Large Aperiodic Semigroups*

Janusz Brzozowski[1] and Marek Szykuła[2]

[1] David R. Cheriton School of Computer Science, University of Waterloo
Waterloo, ON, N2L 3G1, Canada
brzozo@uwaterloo.ca

[2] Institute of Computer Science, University of Wrocław
Joliot-Curie 15, 50-383 Wrocław, Poland
msz@cs.uni.wroc.pl

Abstract. 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 first introduce *unitary* semigroups generated by transformations that change only one state. 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.

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 [14]. 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 [1,14] 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 [5], 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 with two small exceptions.

* This work was supported by the Natural Sciences and Engineering Research Council of Canada grant No. OGP000087 and by Polish NCN grant DEC-2013/09/N/ST6/01194.

M. Holzer and M. Kutrib (Eds.): CIAA 2014, LNCS 8587, pp. 124–135, 2014.

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—in particular, the *syntactic complexity* of a regular language, which is the cardinality of its syntactic semigroup [12]—may also be useful [2]. Syntactic complexity 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 *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 [13] 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. Star-free languages and the DFAs that accept them were studied by McNaughton and Papert in 1971 [11].

Two aperiodic semigroups, monotonic and partially monotonic, were studied by Gomes and Howie [8]. Their results were adapted to finite automata in [4], 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 [3]. 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 [10], 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.
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 $n = 1,000$. For $n \geqslant 4$ the maximal unitary semigroups are larger than any previously known aperiodic semigroup.
3. For each n we found a set of DFAs whose inputs induce *semiconstant tree* transformations that send a non-empty subset of 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 $n = 500$.
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.

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. The classes are listed in the order of increasing size when n is large.

There are two more classes of syntactic semigroups that have the same complexity as the semigroups of finite languages [4]: those of cofinite and reverse definite languages. The lower bound for definite languages ([4]) is the same as the tight upper bound for $\mathcal{J}$-trivial languages ([3]), but it is not known whether this is also an upper bound for definite languages.

Omitted proofs can be found in [6].

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 $\lfloor e(n-1)! \rfloor$	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	?	?	?	?	?

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 $Q = \{0, 1, \dots, n-1\}$. A *deterministic finite automaton (DFA)* is a quintuple $\mathcal{D} = (Q, \Sigma, \delta, 0, F)$, where 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 has 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 $t = [p_0, \dots, p_{n-1}]$ 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 write $t_1 t_2$ for $t_1 \circ t_2$.

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 $q \in Q$. A *permutation* of Q is a mapping of Q *onto* itself. For $k \geqslant 2$, a transformation (permutation) t of a set $P = \{q_0, q_1, \dots, q_{k-1}\} \subseteq Q$ is a k*-cycle* if $q_0 t = q_1, q_1 t = q_2, \dots, q_{k-2} t = q_{k-1}, q_{k-1} t = q_0$. A k-cycle is denoted by $(q_0, q_1, \dots, q_{k-1})$. 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 transformation is *aperiodic* if it contains no cycles. A transformation semigroup is aperiodic if it contains only aperiodic transformations.

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 $\mathcal{D}$, a subsemigroup of $\mathcal{T}_Q$. A DFA is *aperiodic* if its transition semigroup is aperiodic. If $\mathcal{D}$ is minimal, its transition semigroup is isomorphic to the *syntactic semigroup* of the language $L(\mathcal{D})$ [11,12]. 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*. We deal only with transition semigroups and 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 $P = \{p\}$. 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 $m, n_1, n_2, \dots, n_m$ be positive natural numbers. Also, let $n = n_1 + \dots + n_m$, and for each i, $1 \leqslant i \leqslant m$, define r_i by $r_i = \sum_{j=1}^{i-1} n_j$. For $i = 1, \dots, m$, let $Q_i = \{r_i, r_i + 1, \dots, r_{i+1} - 1\}$; thus the cardinality of Q_i is n_i. Let $Q = Q_1 \cup \dots \cup Q_m = \{0, \dots, n-1\}$; the cardinality of Q is n. The sequence $(n_1, n_2, \dots, n_m)$ is called the *distribution* of Q.

