On Deterministic Finite Automata and Syntactic Monoid Size

Markus Holzer and Barbara König

Institut für Informatik, Technische Universität München,
Arcisstraße 21, D-80290 München, Germany
email: {holzer,koenigb}@informatik.tu-muenchen.de

Abstract. We investigate the relationship between regular languages and syntactic monoid size. In particular, we consider the transformation monoids of n-state (minimal) deterministic finite automata. We show tight upper bounds on the syntactic monoid size, proving that an n-state deterministic finite automaton with singleton input alphabet (input alphabet with at least three letters, respectively) induces a linear (n^n, respectively) size syntactic monoid. In the case of two letter input alphabet, we can show a lower bound of $n^n - \binom{n}{\ell}\ell! n^k - \binom{n}{\ell} k^k \ell^\ell$, for some natural numbers k and ℓ close to $\frac{n}{2}$, for the size of the syntactic monoid of a language accepted by an n-state deterministic finite automaton. This induces a family of deterministic finite automata such that the fraction of the size of the induced syntactic monoid and n^n tends to 1 as n goes to infinity.

1 Introduction

Regular languages and their implementations have received more and more attention in recent years due to the many new applications of finite automata and regular expressions in object-oriented modeling, programming languages and other practical areas of computer science. In recent years, quite a few software systems for manipulating formal language objects, with an emphasis on regular-language objects, have been developed. Examples include AMoRE, Automata, FIRE Engine, FSA, Grail, and INTEX [1, 10]. These applications and implementations of regular languages motivate the study of descriptive complexity of regular languages. A very well accepted and studied measure of descriptional complexity for regular languages is the size, i.e., number of states, of deterministic finite automata.

Besides machine oriented characterization of regular languages, they also obey several algebraic characterizations. It is a consequence of Kleene's theorem [3], that a language $L \subseteq \Sigma^*$ is regular if and only if there exists a finite monoid M, a morphism $\varphi : \Sigma^* \to M$, and a finite subset $N \subseteq M$ such that $L = \varphi^{-1}(N)$. The monoid M is said to recognize L. The syntactic monoid of L is the smallest monoid recognizing the language under consideration. It is uniquely defined up to isomorphism and is induced by the syntactic congruence $\sim_L$ defined over Σ^* by $v_1 \sim_L v_2$ if and only if for every $u, w \in \Sigma^*$ we have

$uv_1w \in L \iff uv_2w \in L$. The syntactic monoid of L is the quotient monoid $M(L) = \Sigma^*/\sim_L$. In this paper we propose the size of the syntactic monoid as a natural measure of descriptive complexity for regular languages and study the relationship between automata and monoid size in more detail.

In most cases, we show tight upper bounds on the syntactic monoid, proving that there are languages accepted by n-state deterministic finite automata whose syntactic monoid has a certain size. It is easy to see that for unary regular languages the size is linear, while that for regular languages over an input alphabet with at least three letters is maximal, i.e., n^n. The challenging part is to determine the size of the syntactic monoid for regular languages over a binary alphabet. The trivial lower and upper bounds are $n!$—induced by the two generators of S_n—and $n^n - n! + g(n)$, respectively, where $g(n)$ denotes Landau's function [4–6], which equals the maximal order of all permutations in S_n. Compared to the trivial lower bound, where $\lim_{n\to\infty} \frac{n!}{n^n} = 0$, we can do much better, since we present binary regular languages whose syntactic monoid is at least $n^n - \binom{n}{\ell}\ell!n^k - \binom{n}{\ell}k^k\ell^\ell$, for some natural numbers k and ℓ close to $\frac{n}{2}$, and the fraction of this number (for appropriate k and ℓ) and n^n tends to 1 as n goes to infinity.

The paper is organized as follows. In the next section we introduce the necessary notations. Then in Section 3 we prove the easy cases on syntactic monoid size and devote Section 4 to the study of binary regular languages. Finally, we summarize our results and state some open problems.

2 Definitions

We assume the reader to be familiar with the basic notions of formal language theory and semigroup theory, as contained in [2] and [8]. In this paper we are dealing with regular languages and their syntactic monoid. A *semigroup* is a nonempty set S equipped with an associative binary operation, i.e., $(\alpha\beta)\gamma = \alpha(\beta\gamma)$ for all $\alpha, \beta, \gamma \in S$. The semigroup S is called a *monoid* if it contains an identity element *id*. If E is a set, then we denote by $T(E)$ the monoid of functions from E into E together with the composition of functions. We read composition from left to right, i.e., first α, then β. Because of this convention, it is natural to write the argument i of a function to the left: $(i)\alpha\beta = ((i)\alpha)\beta$. The image of a function α in $T(E)$ is defined as $img(\alpha) = \{\, (i)\alpha \mid i \in E \,\}$ and the kernel of α is the equivalence relation $\equiv$, which is induced by $i \equiv j$ if and only if $(i)\alpha = (j)\alpha$. In particular, if $E = \{1, \ldots, n\}$, we simply write T_n for the monoid $T(E)$. The monoid of all permutations over n elements is denoted by S_n and trivially is a sub-monoid of T_n.

