_2$ such that $q(t_1 \circ t_2) = (qt_1)t_2$ for all $q \in Q$. We usually drop the composition operator "$\circ$" and write $t_1 t_2$.

Let $\mathcal{T}_Q$ be the set of all n^n transformations of Q; then $\mathcal{T}_Q$ is a monoid under composition. The *identity* transformation $\mathbf{1}$ maps each element to itself, that is, $q\mathbf{1} = q$ for all $q \in Q$. For $k \geqslant 2$, a transformation (permutation) t of a set $P = \{q_0, q_1, \ldots, q_{k-1}\} \subseteq Q$ is a *k-cycle* if $q_0 t = q_1, q_1 t = q_2, \ldots, q_{k-2} t = q_{k-1}, q_{k-1} t = q_0$. A k-cycle is denoted by $(q_0, q_1, \ldots, q_{k-1})$. If a transformation t of Q acts like a k-cycle on some $P \subseteq Q$, we say that t has a *k-cycle*. A transformation has a *cycle* if it has a k-cycle for some $k \geqslant 2$. For $p \neq q$, a *transposition* is the 2-cycle (p, q). A *permutation* of Q is a mapping of Q *onto* itself. A transformation is *aperiodic* if it contains no cycles.

In any DFA $\mathcal{D}$, each word $w \in \Sigma^*$ induces a transformation t_w of Q defined by $qt_w = \delta(q, w)$ for all $q \in Q$. The set of all transformations of Q induced in $\mathcal{D}$ by non-empty words is the *transition semigroup* of $\mathcal{D}$. This semigroup is a subsemigroup of $\mathcal{T}_Q$. If $\mathcal{D}$ is minimal, its transition semigroup is isomorphic to the *syntactic semigroup* of the language $L(\mathcal{D})$ [14, 15]. A language is regular if and only if its syntactic semigroup is finite. The size of the syntactic semigroup of a language is called its *syntactic complexity*. In this paper we deal only with transition semigroups; consequently, we view syntactic complexity as the size of the transition semigroup.

If T is a set of transformations, then $\langle T \rangle$ is the semigroup generated by T. If $\mathcal{D} = (Q, \Sigma, \delta, 0, F)$ is a DFA, the transformations induced by letters of Σ are called *generators of the transition semigroup* of $\mathcal{D}$ or simply *generators* of $\mathcal{D}$.

3   Unitary and Semiconstant DFAs

We now define a new class of aperiodic DFAs among which are found the largest transition semigroups known to date. We also study several of its subclasses.

A *unitary* transformation t, denoted by $(p \to q)$, has $p \neq q$, $pt = q$ and $rt = r$ for all $r \neq p$. A DFA is *unitary* if each of its generators is unitary. A semigroup is *unitary* if it has a set of unitary generators.

A *constant* transformation t, denoted by $(Q \to q)$, has $pt = q$ for all $p \in Q$. A transformation t is *semiconstant* if it maps a non-empty subset P of Q to a single element q and leaves the remaining elements of Q unchanged. It is denoted by $(P \to q)$. A constant transformation is semiconstant with $P = Q$, and a unitary transformation $(p \to q)$ is semiconstant with $P = \{p\}$ (or $P = \{p, q\}$). A DFA is *semiconstant* if each of its generators is semiconstant. A semigroup is *semiconstant* if it has a set of semiconstant generators.

For each $n \geqslant 1$ we shall define several DFAs. Let $m, n_1, n_2, \ldots, n_m$ be positive natural numbers. Also, let $n = n_1 + \cdots + n_m$, and for each i, $1 \leqslant i \leqslant m$, define r_i by $r_i = \sum_{j=1}^{i-1} n_j$. For $i = 1, \ldots, m$, let $Q_i = \{r_i, r_i + 1, \ldots, r_{i+1} - 1\}$; thus the cardinality of Q_i is n_i. Let $Q = Q_1 \cup \cdots \cup Q_m = \{0, \ldots, n-1\}$; the cardinality of Q is n. The sequence $(n_1, n_2, \ldots, n_m)$ is called the *distribution* of Q.

Remark 1. The number $d(n)$ of different distributions for each n is 2^{n-1}. This is easily verified by induction on n. For $n = 1$ there is only one distribution, namely (1); hence $d(1) = 2^0$. Suppose that $d(k) = 2^{k-1}$ for $k < n$. For n, each distribution is either (n) or it has m, where $m \in \{n-1, \ldots, 1\}$, combined with any distribution of the integer $n - m$. Hence the number of distributions is $1 + d(1) + d(2) + \cdots + d(n-1) = 1 + 1 + 2 + \cdots + 2^{n-2} = 2^{n-1}$. For example, for $n = 3$ we have the distributions $(3), (2,1), (1,2), (1,1,1)$. ■

A binary tree is *full* if every vertex has either two children or no children. There are C_{m-1} full binary trees, where $C_m = \frac{1}{m+1}\binom{2n}{n}$ is the Catalan number[4].

Let Δ_Q be a full binary tree with m leaves labeled $Q_1, \ldots, Q_m$ from left to right. To each node $v \in \Delta_Q$, we assign the union $\mathrm{Q}(v)$ of all the sets Q_i labeling the leaves in the subtree rooted at v.

With each full binary tree we can associate different distributions. A full binary tree Δ_Q with a distribution attached is denoted by $\Delta_Q(n_1, n_2, \ldots, n_m)$ and is called the *structure* of Q. This structure will uniquely determine the transition function δ of the DFAs defined below. The number of possible structures of Q for a given n is the binomial transform of C_n, the Catalan number[5].

We can denote the structure of Q as a binary expression. For example, the expression $((3,2),(4,1))$ denotes the full binary tree in which the leaves are

---
[4] http://en.wikipedia.org/wiki/Catalan_number
[5] http://oeis.org/A007317

labeled Q_1, Q_2, Q_3, and Q_4, where $|Q_1| = 3, |Q_2| = 2, |Q_3| = 4, |Q_4| = 1$, and the interior nodes are labeled by $Q_1 \cup Q_2$, $Q_3 \cup Q_4$ and $Q_1 \cup Q_2 \cup Q_3 \cup Q_4$. On the other hand, the expression $(((3, 2), 4), 1)$ has interior nodes labeled $Q_1 \cup Q_2$, $Q_1 \cup Q_2 \cup Q_3$ and $Q_1 \cup Q_2 \cup Q_3 \cup Q_4$.

Definition 1 (Transformations).

Type 1: *Suppose $n > 1$ and $(n_1, n_2, \ldots, n_m)$ is a distribution of Q. For all $i = 1, \ldots, m$ and $q, q + 1 \in Q_i$ Type 1 transformations are the unitary transformations $(q \to q + 1)$ and $(q + 1 \to q)$.*

Type 2: *Suppose $n > 1$ and $(n_1, n_2, \ldots, n_m)$ is a distribution of Q. If $1 \leqslant i \leqslant m - 1$ and $i < j \leqslant m$, for each $q \in Q_i$ and $p \in Q_j$, $(q \to p)$ is a Type 2 transformation.*

Type 3: *Suppose $n > 1$ and $\Delta_Q(n_1, n_2, \ldots, n_m)$ is a structure of Q. For each internal node w the semiconstant transformation $(Q(w) \to \min(Q(w)))$ is of Type 3.*

Type 4: *The identity transformation $\mathbf{1}$ on Q is of Type 4.*

For a fixed i there are $2n_i - 2$ Type 1 transformations and $n_i(n_{i+1} + \cdots + n_m)$ Type 2 transformations. The number of Type 3 transformations is $m - 1$.

Note that the distribution $(n_1, n_2, \ldots, n_m)$ affects transformations of Types 1, 2, and 3, whereas the binary tree affects only transformations of Type 3.

In the following DFAs the transition function is defined by a set of transformations and the alphabet consists of letters inducing these transformation.