A binary tree is *full* if every vertex has either two children or no children. Let Δ_Q be a full binary tree with m leaves labeled $Q_1, \dots, Q_m$ 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 $\Delta_Q(n_1, n_2, \dots, n_m)$ and is called the *structure* of Q. This structure will uniquely determine the transition function δ of the DFAs defined below.

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 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* $(n_1, n_2, \dots, n_m)$ *is a distribution of* Q. *For all* $i = 1, \dots, m$ *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* $(n_1, n_2, \dots, n_m)$ *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* $\Delta_Q(n_1, n_2, \dots, n_m)$ *is a structure of* Q. *For each internal node* w *the semiconstant transformation* $(\mathrm{Q}(w) \to \min(\mathrm{Q}(w)))$ *is of Type 3.*

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

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* **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* **1** *added.*

Following [7], 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 $k = 1$, $(\{v_0\}, \emptyset)$ is 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.

Remark 1. All four DFAs of Definition 2 are minimal as is easily verified.

4 Unitary Semigroups

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

Monotonic Semigroups [4,8,9]

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 $pt \leqslant qt$. A DFA is *monotonic* if each of its generators is monotonic. A semigroup is *monotonic* if it has a set of monotonic generators. We assume that $\leqslant$ is the usual order on integers.

The following result of [8] 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* **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.*

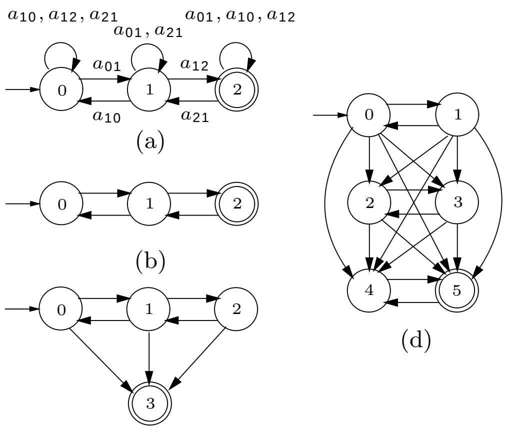

Fig. 1. Unitary DFAs: (a) $\mathcal{D}_u(3)$; (b) $\mathcal{D}_u(3)$ simplified; (c) $\mathcal{D}_u(3,1)$; (d) $\mathcal{D}_u(2,2,2)$

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 $n = 3$ [4].

Partially Monotonic Semigroups [4,8]

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 $qt = \Box$. By convention, $\Box t = \Box$. The *domain* of t is the set $dom(t) = \{q \in Q \mid qt \neq \Box\}$. 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 $pt \leqslant qt$.

We start with all partial transformations of $Q \setminus \{n-1\}$ and add state $(n-1)$ for the undefined value $\Box$. The resulting transformations are *partially monotonic.* The next result follows from [8]:

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

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 $PM_Q \setminus \{\mathbf{1}\}$.

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

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.

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 [13], 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. □

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 $\mathcal{D}_u(n_1, \dots, n_m)$. Otherwise we can add more unitary transformations of Type 2 and obtain a larger semigroup. □

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

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

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

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 $\mathcal{D}_{ui}(n_1, \dots, n_m)$ is maximal, then $\mathcal{D}_{ui}(n_2, \dots, n_m)$ 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* $\mathcal{D}_{ui}(n_1, \dots, n_m)$ *with* n *states. If we define* $m_{ui}(0) = 1$*, then for* $n > 0$

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

This leads directly to a dynamic algorithm taking $O(n^3)$ time for computing $m_{ui}(n)$ and the distributions $(n_1, \dots, n_m)$ 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. 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}.

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 even* n *the size of the maximal unitary semigroup is at least*

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

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

5 Semiconstant Semigroups

Nearly Monotonic Semigroups [4]

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

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.