A deterministic finite automaton is a 5-tuple $A = (Q, \Sigma, \delta, q_0, F)$, where Q is the finite set of states, Σ is a finite alphabet, $\delta : Q \times \Sigma \to Q$ denotes the transition function, $q_0 \in Q$ is the initial state, and $F \subseteq Q$ is the set of final states. Observe, that a deterministic finite automaton is complete by definition. As usual, δ is extended to act on $Q \times \Sigma^*$ by $\delta(q, \lambda) = q$ and $\delta(q, aw) = \delta(\delta(q, a), w)$ for $q \in Q$, $a \in \Sigma$, and $w \in \Sigma^*$, where λ denotes the empty word of length zero. Unless

otherwise stated, we assume that $Q = \{1, \ldots, n\}$ for some $n \in \mathbb{N}$. The language accepted by the deterministic finite automaton A is defined as

$$L(A) = \{\, w \in \Sigma^* \mid \delta(q_0, w) \in F \,\}.$$

The family of regular languages is the set of all languages which are accepted by some deterministic finite automaton.

In order to compute the syntactic monoid of a language it is convenient to consider the transition monoid induced by a finite automaton. Let $A = (Q, \Sigma, \delta, q_0, F)$ be a deterministic finite automaton. Naturally, each word $w \in \Sigma^*$ defines a function from Q into Q. The monoid generated by all these functions thus defined, where w varies over Σ^*, is a sub-monoid of $T(Q)$; it is the transition monoid $M(A)$ of the automaton A. Clearly, $M(A)$ is generated by the functions defined by the letters of the alphabet and we have a canonical morphism $\Sigma^* \to M(A)$. The intrinsic relationship between the transition monoid $M(A)$ and the syntactic monoid of the language $L(A)$ is as follows: The transition monoid of the minimal deterministic finite automata is isomorphic to $M(L)$. This allows the computation of $M(L)$ in a convenient way.

3 Syntactic Semigroup Size—The Easy Cases

We start our investigation on syntactic monoid size with two easy cases, which mostly follow from results from the literature. We state these results for completeness only. Firstly, we consider unary regular languages, where we can profit from the following result on monogenic (sub)semigroups, which can be found in [2].

Theorem 1. *Let α be an element of a semigroup S. Then either all powers of α are distinct and the monogenic sub-semigroup $\langle \alpha \rangle := \{\, \alpha^i \mid i \geq 1 \,\}$ of S is isomorphic to the semigroup $(\mathbb{N}, +)$ of the natural numbers under addition, or there exists positive integers m and r such that $\alpha^m = \alpha^{m+r}$ and $\langle \alpha \rangle = \{\alpha, \alpha^2, \ldots, \alpha^{m+r-1}\}$. Here m is called the index and r the period of α.*

Then we can estimate the syntactic monoid size of regular languages over a unary input alphabet as follows:

Theorem 2. *Let A be an n-state deterministic finite automaton with a unary input alphabet. Then a monoid of size n is sufficient and necessary in the worst case to recognize the language $L(A)$.*

Proof. Observe, that the transition graph of a deterministic finite automaton A with unary input alphabet consists of a path, which starts from the initial state, followed by a cycle of one or more states. Assume that m is the number of states of the path starting from the initial state, and r the number of states in the cycle. Then $n = m + r$ and A, by appropriately numbering the states, induces the mapping

$$\alpha = \begin{pmatrix} 1 & 2 & \ldots & m & m+1 & \ldots & m+r-1 & m+r \\ 2 & 3 & \ldots & m+1 & m+2 & \ldots & m+r & m+1 \end{pmatrix}$$

of the semigroup T_n. It is a routine matter to verify that α has index m and period r. Hence by Theorem 1 the semigroup generated by α equals the $n-1$ element set $\{\alpha, \alpha^2, \ldots, \alpha^{m+r-1}\}$. This shows the upper bound n on the monoid size, since the neutral element has to be taken into consideration, too. On the other hand, if A was chosen to be a minimal deterministic finite automaton then the induced transformation monoid equals $\{id\} \cup \{\alpha, \alpha^2, \ldots, \alpha^{m+r-1}\}$ by our previous investigation. Therefore, n is also a lower bound for the maximal syntactic monoid size. □