Definition 2 (DFAs). *Suppose $n > 1$.*

1. *If there is no $i \in \{1, \ldots, m - 1\}$ such that $|Q_i| = |Q_{i+1}| = 1$, then any DFA of the form $\mathcal{D}_u(n_1, \ldots, n_m) = (Q, \Sigma_u, \delta_u, 0, \{n - 1\})$, where δ_u has all the transformations of Types 1 and 2, is a complete unitary DFA.*
2. *$\mathcal{D}_{ui}(n_1, \ldots, n_m) = (Q, \Sigma_{ui}, \delta_{ui}, 0, \{n - 1\})$ is $\mathcal{D}_u(n_1, \ldots, n_m)$ with $\mathbf{1}$ added.*
3. *Any DFA $\mathcal{D}_{sct}(\Delta_Q(n_1, \ldots, n_m)) = (Q, \Sigma_{sct}, \delta_{sct}, 0, \{n - 1\})$, where δ_{sct} has all the transformations of Types 1, 2 and 3, is a semiconstant tree DFA.*
4. *$\mathcal{D}_{scti}(\Delta_Q(n_1, \ldots, n_m)) = (Q, \Sigma_{scti}, \delta_{scti}, 0, \{n - 1\})$ is $\mathcal{D}_{sct}(\Delta_Q(n_1, \ldots, n_m))$ with $\mathbf{1}$ added.*

Using terminology analogous to that of [8], we define a *bipath (bidirectional path)* to be a graph (V, E), where $V = \{v_0, \ldots, v_{k-1}\}$ for some $k \geqslant 1$, and for each $v_q, v_{q+1} \in V$ there are two edges (v_q, v_{q+1}) and (v_{q+1}, v_q). If $k = 1$, the graph $(\{v_0\}, \emptyset)$ is also considered a (trivial) bipath. If we ignore self-loops, each edge in the graph uniquely determines a unitary transformation, and the states in each Q_i in $\mathcal{D}_u(n_1, \ldots, n_m)$ constitute a *bipath*. Also, the graph of $\mathcal{D}_u(n_1, \ldots, n_m)$ is a sequence $(Q_1, \ldots, Q_m)$ of bipaths, where there are transitions from every q in Q_i to every p in Q_j, if $i < j$.

Example 1. Figure 1 shows three examples of unitary DFAs. In Fig. 1 (a) we have DFA $\mathcal{D}_u(3)$, where the letter a_{pq} induces the unitary transformation $(p \to q)$. In Fig. 1 (b) we present $\mathcal{D}_u(3)$, where only the transitions between *different* states

are included to simplify the figure. Also, the letter labels are deleted because they are easily deduced. Next, in Figs. 1 (c) and (d), we have the DFAs $\mathcal{D}_u(3,1)$ and $\mathcal{D}_u(2,2,2)$, respectively. We shall return to these examples later. ∎
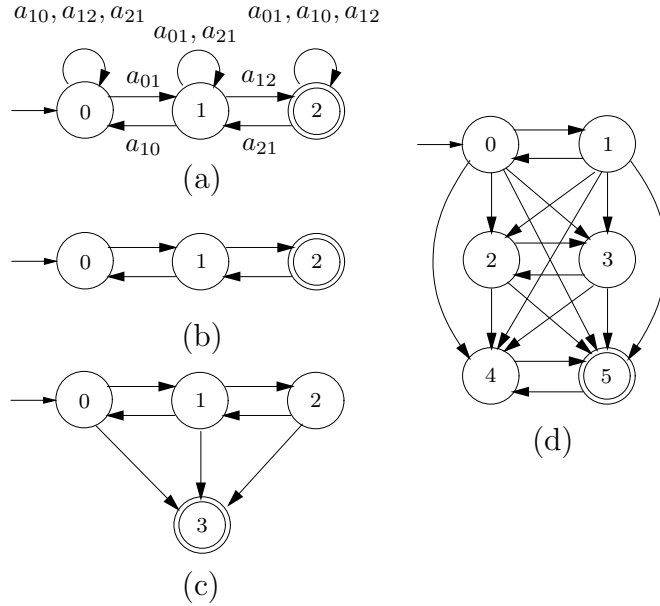

Fig. 1. Unitary DFAs: (a) $\mathcal{D}_u(3)$; (b) $\mathcal{D}_u(3)$ simplified; (c) $\mathcal{D}_u(3,1)$; (d) $\mathcal{D}_u(2,2,2)$.

Remark 2. All four DFAs of Definition 2 are minimal as is easily verified. Hence the syntactic semigroup of the language of each DFA is isomorphic to the transition semigroup of the DFA. ∎

4 Unitary Semigroups

We study unitary semigroups because their generators are the simplest. We begin with three previously studied special semigroups which are subsemigroups of a unitary semigroups.

4.1 Monotonic Semigroups

Monotonic semigroups were previously studied in [6, 10, 11]. A transformation t of Q is *monotonic* if there exists a total order $\leqslant$ on Q such that, for all $p, q \in Q$,

$p \leqslant q$ implies $pt \leqslant qt$. Note that the identity transformation is monotonic. A DFA is *monotonic* if each of its input transformations is monotonic. A semigroup is *monotonic* if it has a set of monotonic generators. From now on we assume that $\leqslant$ is the usual order on integers.

The following result of [10] is somewhat modified for our purposes:

Proposition 1 (Gomes and Howie). *The set M of all $\binom{2n-1}{n} - 1$ monotonic transformations other than $\mathbf{1}$ is an aperiodic semigroup generated by*

$$G_M = \{(q \to q+1) \mid 0 \leqslant q \leqslant n-2\} \cup \{(q \to q-1) \mid 1 \leqslant q \leqslant n-1\},$$

and no smaller set of unitary transformations generates M.

Corollary 1. *The transition semigroup of $\mathcal{D}_{ui}(n)$ is the semigroup $M \cup \{\mathbf{1}\}$ of all monotonic transformations.*

Note that $\mathcal{D}_u$ has transitions of Type 1 only, and D_{ui} has Type 1 and 4 only. Figure 1 (b) shows $\mathcal{D}_u(3)$ and $\mathcal{D}_{ui}(3)$, if $\mathbf{1}$ is added. The transition semigroup of $\mathcal{D}_{ui}(3)$ has ten elements and is the largest aperiodic semigroup for $n = 3$ [6].

Note also that there are monotonic semigroups that do not have unitary generating sets; each monotonic semigroup, however, is a subsemigroup of the transition semigroup of $\mathcal{D}_{ui}(n)$ consisting of all monotonic transformations.

4.2 Partially Monotonic Semigroups

A *partial transformation* t of Q is a partial mapping of Q into itself. If t is defined for $q \in Q$, then qt is the image of q under t; otherwise, we write $qt = \square$. By convention, $\square t = \square$. The *domain* of t is the set $dom(t) = \{q \in Q \mid qt \neq \square\}$. A partial transformation is *monotonic* if there exists an order $\leqslant$ on Q such that for all $p, q \in dom(t)$, $p \leqslant q$ implies $pt \leqslant qt$.

Semigroups of monotonic partial transformations were studied by Gomes and Howie [10]. They were adapted to automata in [6]. We follow [6] by starting with all partial transformations of $Q \setminus \{n-1\}$ and adding state $(n-1)$ for the undefined value $\square$. We call the resulting transformations *partially monotonic*. The following is an adaptation of the results of [10]:

Proposition 2. *For $n \geqslant 2$, the DFA $\mathcal{D}_{ui}(n-1, 1) = (Q, \Sigma_{ui}, \delta_{ui}, 0, \{n-1\})$ has the following properties:*

1. *Each of the $3n - 4$ transformations of $\mathcal{D}_{ui}(n-1, 1)$ is partially monotonic. Thus $\mathcal{D}_{ui}(n-1, 1)$ is partially monotonic, and hence aperiodic.*
2. *The transition semigroup PM_Q of $\mathcal{D}_{ui}(n-1, 1)$ consists of all the $e(n)$ partially monotonic transformations of Q, where*

$$e(n) = \sum_{k=0}^{n-1} \binom{n-1}{k} \binom{n+k-2}{k}. \tag{1}$$

9

3. *Each generator is idempotent, and $3n - 4$ is the smallest number of idempotent generators of PM_Q. Moreover, each generator except $\mathbf{1}$ is unitary, and $3n - 5$ is the smallest number of unitary generators of $PM_Q \setminus \{\mathbf{1}\}$.*