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, where $Q_\mathcal{A} \cap Q_\mathcal{B} = \emptyset$, and $\Sigma_\mathcal{A} \cap \Sigma_\mathcal{B} = \emptyset$. The* semiconstant sum *of $\mathcal{A}$ and $\mathcal{B}$ is denoted by $\mathcal{C} = (\mathcal{A}, \mathcal{B})$ and is the DFA $(Q_\mathcal{C}, \Sigma_\mathcal{C}, \delta_\mathcal{C}, q_\mathcal{A}, F_\mathcal{B})$, where $Q_\mathcal{C} = Q_A \cup Q_B$. 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 $(Q_\mathcal{C} \to q_\mathcal{A})$.*

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.*

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 3. *If $\mathcal{A}$ and $\mathcal{B}$ are aperiodic, so is their semiconstant sum.*

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. □

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, so is their semiconstant sum.*

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

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* $Q \cup \{\Box_1, \Box_2, \dots, \Box_k\}$, *where* $\Box_1, \Box_2, \dots, \Box_k$ *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 compositions.

The transition semigroup of $\mathcal{A}$ can be characterized by a function $f_{\mathcal{A}} \colon \mathbb{N} \to \mathbb{N}$ 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 $\mathcal{A} = \mathcal{D}_{ui}(n_1, \dots, n_m)$, $f_{\mathcal{A}}(1)$ is the size of the semigroup of $\mathcal{D}_{ui}(n_1, \dots, n_m, 1)$.

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

Corollary 4. *The number of* k*-partial transformations of* $\mathcal{D}_{scti}(\Delta_Q(n_1, \dots, n_m))$ *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* $\Delta_{Q_{left}}(n_1, \dots, n_i)$, *the left subtree of the tree* $\Delta_Q(n_1, \dots, n_m)$, $\mathcal{D}_{right}$ *is defined by* $\Delta_{Q_{right}}(n_{i+1}, \dots, n_m)$, *the right subtree of* $\Delta_Q(n_1, \dots, n_m)$, *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. □

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

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

$$m_{scti}(n,k) = \max \begin{cases} m_{bi}(n,k) \\ \max\limits_{s=1,\dots,n-1} \left\{ \begin{array}{l} m_{scti}(n-s, s+k) m_{scti}(s,k) \\ + (n-s)(k+1)^{n-s}((k+1)^s - k^s) \end{array} \right\} \end{cases}. \quad (3)$$

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

$$\begin{aligned}\mathcal{D}_{scti}\;\; &((((((((2,2),(2,2)),((2,2),(2,2))),(((2,2),(2,2)),((2,2),3))),\\ &((((2,2),3),(3,3)),((3,3),(3,3)))),((((3,2),(3,2)),((3,2),(2,2))),\\ &((2,2),(2,2)))),(((3,3),(3,2)),((2,2),2))),\end{aligned}$$

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

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., Li, B.: Syntactic complexity of $\mathcal{R}$- and $\mathcal{J}$-trivial languages. In: Jurgensen, H., Reis, R. (eds.) DCFS 2013. LNCS, vol. 8031, pp. 160–171. Springer, Heidelberg (2013)
4. 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)
5. Brzozowski, J., Liu, B.: Quotient complexity of star-free languages. Internat. J. Found. Comput. Sci. 23(6), 1261–1276 (2012)
6. Brzozowski, J., Szykuła, M.: Large aperiodic semigroups (2014), `http://arxiv.org/abs/1401.0157`
7. Diestel, R.: Graph Theory, Graduate Texts in Mathematics, 4th edn., vol. 173. Springer, Heidelberg (2010), `http://diestel-graph-theory.com`
8. Gomes, G., Howie, J.: On the ranks of certain semigroups of order-preserving transformations. Semigroup Forum 45, 272–282 (1992)
9. Howie, J.M.: Products of idempotents in certain semigroups of transformations. Proc. Edinburgh Math. Soc. 17(2), 223–236 (1971)
10. Kisielewicz, A., Szykuła, M.: Generating small automata and the Černý conjecture. In: Konstantinidis, S. (ed.) CIAA 2013. LNCS, vol. 7982, pp. 340–348. Springer, Heidelberg (2013)
11. McNaughton, R., Papert, S.A.: Counter-Free Automata, MIT Research Monographs, vol. 65. MIT Press (1971)
12. Pin, J.E.: Syntactic semigroups. In: Handbook of Formal Languages. Word, Language, Grammar, vol. 1, pp. 679–746. Springer, New York (1997)
13. Schützenberger, M.: On finite monoids having only trivial subgroups. Inform. and Control 8, 190–194 (1965)
14. Yu, S.: State complexity of regular languages. J. Autom. Lang. Comb. 6, 221–234 (2001)