In the remainder of this section we consider regular languages over an input alphabet with at least three letters. Obviously, for all n, the elements

$$\alpha = \begin{pmatrix} 1 & 2 & \ldots & n-1 & n \\ 2 & 3 & \ldots & n & 1 \end{pmatrix}, \quad \beta = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ 2 & 1 & 3 & \ldots & n \end{pmatrix}, \quad \text{and} \quad \gamma = \begin{pmatrix} 1 & 2 & \ldots & n-1 & n \\ 1 & 2 & \ldots & n-1 & 1 \end{pmatrix}$$

of T_n form a complete basis of T_n, i.e., they generate all of the monoid T_n. In particular, if $n = 2$ we find that $\alpha = \beta$, and thus two elements suffice for the generation of T_2, while for $n = 1$ trivially one element is enough to generate all of T_1—here $\alpha = \beta = \gamma$ holds. Thus we have shown the following theorem:

Theorem 3. *Let A be an n-state deterministic finite automaton with input alphabet Σ. Then a monoid of size n^n is sufficient and necessary in the worst case to recognize the language $L(A)$ if either (i) $n = 1$, or (ii) $n = 2$ and $|\Sigma| \geq 2$, or (iii) $n \geq 3$ and $|\Sigma| \geq 3$.*

Proof. The upper bound n^n is trivial. From the above given generators α, β, and γ we define the deterministic finite automata $A = (\{Q, \{a, b, c\}, \delta, 1, F)$, where $Q = \{1, \ldots, n\}$, $F = \{n\}$ and $\delta(i, a) = (i)\alpha$, $\delta(i, b) = (i)\beta$, and $\delta(i, c) = (i)\gamma$. It remains to prove that A is minimal. In order to show this, it is sufficient to verify that all states of A are reachable and lie in different equivalence classes. The reachability claim is easy to see, since for every state $i \in Q$ we have $\delta(1, a^{i-1}) = i$ and the latter claim follows since for $i, j \in Q$ with $i < j$ we find $\delta(i, a^{n-j}) = i + (n-j) \notin F$, since $i + (n-j) < n$, and $\delta(j, a^{n-j}) = n \in F$. Thus, i and j are not in the same equivalence class. □

The question arises, whether the above given theorem can be improved with respect to the alphabet size. By easy calculations one observes, that for $n = 2$ this is not the case, since a unary language will only induce a syntactic monoid of size 2, due to Theorem 2. For $n \geq 3$ the following completeness theorem for unary functions given in [9], shows that an improvement is also not possible. The completeness result reads as follows.

Theorem 4. *Assume $n \geq 3$. Then three elements of T_n generate all functions of T_n if and only if two of them generate the symmetric group S_n and the third has kernel size $n-1$. Moreover, no less than three elements generate all functions from T_n.*

Thus, it remains to classify the syntactic monoid size of binary languages in general, which is done in the remaining part of the paper.

4 Syntactic Semigroup Size—A More Complicated Case

In this section we consider binary languages and the size of their syntactic monoid in more detail. Compared to the previous section here we are only able to prove a trivial upper and a non-matching lower bound on the syntactic monoid size for languages accepted by n-state deterministic finite automata.

The outline of this section is as follows: First we define a subset of T_n by some easy properties, verify that it is a semigroup and that it is generated by two generators only. Then, we argue that there is a minimal deterministic finite automaton, the transition monoid of which equals the defined semigroup and finally, we determine a lower bound of the semigroup size. The advantage of the explicit definition of the semigroup is that we don't have to go into some tedious analysis of the Green's relations if the semigroup would be given by generators only. The subset of T_n we are interested in, is defined as follows:

Definition 1. *Let $n \geq 2$ such that $n = k + \ell$ for some natural numbers k and ℓ. Furthermore, let $\alpha = (1\,2\,\ldots\,k)(k{+}1\,k{+}2\,\ldots\,n)$ be a permutation of S_n consisting of two cycles. We define $U_{k,\ell}$ as a subset of T_n as follows: A transformation γ is an element of $U_{k,\ell}$ if and only if*

1. *there exists a natural number $m \in \mathbb{N}$ such that $\gamma = \alpha^m$* or
2. *the transformation γ satisfies that*
   (a) *there exist $i \in \{1, \ldots, k\}$ and $j \in \{k+1, \ldots, n\}$ such that $(i)\gamma = (j)\gamma$* and
   (b) *there exists $h \in \{k+1, \ldots, n\}$ such that $h \notin img(\gamma)$.*

The intuition behind choosing this specific semigroup $U_{k,\ell}$ is the following: We intend to generate it with two transformations, one being the permutation α, the other a non-bijective transformation β. Since β is non-bijective there are at least two indices i, j such that $(i)\beta = (j)\beta$. By applying a multiple of α before applying β the number of index pairs which may be mapped to the same image can be increased. If the permutation is one cycle of the form $(1\,2\,\ldots\,n)$ the number of pairs is only n, whereas in the case of the α above which consists of two cycles whose lengths do not have a non-trivial common divisor, there are $k\ell$ possible pairs to choose from. And if k and ℓ are chosen close to $\frac{n}{2}$, then $k\ell > n$. Next we have to show that $U_{k,\ell}$ is indeed a semigroup.