Example 2. There are eight monotonic partial transformations of the set $Q = \{0, 1\}$, namely: $[\square, \square]$, $[0, \square]$, $[1, \square]$, $[\square, 0]$, $[\square, 1]$, $[0, 0]$, $[0, 1]$, $[1, 1]$. When we replace $\square$ by state 2, the eight partial transformations become total transformations $[2, 2, 2]$, $[0, 2, 2]$, $[1, 2, 2]$, $[2, 0, 2]$, $[2, 1, 2]$, $[0, 0, 2]$, $[0, 1, 2]$, $[1, 1, 2]$. The $9 - 4 = 5$ generators of $\mathcal{D}_{ui}(2, 1)$ are: $(0 \to 1) = [1, 1, 2]$, $(0 \to 2) = [2, 1, 2]$, $(1 \to 0) = [0, 0, 2]$, $(1 \to 2) = [0, 2, 2]$ and $\mathbf{1}$. The DFA of Figure 1 (c) is an example of $\mathcal{D}_{ui}(3, 1)$. ∎

For $n \geqslant 4$ the semigroup of all partially monotonic transformations is larger than the semigroup of all monotonic transformations.

Note that there are partially monotonic semigroups that do not have unitary generating sets; each partially monotonic semigroup, however, is a subsemigroup of the transition semigroup of $\mathcal{D}_{ui}(n - 1, 1)$ consisting of all partially monotonic transformations.

4.3 Other Previously Studied Aperiodic Semigroups

As we have mentioned in the introduction, the syntactic complexity of five other language classes was studied previously. *Cofinite* languages are complements of finite languages, and therefore their minimal DFAs have the same transition semigroup as the DFAs of finite languages.

The reverse w^R of a word $w \in \Sigma^+$ is w spelled backwards and $\varepsilon^R = \varepsilon$. The reverse of a language L is $L^R = \{w^R \mid w \in L\}$. A language is *definite* if it has the form $E \cup \Sigma^* F$, where E and F are finite. It is *reverse definite* if its reverse is definite, that is, if it has the form $E \cup F \Sigma^*$, where E and F are finite. It was shown in [6] that the syntactic complexity of reverse definite languages is the same as that of finite languages. A lower bound of $\lfloor e(n - 1)! \rfloor$ was proved for definite languages; it is an open question whether this is also an upper bound.

The well known Green relations define $\mathcal{R}$-trivial and $\mathcal{J}$-trivial monoids (semigroups with an identity). If M is a monoid, the relation $\mathcal{R}$ is defined by $s \mathcal{R} t \Leftrightarrow Ms = Mt$ for $s, t \in M$. A monoid is $\mathcal{R}$-*trivial* if $s \mathcal{R} t$ implies $s = t$. The relation $\mathcal{J}$ is defined by $s \mathcal{J} t \Leftrightarrow MsM = MtM$, and M is $\mathcal{J}$-*trivial* if $MsM = MtM$ implies $s = t$. Languages whose minimal DFAs have $\mathcal{R}$-trivial ($\mathcal{J}$-trivial) transition monoids are also called $\mathcal{R}$-*trivial* ($\mathcal{J}$-*trivial*).

Syntactic complexities of $\mathcal{R}$-trivial and $\mathcal{J}$-trivial languages were studied by Brzozowski and Li [5]. Consider the natural order $<$ on Q. We say that a transformation t is non-decreasing if $q \leqslant qt$ for all $q \in Q$. Let $\mathcal{F}_Q$ be the set of all non-decreasing transformations. The size of $\mathcal{F}_Q$ is $n!$.

It was shown in [3] that L is an $\mathcal{R}$-trivial language if and only if its minimal DFA is partially ordered, or equivalently, if its transition semigroup contains only non-decreasing transformations. Thus the largest semigroup generated by DFAs accepting $\mathcal{R}$-trivial languages is $\mathcal{F}_Q$.

Proposition 3. *The transition semigroup of $\mathcal{D}_{ui}(1, 1, \ldots, 1)$ is the semigroup $\mathcal{F}_Q$ of all non-decreasing transformations.*

Proof. DFA $\mathcal{D}_{ui}(1, 1, \ldots, 1)$ has only unitary transformations of Type 2. They generate only non-decreasing transformations, since each of them preserves the natural order. An arbitrary non-decreasing transformation has the form

$$t = \begin{pmatrix} 0 & 1 & \cdots & n-2 & n-1 \\ p_0 & p_1 & \cdots & p_{n-2} & n-1 \end{pmatrix},$$

where $p_q \geqslant q$ for $q = 0, \ldots, n - 2$. Since $\mathcal{D}_{ui}(1, 1, \ldots, 1)$ contains all unitary transformations of the form $(q \to p)$ for $q \leqslant p$, all transformations $t_q = (q \to p_q)$ are present. One verifies that applying $t_{n-2} t_{n-3} \cdots t_1 t_0$ results in t. Thus each non-decreasing transformation can be generated by at most $n - 1$ unitary transformations. $\qquad\square$

Note that there are semigroups with only non-decreasing transformations that do not have unitary generating sets; each such semigroup, however, is a subsemigroup of $\mathcal{F}_Q$. Since every $\mathcal{J}$-trivial language is also $\mathcal{R}$-trivial, the transition semigroups of all minimal DFAs accepting $\mathcal{J}$-trivial languages are also subsemigroups of $\mathcal{D}_{ui}(1, 1, \ldots, 1)$.

4.4 General Unitary Semigroups

A set $\{t_0, \ldots, t_{k-1}\}$ of unitary transformations is *k-cyclic* if it has the form $t_0 = (q_0 \to q_1)$, $t_1 = (q_1 \to q_2), \ldots, t_{k-2} = (q_{k-2} \to q_{k-1})$, $t_{k-1} = (q_{k-1} \to q_0)$, where the q_i are distinct.

Lemma 1. *Let T be a set of unitary transformations.*

1. *If T has a k-cyclic subset $\{t_0, \ldots, t_{k-1}\}$ with $k \geqslant 3$, then $\langle T \rangle$ is not aperiodic.*
2. *If T contains a subset $T_6 = \{t_{01}, t_{10}, t_{12}, t_{13}, t_{21}, t_{31}\}$ where $t_{i,j} = (q_i \to q_j)$ and $q_0, q_1, q_2, q_3 \in Q$, then $\langle T \rangle$ is not aperiodic.*

Proof. Without loss of generality, we can replace q_i by i in both claims.

1. Suppose that T contains $t_0, \ldots, t_{k-1}$, where $k \leqslant n$, $t_q = (q, q + 1)$ for $q = 0, \ldots, k - 2$, and $t_{k-1} = (k - 1 \to 0)$. Then $t_{k-2} t_{k-3} \ldots t_1 t_0 t_{k-1}$ maps 0 to $1, 1$ to $2, \ldots, k-3$ to $k-2, k-2$ to 0, and $k-1$ to 0, and does not affect any other states. Thus the set $\{0, 1, \ldots, k - 2\}$ is cyclically permuted, which shows that $\langle T \rangle$ is not aperiodic.
2. If $\{t_{01}, t_{12}, t_{13}, t_{10}, t_{21}, t_{31}\} \subseteq T$, then the transformation $t_{12} t_{01} t_{13} t_{21} t_{10} t_{31}$ transposes 0 and 1; hence $\langle T \rangle$ is not aperiodic. $\qquad\square$

Theorem 1. *If $\mathcal{D} = (Q, \Sigma, \delta, 0, F)$ is unitary, the following are equivalent:*

1. *$\mathcal{D}$ is aperiodic.*
2. *The set of generators of $\mathcal{D}$ does not contain any k-cyclic subsets with $k \geqslant 3$, and does not contain any sets of type T_6.*

3. Every strongly connected component of $\mathcal{D}$ is a bipath.

Proof. $1 \Rightarrow 2$: This follows from Lemma 1.

$2 \Rightarrow 3$: Consider a strongly connected component C. If $|C| = 1$, the claim holds. Otherwise, suppose $p \in C$ and $(p \to q)$ is a transition. Then there must also be a directed path from q to p. If the last transition in that path is $(r \to p)$, where $r \neq q$, then the set of generators must contain a k-cyclic subset with $k \geqslant 3$, which is a contradiction. Hence the transition $(q \to p)$ must be present.

Next, suppose that there are transitions $(p \to q)$, $(p \to r)$, and $(p \to s)$. By the argument above there must also be transitions $(q \to p)$, $(r \to p)$, and $(r \to s)$. But then the set of generators contains a subset of type T_6, which is again a contradiction.

It follows that every strongly connected component is a bipath, and the graph of the transitions of $\mathcal{D}$ is a loop-free connection of such bipaths.

$3 \Rightarrow 1$: Since a bipath is monotonic, it is aperiodic by Proposition 1. By Schützenberger's theorem [16], the language of all words taking any state of the bipath to any other state of that bipath is star-free. Since the graph of $\mathcal{D}$ is a loop-free connection of bipaths, the language of all words taking any state of $\mathcal{D}$ to any other state of $\mathcal{D}$ is star-free. Hence $\mathcal{D}$ is aperiodic. $\qquad\square$

A unitary DFA is *complete* if the addition of any unitary transition results in a DFA that is not aperiodic.

Theorem 2. *A maximal aperiodic unitary semigroup is isomorphic to the transition semigroup of a complete unitary DFA $\mathcal{D}_u(n_1, \ldots, n_m)$, where $(n_1, \ldots, n_m)$ is some distribution of Q.*

Proof. We know that an aperiodic unitary DFA $\mathcal{D}$ is a loop-free connection of bipaths. Let $Q_1, \ldots, Q_m$ be the bipaths of $\mathcal{D}$. There exists a linear ordering $<$ of them, such that there is no transformation $(p \to q)$ for $q \in Q_i, p \in Q_j, i < j$. If all possible transformations $(q \to p)$ for $q \in Q_i, p \in Q_j, i < j$ are present, then $\mathcal{D}$ is isomorphic to $\mathcal{D}_u(n_1, \ldots, n_m)$. Otherwise we can add more unitary transformations of Type 2 and obtain a larger semigroup. $\qquad\square$

For each distribution $(n_1, \ldots, n_m)$, we calculate the size of the transition semigroup of $\mathcal{D}_{ui}(n_1, \ldots, n_m)$.

Theorem 3. *The cardinality of the transition semigroup of $\mathcal{D}_{ui}(n_1, \ldots, n_m)$ is*

$$\prod_{i=1}^{m} \left(\binom{2n_i - 1}{n_i} + \sum_{h=0}^{n_i - 1} \left(\sum_{j=i+1}^{m} n_j \right)^{n_i - h} \binom{n_i}{h} \binom{n_i + h - 1}{h} \right). \qquad (2)$$

Proof. As above $\mathcal{D}_{ui}(n_1, \ldots, n_m)$ is a loop-free connection of bipaths, and its generators are the transformations within each bipath, all transformations of the form $(p \to q)$ where $p \in Q_i$, $q \in Q_j$, $i < j$, and **1**.

In the transition semigroup of $\mathcal{D}_{ui}(n_1, \ldots, n_m)$, consider the transformation t_i that (a) does not affect any states in Q_j for $j < i$, (b) maps some number h

12

of states of Q_i to Q_i, and (c) maps the remaining $n_i - h$ states of Q_i to some states in $Q_{i+1} \cup \cdots \cup Q_m$. It is convenient to temporarily consider a partial transformation t'_i which for all $q \in Q_i$ has the property $qt'_i = qt_i$, if $qt_i \in Q_i$ and $qt'_i = \square$, otherwise. In other words, the images of the $n_i - h$ states mapped to the outside of Q_i are all lumped together into the undefined value $\square$. The number of such partial transformations generated by the transitions in the bipath is $\binom{n_i}{h}\binom{n_i+h-1}{h}$ [10]; these are all the partially monotonic transformations of Q_i that map exactly h states of Q_i to Q_i.

Returning now to t_i, consider first the case $h = n_i$; then t'_i is a total transformation equal to t_i, and there are $\binom{2n_i-1}{n_i}$ such transformations. Otherwise, t_i maps $n_i - h$ states of Q_i to arbitrary states in $Q_{i+1} \cup \cdots \cup Q_m$. If $k = n_{i+1} + \cdots + n_m$ is the number of states in the bipaths below Q_i, then for each t'_i there are k^{n_i-h} transformations t_i. Altogether, for a fixed bipath Q_i, the number of transformations t_i is

$$\binom{2n_i - 1}{n_i} + \sum_{h=0}^{n_i-1} k^{n_i-h}\binom{n_i}{h}\binom{n_i + h - 1}{h}. \tag{3}$$

If t is any transformation of $\mathcal{D}_{ui}(n_1, \ldots, n_m)$, then it can be represented by $t = t_m \circ t_{m-1} \circ \cdots \circ t_1$, where t_i maps Q_i into $Q_i \cup \ldots \cup Q_m$. Since the domains of $t_1, \ldots, t_m$ are disjoint, there is a bijection between transformations t and the sets $\{t_1, \ldots, t_m\}$. Hence we can multiply the numbers of different transformations t_i for each $1 \leqslant i \leqslant m$, and the formula in the theorem results. $\square$

Note that each factor of the product in Theorem 3 depends only on n_i and on the sum $k = n_{i+1} + \cdots + n_m$. Hence if $\mathcal{D}_{ui}(n_1, \ldots, n_m)$ is maximal, then $\mathcal{D}_{ui}(n_2, \ldots, n_m)$ is also maximal and so on. Consequently, we have

Corollary 2. *Let $m_{ui}(n)$ be the cardinality of the largest transition semigroup of DFA $\mathcal{D}_{ui}(n_1, \ldots, n_m)$ with n states. If we define $m_{ui}(0) = 1$, then for $n > 0$*

$$m_{ui}(n) = \max_{j=1,\ldots,n} \left(m_{ui}(n - j)\left(\binom{2j - 1}{j} + \sum_{h=0}^{j-1}(n - j)^{j-h}\binom{j}{h}\binom{j + h - 1}{h}\right)\right). \tag{4}$$

This leads directly to a dynamic algorithm taking $O(n^3)$ time for computing $m_{ui}(n)$ and the distributions $(n_1, \ldots, n_m)$ yielding the maximal unitary semigroups. This holds assuming constant time for computing the internal terms in the summation and summing them, where, however, the numbers can be very large ($O(n^n)$). The precise complexity depends on the algorithms used for multiplication, exponentiation and calculation of binomial coefficients.

We were able to compute the maximal $\mathcal{D}_{ui}$ up to $n = 1,000$. Here is an example of the maximal one for $n = 100$:

$$\mathcal{D}_{ui}(12, 11, 10, 10, 9, 8, 8, 7, 6, 5, 5, 4, 3, 2);$$

its syntactic semigroup size exceeds 2.1×10^{160}. Compare this to the previously known largest semigroup of an $\mathcal{R}$-trivial language; its size is 100! which is approximately 9.3×10^{157}. On the other hand, the maximal possible syntactic semigroup of any regular language for $n = 100$ is 10^{200}.

13

4.5 Asymptotic Lower Bound

We were not able to compute the tight asymptotic bound on the maximal size of unitary semigroups. However, we computed a lower bound which is larger than $n!$, the previously known lower bound for the size of aperiodic semigroups.

Theorem 4. *For n even the size of the maximal unitary semigroup is at least*

$$\frac{n!(n+1)!}{2^n((n/2)!)^2}.$$

Proof. Let n be even and consider $\mathcal{D}_{ui}(2, 2, \ldots, 2)$ consisting of $m = n/2$ bipaths. From Theorem 3 we have:

$$\prod_{i=1}^{m}\left(\binom{4-1}{2} + \sum_{h=0}^{1}\left(\sum_{j=i+1}^{m} 2\right)^{2-h}\binom{2}{h}\binom{2+h-1}{h}\right)$$

$$= \prod_{i=1}^{m} 4(m-i)^2 + 8(m-i) + 3$$

$$= \prod_{i=1}^{m}(2i-1)(2i+1)$$

$$= (2m-1)!!(2m+1)!!$$

$$= (2m-1)!!(2(m+1)-1)!!$$

By using the equality $(2k-1)!! = \frac{(2k)!}{2^k k!}$ we obtain:

$$= \frac{(2m)!}{2^m m!}\frac{(2(m+1))!}{2^{m+1}(m+1)!}$$

$$= \frac{(2m)!(2m+2)!}{2^{2m+1}m!(m+1)!}$$

$$= \frac{n!(n+2)!}{2^{n+1}(n/2)!((n/2)+1)!}$$

$$= \frac{n!(n+2)(n+1)!}{2^{n+1}(n/2)!(n/2+1)(n/2)!}$$

$$= \frac{n!(n+1)!}{2^n((n/2)!)^2}.$$

$\square$

For $n = 100$ the bound exceeds 7.5×10^{158}. Larger lower bounds can also be found using increasing values of j in $\mathcal{D}_{ui}(j, j, \ldots, j)$, but the complexity of the calculations increases, and such bounds are not tight.

5 Semiconstant Semigroups

We now consider our largest aperiodic semigroups, the semiconstant ones.

5.1 Nearly Monotonic Semigroups

Let K_Q be the set of all constant transformations of Q, and $NM_Q = PM_Q \cup K_Q$. We call the transformations in NM_Q *nearly monotonic* with respect to the usual order on integers. The next result follows from Proposition 2 and [6].

Proposition 4. *Let $n \geqslant 2$ and $\mathcal{D}_{scti}((n-1,1)) = (Q, \Sigma_{scti}, \delta_{scti}, 0, \{n-1\})$. Then*

1. *Each of the $3n - 4$ transformations of $\mathcal{D}_{scti}((n-1,1))$ of Types 1, 2, and 4 is partially monotonic, and there is one constant transformation $(Q \to 0)$. Thus DFA $\mathcal{D}_{scti}((n-1,1))$ is nearly monotonic, and hence aperiodic.*
2. *The transition semigroup NM_Q of $\mathcal{D}_{scti}((n-1,1))$ consists of all the $h(n)$ nearly monotonic transformations of Q, where*

$$h(n) = e(n) + n - 1. \tag{5}$$

3. *Each generator, other than the constant and $\mathbf{1}$, is unitary, and $3n - 3$ is the smallest number of unitary, constant and identity generators of NM_Q.*

For $n \geqslant 4$ the semigroup of all nearly monotonic transformations is larger than the semigroup of all partially monotonic transformations. Note that there are nearly monotonic semigroups that do not have semiconstant generating sets; each nearly monotonic semigroup, however, is a subsemigroup of the transition semigroup of $\mathcal{D}_{scti}((n-1,1))$.

5.2 Semiconstant Tree Semigroups

An example of a maximal semiconstant tree DFA for $n = 6$ is $\mathcal{D}_{scti}(((2,2),2))$; its transition semigroup has 1,849 elements. For $n \geqslant 4$, the maximal semiconstant tree semigroup is the largest aperiodic semigroup known.

First we define a new operation on DFAs.

Definition 3. *Let $\mathcal{A} = (Q_\mathcal{A}, \Sigma_\mathcal{A}, \delta_\mathcal{A}, q_\mathcal{A}, F_\mathcal{A})$ and $\mathcal{B} = (Q_\mathcal{B}, \Sigma_\mathcal{B}, \delta_\mathcal{B}, q_\mathcal{B}, F_\mathcal{B})$ be DFAs. Let $Q_\mathcal{C} = Q_A \cup Q_B$. The* semiconstant sum *of $\mathcal{A}$ and $\mathcal{B}$ is the DFA $\mathcal{C} = (\mathcal{A}, \mathcal{B}) = (Q_\mathcal{C}, \Sigma_\mathcal{C}, \delta_\mathcal{C}, q_\mathcal{A}, F_\mathcal{B})$. For each transition t in δ_A, we have a transition t' in δ_C such that $qt' = qt$ for $q \in Q_\mathcal{A}$ and $qt' = q$ otherwise. Dually, we have transitions defined by t in δ_B. Moreover we have a unitary transformation $(p \to q)$ for each $p \in Q_\mathcal{A}, q \in Q_\mathcal{B}$, and a constant transformation $(Q_\mathcal{C} \to q_\mathcal{A})$.*

For $m > 1$, each $\mathcal{D}_{scti}(\Delta_Q(n_1, \ldots, n_m))$ is a semiconstant sum of two smaller semiconstant tree DFAs $\mathcal{D}_{scti}(\Delta_{Q_{left}}(n_1, \ldots, n_r))$, defined by the left subtree of the root of $\Delta_Q(n_1, \ldots, n_m)$, and $\mathcal{D}_{scti}(\Delta_{Q_{right}}(n_{r+1}, \ldots, n_m))$, defined by the right subtree.

Lemma 2. *The semiconstant sum $\mathcal{C} = (\mathcal{A}, \mathcal{B})$ is minimal if and only if every state of $\mathcal{A}$ is reachable from $q_\mathcal{A}$, the states of $\mathcal{B}$ are pairwise distinguishable, and $F_\mathcal{B}$ is non-empty.*

Proof. If $\mathcal{C}$ is minimal, then every state of $\mathcal{C}$ is reachable from $q_\mathcal{A}$ in $\mathcal{C}$. Since any transformation mapping a state $q \in Q_\mathcal{B}$ to a state from $Q_\mathcal{A}$ is composed from the constant transformation $(Q_\mathcal{C} \to q_\mathcal{A})$, every state of $\mathcal{A}$ is reachable from $q_\mathcal{A}$. Now consider two distinct states $p, q \in Q_\mathcal{B}$. Since $\mathcal{C}$ is minimal, p and q are distinguishable by some word w, and no letter of w can induce the constant transformation $(Q_\mathcal{C} \to q_\mathcal{A})$. Hence every letter of w induces a transformation that acts on $Q_\mathcal{B}$ either as the identity or as some $t' \in \delta_\mathcal{B}$. If we omit the letters that act as the identity, we obtain a word w' that distinguishes p and q in $\mathcal{B}$.

Conversely, distinct states $p \in Q_\mathcal{A}$, $q \in Q_\mathcal{C} \setminus F_\mathcal{B}$ are distinguishable as follows. Apply a unitary transformation t that takes p to a state in $F_\mathcal{B}$. Since q is not changed by t, p and q are distinguishable. If $p \in Q_\mathcal{A}$ and $q \in F_\mathcal{B}$ then p and q are already distinguished (by the empty word). If $p \in Q_\mathcal{B}$ and $q \in Q_\mathcal{B}$ then they are distinguishable by assumption. Every state of $\mathcal{A}$ is reachable from $q_\mathcal{A}$ by assumption. Also, any state in $q \in Q_\mathcal{B}$ is reachable from $q_\mathcal{A}$ by a unitary transformation. Hence all the states of $\mathcal{C}$ are reachable, and $\mathcal{C}$ is minimal. $\qquad\square$

Lemma 3. *If $\mathcal{A}$ and $\mathcal{B}$ are aperiodic, then their semiconstant sum $(\mathcal{A}, \mathcal{B})$ is also aperiodic.*

Proof. Suppose that $\langle(\mathcal{A}, \mathcal{B})\rangle$ contains a cycle t. This cycle cannot include both a state from $\mathcal{A}$ and a state from $\mathcal{B}$, since the only way to map a state from $\mathcal{B}$ to a state from $\mathcal{A}$ in $(\mathcal{A}, \mathcal{B})$ is by a constant transformation, and a constant transformation cannot be used as a generator of a cycle. Hence all the cyclic states must be either in $Q_\mathcal{A}$ or $Q_\mathcal{B}$, which contradicts the assumption that $\mathcal{A}$ and $\mathcal{B}$ are aperiodic. $\qquad\square$

An DFA is *transition-complete* if it is aperiodic and adding any transition to it destroys aperiodicity.

Lemma 4. *If $\mathcal{A}$ and $\mathcal{B}$ are transition-complete, their semiconstant sum $(\mathcal{A}, \mathcal{B})$ is also transition-complete.*

Proof. We know from Lemma 3 that $(\mathcal{A}, \mathcal{B})$ is aperiodic. Suppose that a new transformation t can be added to $(\mathcal{A}, \mathcal{B})$ in such away that the resulting DFA remains aperiodic. We consider the following cases depending on the image $Q_\mathcal{B}t$.

If $|Q_\mathcal{B}t \cap Q_\mathcal{A}| = 0$ then $t = t_\mathcal{B} \circ u \circ t_\mathcal{A}$, where $t_\mathcal{A}$ and $t_\mathcal{B}$ are transformations changing only the states of $Q_\mathcal{A}$ and $Q_\mathcal{B}$, respectively, and u only maps some of the states of $Q_\mathcal{A}$ to $Q_\mathcal{B}$. If t is new, then one of $t_\mathcal{B}$, or $t_\mathcal{A}$ or u is new. But we know that no new transition can be added to $\mathcal{A}$ or $\mathcal{B}$, and we have all possible transitions of type u.

If $|Q_\mathcal{B}t \cap Q_\mathcal{A}| > 0$ and $|Q_\mathcal{C}t| = 1$, then t is a constant transformation that we have already, because we have $(Q_\mathcal{B} \to q_\mathcal{A})$, $q_\mathcal{A} \in Q_\mathcal{A}$ from the construction of semiconstant sum, and each constant transformation on $Q_\mathcal{A}$, since $\mathcal{A}$ is transition-complete.

If $|Q_\mathcal{B}t \cap Q_\mathcal{A}| > 0$ and $|Q_\mathcal{C}t| > 1$, then let $q_1 \in Q_\mathcal{B}$ be some state such that $q_1 t = p_1 \in Q_\mathcal{A}$, and let $q_2 \in Q_\mathcal{C}$ be some state such that $q_2 t = p_2$, where $q_1 \neq q_2$ and $p_2 \neq p_1$.

If $p_2 \in Q_\mathcal{B}$, let $c = (Q_\mathcal{B} \to q_1)$; since we cannot add any transformation to $\mathcal{B}$ and c is constant in $\mathcal{B}$, it must be present. Otherwise, let $c = (p_2 \to q_1)$. Note that c does not affect p_1. Similarly, if $q_2 \in Q_\mathcal{A}$, let $d = (Q_\mathcal{A} \to q_2)$; otherwise, let $d = (p_1 \to q_2)$. Note that d does not affect q_1. Then the transformation $t' = t \circ c \circ d$ is such that $q_1 t' = q_2$ and $q_2 t' = q_1$ and the DFA cannot be aperiodic.

Corollary 3. *All semiconstant tree DFAs of the form $\mathcal{D}_{scti}(\Delta_Q(n_1, \ldots, n_m))$ are transition-complete.*

Proof. This follows by induction on m. For $m = 1$ we have a bipath. For $m > 1$, $\mathcal{D}_{scti}(\Delta_Q(n_1, \ldots, n_m))$ is the semiconstant sum of $\mathcal{D}_{scti}(\Delta_Q(n_1, \ldots, n_r))$ and $\mathcal{D}_{scti}(\Delta_Q(n_{r+1}, \ldots, n_m))$. By the inductive assumption and Lemma 3 we know that $\mathcal{D}_{scti}(\Delta_Q(n_1, \ldots, n_m))$ is also aperiodic. And by Lemma 4 we know that no more transitions can be added. $\square$

In order to count the size of the semigroup of a semiconstant sum, we extend the concept of partial transformations to k-partial transformations.

Definition 4. *A k-partial transformation of Q is a transformation of Q into $Q \cup \{\square_1, \square_2, \ldots, \square_k\}$, where $\square_1, \square_2, \ldots, \square_k$ are pairwise distinct, and distinct from all $q \in Q$.*

Let $\mathcal{A} = (Q, \Sigma, \delta, s, F)$ be a DFA, and let t be a k-partial transformation of Q. We say that t is *consistent* for $\mathcal{A}$ if there exists t' in δ such that if $qt \in Q$, then $qt = qt'$ for all $q \in Q$.

The set of consistent k-partial transformations of a semigroup describes its potential for forming a large number of transformations, when used in a semiconstant sum. For a fixed $n \geqslant 6$, there exist semigroups with smaller cardinalities than the maximal ones, but with larger numbers of consistent k-partial transformations for some k. Thus k-partial transformations are useful for finding such non-maximal semigroups, as they can result in larger semigroups when used in sums.

The transition semigroup of $\mathcal{A}$ can be characterized by a function $f_\mathcal{A} : \mathbb{N} \to \mathbb{N}$ counting all consistent k-partial transformations for a given k. For example, for $k = 1$, $f_\mathcal{A}$ is the number of all consistent partial transformations for $\mathcal{A}$. For a DFA $\mathcal{A} = \mathcal{D}_{ui}(n_1, \ldots, n_m)$, $f_\mathcal{A}(1)$ is the size of the semigroup of $\mathcal{D}_{ui}(n_1, \ldots, n_m, 1)$.

From the proof of Theorem 3 we know that the number of consistent k-partial transformations for a bipath of size n having an identity transformation is

$$m_{bi}(n, k) = \binom{2n-1}{n} + \sum_{h=0}^{n-1} k^{n-h} \binom{n}{h} \binom{n+h-1}{h}.$$

Theorem 5. *Let $\mathcal{A}$ and $\mathcal{B}$ be strongly connected DFAs with n and m states, respectively. Let $f_{\mathcal{A}}(k)$ and $f_{\mathcal{B}}(k)$ be the functions counting their consistent k-partial transformations. Then the function $f_{\mathcal{C}}$ counting the consistent k-partial transformations of the semiconstant sum $\mathcal{C} = (\mathcal{A}, \mathcal{B})$ is*

$$f_{\mathcal{C}}(k) = f_{\mathcal{A}}(m + k)f_{\mathcal{B}}(k) + n(k + 1)^n((k + 1)^m - k^m).$$

Proof. Consider a transformation t in $\langle (\mathcal{A}, \mathcal{B}) \rangle$.

If $|Q_{\mathcal{B}}t \cap Q_{\mathcal{A}}| = 0$, then $t = t_{\mathcal{B}} \circ t_{\mathcal{A}}$, where $t_{\mathcal{B}}$ is a k-partial transformation of Q_B into Q_B, and t_A is a k-partial transformation of $Q_{\mathcal{A}}$ into $Q_{\mathcal{B}}$. Moreover $t_{\mathcal{B}}$ and $t_{\mathcal{A}}$ are uniquely defined by the images $Q_{\mathcal{B}}t$ and $Q_{\mathcal{A}}t$, respectively. We have $f_{\mathcal{B}}(k)$ possible t_B transformations, and $f_{\mathcal{A}}(m + k)$ possible $t_{\mathcal{A}}$ transformations, since $t_{\mathcal{A}}$ corresponds to an $(m + k)$-partial transformation of $\mathcal{A}$. So we have $f_{\mathcal{A}}(m + k)f_{\mathcal{B}}(k)$ different k-partial transformations t in this case.

If $|Q_{\mathcal{B}}t \cap Q_{\mathcal{A}}| \leqslant 1$, then the constant generator $c = (Q_{\mathcal{B}} \rightarrow q_{\mathcal{A}}), q_{\mathcal{A}} \in Q_{\mathcal{A}}$ must be used, since it is the only generator mapping a state from $Q_{\mathcal{B}}$ into a state from $Q_{\mathcal{A}}$. So the case $|Q_{\mathcal{B}}t \cap Q_{\mathcal{A}}| > 1$ is not possible. For each state $q \in Q_{\mathcal{A}}$ either qt is one of the k undefined values or $qt = q_{\mathcal{A}}$. This yields $k + 1$ possible mappings for a given x, and $(k + 1)^n$ possibilities in total. Also, for each state $q \in Q_{\mathcal{B}}$ either qt is one of the k undefined values or $qt = q_{\mathcal{A}}$. However, the latter case must occur for at least one $q \in Q_{\mathcal{B}}$. This yields $(k+1)^m - k^m$ possibilities in total. Because $\mathcal{A}$ is strongly connected, we have n possibilities for the selection of q. This yields $n(k + 1)^n((k + 1)^m - k^m)$ different k-partial transformations in this case.

Altogether, we have $f_{\mathcal{A}}(m + k)f_{\mathcal{B}}(k) + n(k + 1)^n((k + 1)^m - k^m)$. $\qquad\square$

Corollary 4. *The number of k-partial transformations of $\mathcal{D}_{scti}(\Delta_Q(n_1, \ldots, n_m))$ of size n is:*

$$f_{\mathcal{D}}(k) = \begin{cases} m_{bi}(n, k), & \text{if } m = 1; \\ f_{\mathcal{D}_{left}}(r + k)f_{\mathcal{D}_{right}}(k) + \ell(k + 1)^{\ell}((k + 1)^r - k^r), & \text{if } m > 1, \end{cases}$$

where $\mathcal{D}_{left}$ is the DFA defined by $\Delta_{Q_{left}}(n_1, \ldots, n_i)$, the left subtree of the tree $\Delta_Q(n_1, \ldots, n_m)$, $\mathcal{D}_{right}$ is defined by $\Delta_{Q_{right}}(n_{i+1}, \ldots, n_m)$, the right subtree of $\Delta_Q(n_1, \ldots, n_m)$, and ℓ, r are the numbers of states in $\mathcal{D}_{left}$ and $\mathcal{D}_{right}$, respectively.

Proof. This follows from Theorems 3 and 5. $\qquad\square$

The size of the semigroup of DFA $\mathcal{D}_{scti}(\Delta_Q(n_1, \ldots, n_m))$ is $f_{\mathcal{D}}(0)$.

Corollary 5. *Let $m_{scti}(n, k)$ be the maximal number of k-partial transformations of a semiconstant DFA $\mathcal{D}_{scti}(\Delta_Q(n_1, \ldots, n_m))$ with n states. Then*

$$m_{scti}(n, k) = \max \begin{cases} m_{bi}(n, k) \\ \max_{s=1,\ldots,n-1} \begin{cases} m_{scti}(n - s, s + k)m_{scti}(s, k) \\ + (n - s)(k + 1)^{n-s}((k + 1)^s - k^s) \end{cases} \end{cases}. \quad (6)$$

Proof. A semiconstant tree DFA is either a bipath, or a semiconstant sum of two smaller semiconstant tree DFAs. Since its number of transformations depends only on the numbers of k-partial transformations of the smaller ones, we can use the maximal ones, and select the best split for the sum.

The maximal size of semigroups of the DFAs $\mathcal{D}_{scti}$ with n states is $m_{scti}(n, 0)$.

Instead of a bipath and the value $m_{bi}(n, k)$ we could use any strongly connected automaton with an aperiodic semigroup. If such a semigroup would have a larger number of k-partial transformations than our semiconstant tree DFAs for some k, then we could obtain even larger aperiodic semigroups.

The corollary results directly in a dynamic algorithm working in $O(n^3)$ time (assuming constant time for arithmetic operations and computing binomials) for computing $m_{scti}(n, 0)$, and the distribution with the full binary tree yielding the maximal semiconstant tree semigroup.

We computed the maximal semiconstant tree semigroups up to $n = 500$. For $n = 100$, for example, one of the maximal DFAs is

$$\mathcal{D}_{scti} \quad ((((((((2, 2), (2, 2)), ((2, 2), (2, 2))), (((2, 2), (2, 2)), ((2, 2), 3))),$$
$$(((2, 2), 3), (3, 3)), ((3, 3), (3, 3)))), ((((3, 2), (3, 2)), ((3, 2), (2, 2))),$$
$$((2, 2), (2, 2)))), (((3, 3), (3, 2)), ((2, 2), 2))),$$

and its syntactic semigroup size exceeds 3.3×10^{160}.

6 Quotient Complexity of Reversal and Product

In this section we refer to quotient/state complexity simply as complexity. We settle two open problems about the complexity of reversal and concatenation of star-free languages.

6.1 Reversal

The bound $2^n - 1$ is reachable by the reverse of a star-free language [7], but it was not known if 2^n can be reached. We answer this question now.

A *nondeterministic finite automaton (NFA)* is a quintuple $\mathcal{N} = (Q, \Sigma, \delta, I, F)$, where Q, Σ, and F are as in a DFA, $\delta \colon Q \times \Sigma \to 2^Q$ is the *transition function*, and $I \subseteq Q$ is the *set of initial states*. As usual, we extend δ to functions $\delta \colon Q \times \Sigma^* \to 2^Q$, and $\delta \colon 2^Q \times \Sigma^* \to 2^Q$. The *language accepted* by an NFA $\mathcal{N}$ is $L(\mathcal{N}) = \{w \in \Sigma^* \mid \delta(I, w) \cap F \neq \emptyset\}$.

Consider a DFA $\mathcal{D} = (Q, \Sigma, \delta, 0, F)$ accepting a language L. We extend δ to a function $\delta \colon 2^Q \to 2^Q$ as usual. To construct a DFA for L^R, we first take the NFA $\mathcal{D}^R = (Q, \Sigma, \delta^R, F, \{0\})$, where $q \in \delta^R(p, a)$ if and only if $\delta(q, a) = p$ for all $p, q \in Q$, $a \in \Sigma$; here δ^R is a relation. We then determinize $\mathcal{D}^R$ by the subset construction to get the DFA $\mathcal{D}^{RD} = (2^Q, \Sigma, \delta^R, F, \{0\})$, where now δ^R is a function $\delta^R \colon 2^Q \to 2^Q$. For any $P \subseteq Q$, let $\overline{P} = Q \setminus P$.

Lemma 5. *For any $P \subseteq Q$ and $w \in \Sigma^*$, $\delta^R(\overline{P}, w) = \overline{\delta^R(P, w)}$.*

Proof. By the reversal and subset constructions, for $P, S \subseteq Q$, we have $\delta^R(S, w) = P$ if and only if $\delta(P, w^R) = S$. Thus

$$\overline{\delta^R(P, w)} = \{q \in Q \mid \delta(q, w^R) \notin P\} = \{q \in Q \mid \delta(q, w^R) \in \overline{P}\} = \delta^R(\overline{P}, w). \qquad \square$$

Theorem 6. *If $L \subseteq \Sigma^*$ is star-free, the complexity of L^R is at most $2^n - 1$.*

Proof. Let $\mathcal{D}$ be the DFA accepting L. In the DFA $\mathcal{D}^{RD}$, state $\overline{F}$ must be reachable from state F, if all 2^n states are reachable. If $\delta^R(F, w) = \overline{F}$, then by Lemma 5, $\delta^R(\overline{F}, w) = F$. Hence $\delta^R(F, ww) = F$ and $\delta^R(\overline{F}, ww) = \overline{F}$. So ww transposes F and $\overline{F}$ in $\mathcal{D}^{RD}$. Therefore $\mathcal{D}^{RD}$ is not aperiodic, and L^R and L are not star-free. $\qquad \square$

6.2   Product

The complexity of product (catenation, concatenation) of star-free languages has the same tight upper bound as the product of regular languages, with a small exception [7]. Let K and L be star-free languages with complexities m and n, respectively. If $m \geqslant 1$ and $n \geqslant 3$, the complexity of KL is $(m-1)2^n + 2^{n-1}$, which is the bound for regular languages. If $m = 1$, then either $K = \emptyset$ and the complexity of $KL = \emptyset$ is 1, or $K = \Sigma^*$. In the latter case, the complexity of $\Sigma^* L$ is 2^{n-1}, which is again the same as for regular languages [7]. If $n = 1$, then either $KL = \emptyset$, or $KL = K\Sigma^*$. In the second case the bound is m for both star-free and regular languages [4, 18].

This leaves the case of $m \geqslant 2$ and $n = 2$. Let $\mathcal{D}_K = (Q_K, \Sigma, \delta_K, q_0, F_K)$, where $Q_K = \{q_0, q_1, \ldots, q_{m-1}\}$, and let $\mathcal{D}_L = (\{0, 1\}, \Sigma, \delta_L, 0, F_L)$ be the DFAs accepting K and L, respectively. It was shown in [7] that if $F_L = \{0\}$, then $3m - 2$ is a tight upper bound on the complexity of KL; otherwise, $3m - 1$ is an upper bound. Here we prove that $3m - 2$ is also a tight upper bound if $F_L = \{1\}$, thus closing the gap.

Assume from now on that $F_L = \{1\}$. The state complexity of KL is maximized if $\mathcal{D}_K$ has only one final state [18]; without loss of generality we can assume that $F_K = \{q_{m-1}\}$. To find the DFA accepting KL we first construct an ε-NFA $\mathcal{N}$ (an NFA with empty word transitions) from $\mathcal{D}_K$ and $\mathcal{D}_L$ by adding an ε-transition from the final state q_{m-1} of $\mathcal{D}_K$ to the initial state 0 of $\mathcal{D}_L$. The set of states of $\mathcal{N}$ is $Q_K \cup \{0, 1\}$, the set of initial states is $\{q_0\}$, and the set of final states is $\{1\}$.

Next, we the use the subset construction on $\mathcal{N}$ to find the DFA $\mathcal{D}_{KL} = (Q, \Sigma, \delta, \{q_0\}, \{\{1\}\})$ accepting KL. The states of $\mathcal{D}_{KL}$ are subsets of $Q_K \cup \{0, 1\}$. The possibly reachable sets of states of $\mathcal{N}$ are the following: the $(m-1) \cdot 2^2$ sets of the form $\{q_i\} \cup S$, where $i \neq m-1$, $S \in \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$, and the two sets $\{q_{m-1}, 0\}$ and $\{q_{m-1}, 0, 1\}$, for a total of at most $4m - 2$ states.

Lemma 6. *If $F_L = \{1\}$, then for $i = 1, \ldots, m-1$, $\{q_i, 1\}$ is equivalent to $\{q_i, 0, 1\}$. Also, for any $i, j \neq m-1$ and $i \neq j$, $\{q_i, 1\}$ and $\{q_j, 1\}$ are equivalent.*

Proof. As noted in [7], $\{q_i, 1\}$ and $\{q_i, 0, 1\}$ are equivalent for all $i \neq m - 1$, because only three types of transitions are possible in $\mathcal{D}_L$: (a) the identity transition, (b) the constant transition ($\{0, 1\} \to 0$), and (c) the constant transition ($\{0, 1\} \to 1$). Thus we can keep the representative $\{q_i, 1\}$ and remove $\{q_i, 0, 1\}$. Hence there are at most $4m - 2 - (m - 1) = 3m - 1$ states.

For the second claim, assume to the contrary that $\{q_i, 1\}$ and $\{q_j, 1\}$ are distinguishable in $\mathcal{D}_{KL}$. Then there exists some $w \in \Sigma^*$ such that (without loss of generality) $\delta(\{q_i, 1\}, w)$ contains 1 (w is accepted from $\{q_i, 1\}$) and $\delta(\{q_j, 1\}, w)$ does not contain 1 (w is rejected from $\{q_j, 1\}$).

Since $\delta(\{q_j, 1\}, w)$ does not contain 1, we have $\delta_L(1, w) = 0$. Since $\delta(\{q_i, 1\}, w)$ contains 1, also $\delta(\{q_i\}, w)$ must contain 1. Since the only way to reach 1 from q_i is through 0, there are some words u and v such that $uv = w$, $\delta(\{q_i\}, u)$ contains 0 and $\delta_L(0, v) = 1$. We have two cases depending on $\delta_L(1, u)$:

1. If $\delta_L(1, u) = 0$, then $\delta_L(1, uv) = 1$, contradicting that $\delta_L(1, w) = 0$.
2. If $\delta_L(1, u) = 1$, then $\delta_L(1, v) = 0$ (because $\delta_L(1, w) = 0$). But we know that $\delta_L(0, v) = 1$; so v induces the cycle $(0, 1)$ and L is not aperiodic.

Thus all $m - 1$ states of the form $\{q_i, 1\}$ can be represented by one state, say $\{q_0, 1\}$, reducing the possible number of indistinguishable states of $\mathcal{D}_{KL}$ to $3m - 1 - (m - 2) = 2m + 1$. Therefore in the case where $F_L = \{1\}$, the state complexity of KL is at most $2m + 1$, which is smaller than $3m - 2$. $\qquad\square$

As a consequence of the lemma, the result of [7] can be strengthened as follows:

Theorem 7. *Let K and L be star-free languages with complexities $m \geqslant 2$ and 2, respectively; then the complexity of KL is $3m - 2$.*

7 Conclusions

We have found two new types of aperiodic semigroups. Maximal semiconstant semigroups of type $\mathcal{D}_{scti}(\Delta_Q(n_1, \ldots, n_m))$ are currently the largest aperiodic semigroups known. A tight upper bound on the size of aperiodic semigroups remains unknown.

References

1. Brzozowski, J.: Quotient complexity of regular languages. J. Autom. Lang. Comb. 15(1/2), 71–89 (2010)
2. Brzozowski, J.: In search of the most complex regular languages. Internat. J. Found. Comput. Sci. 24(6), 691–708 (2013)
3. Brzozowski, J., Fich, F.E.: Languages of $\mathcal{R}$-trivial monoids. J. Comput. System Sci. 20(1), 32–49 (1980)
4. Brzozowski, J., Jirásková, G., Li, B.: Quotient complexity of ideal languages. Theoret. Comput. Sci. 470, 36–52 (2013)
5. Brzozowski, J., Li, B.: Syntactic complexity of $\mathcal{R}$- and $\mathcal{J}$-trivial languages. In: Jürgensen, H., Reis, R. (eds.) DCFS 2013. LNCS, vol. 8031, pp. 160–171. Springer (2013)

6. Brzozowski, J., Li, B., Liu, D.: Syntactic complexities of six classes of star-free languages. J. Autom. Lang. Comb. 17(2–4), 83–105 (2012)
7. Brzozowski, J., Liu, B.: Quotient complexity of star-free languages. Internat. J. Found. Comput. Sci. 23(6), 1261–1276 (2012)
8. Diestel, R.: Graph Theory, Graduate Texts in Mathematics, vol. 173. Springer-Verlag, Heldelberg, fourth edn. (2010), http://diestel-graph-theory.com
9. Ginzburg, A.: Abour some properties of definite, reverse definite and related automata. IEEE Trans. Electronic Comput. EC–15, 806–810 (1966)
10. Gomes, G., Howie, J.: On the ranks of certain semigroups of order-preserving transformations. Semigroup Forum 45, 272–282 (1992)
11. Howie, J.M.: Products of idempotents in certain semigroups of transformations. Proc. Edinburgh Math. Soc. 17(2), 223–236 (1971)
12. Iván, S., Nagy-György, J.: On nonpermutational transformation semigroups with an application to syntactic complexity (2014), http://arxiv.org/abs/1402.7289
13. Kisielewicz, A., Szykuła, M.: Generating small automata and the Černý conjecture. In: Konstantinidis, S. (ed.) CIAA 2013. LNCS, vol. 7982, pp. 340–348. Springer (2013)
14. McNaughton, R., Papert, S.A.: Counter-Free Automata, MIT Research Monographs, vol. 65. The MIT Press (1971)
15. Pin, J.E.: Syntactic semigroups. In: Handbook of Formal Languages, vol. 1: Word, Language, Grammar, pp. 679–746. Springer, New York, NY, USA (1997)
16. Schützenberger, M.: On finite monoids having only trivial subgroups. Inform. and Control 8, 190–194 (1965)
17. Yu, S.: State complexity of regular languages. J. Autom. Lang. Comb. 6, 221–234 (2001)
18. Yu, S., Zhuang, Q., Salomaa, K.: The state complexities of some basic operations on regular languages. Theoret. Comput. Sci. 125, 315–328 (1994)