Lemma 1. *The set $U_{k,\ell}$ is closed under composition and is therefore a (transformation) semigroup.*

Proof. Let $\gamma_1, \gamma_2 \in U_{k,\ell}$ be two transformations. We show that $\gamma_1\gamma_2$ is also an element of $U_{k,\ell}$. We have to distinguish the following four cases:

1. The transformation γ_1 is of the form α^{m_1} and the transformation γ_2 is of the form α^{m_2} for some $m_1, m_2 \geq 1$. Then clearly $\gamma_1\gamma_2 = \alpha^{m_1+m_2}$ is an element of $U_{k,\ell}$.

2. Let $\gamma_1 = \alpha^m$, for some $m \geq 1$, and γ_2 satisfies the second condition of Definition 1, i.e., there are indices $i \in \{1, \ldots, k\}$ and $h, j \in \{k+1, \ldots, k+\ell\}$ such that $(i)\gamma_2 = (j)\gamma_2$ and $h \notin img(\gamma_2)$.
   The element h also fails to be a member of $img(\gamma_1\gamma_2)$. Furthermore, because of the nature of α it holds that $i' = (i)\gamma_1^{-1} \in \{1, \ldots, k\}$ and $j' = (j)\gamma_1^{-1} \in \{k+1, \ldots, k+\ell\}$. And it holds that $(i')\gamma_1\gamma_2 = (i)\gamma_2 = (j)\gamma_2 = (j')\gamma_1\gamma_2$. Therefore $\gamma_1\gamma_2$ satisfies also the second condition of Definition 1.
3. Assume that $\gamma_2 = \alpha^m$, for some $m \geq 1$, and γ_1 satisfies the second condition of Definition 1, i.e., there are indices $i \in \{1, \ldots, k\}$ and $h, j \in \{k+1, \ldots, k+\ell\}$ such that $(i)\gamma_1 = (j)\gamma_1$ and $h \notin img(\gamma_1)$.
   It obviously holds that $(i)\gamma_1\gamma_2 = (j)\gamma_1\gamma_2$. And since $\gamma_2 = \alpha^m$ and the permutation α maps elements of its second cycle only to other elements of the second cycle, it holds that $h' = (h)\gamma_2 \notin img(\gamma_1\gamma_2)$, since otherwise $h = (h')\gamma_2^{-1}$ would be in the image of γ_1 which is a contradiction.
4. Finally, let γ_1 and γ_2 both satisfy the second condition of Definition 1. Then there are indices $i_1, i_2, \in \{1, \ldots, k\}$ and $h_1, h_2, j_1, j_2 \in \{k+1, \ldots, k+\ell\}$ such that $(i_r)\gamma_r = (j_r)\gamma_r$ and $h_r \notin img(\gamma_r)$ for $1 \leq r \leq 2$.
   By setting $i = i_1$, $j = j_1$, and $h = h_2$, it is easy to see that $\gamma_1\gamma_2$ satisfies also the second part of Definition 1. □

Before we can prove that $U_{k,\ell}$ is generated by two elements of $T_{k+\ell}$ we need some result, which constitutes how to find a complete basis for the symmetric group S_n. The below given result was shown in [7].

Theorem 5. *Given a non-identical element α in S_n, then there exists β such both generate the symmetric group S_n, provided that it is not the case that $n = 4$ and α is one of the three permutations $(1\,2)(3\,4)$, $(1\,3)(2\,4)$, and $(1\,4)(2\,3)$.*

Now we are ready for the proof that two elements are enough to generate all of $U_{k,\ell}$, provided that k and ℓ obey some nice properties.

Theorem 6. *Let $k, \ell \in \mathbb{N}$ be two natural numbers with $k < \ell$ and $\gcd\{k, \ell\} = 1$, and set $n = k+\ell$. The semigroup $U_{k,\ell}$ can be generated with two elements of T_n, where one element is the permutation $\alpha = (1\,2\,\ldots\,k)(k+1\,k+2\,\ldots n)$ and the other is an element β of kernel size $n-1$.*

Proof. The first generator of $U_{k,\ell}$ is the permutation α of Definition 1. Now set $\pi_1 = (1\ 2\ \ldots\ k)$, which will be considered as a permutation in S_{n-1}. Since π_1 is not the identity and not an element of the listed exceptions, then according to Theorem 5, there exists a permutation π_2 such that π_1 and π_2 generate S_{n-1}. Now define the second generator β of $U_{k,\ell}$ as follows: Let $(i)\beta = (i)\pi_2$ whenever $1 \leq i \leq n-1$ and $(n)\beta = (1)\pi_2$. Hence β has kernel size $(k+\ell)-1 = n-1$.

We will first show that α and β generate at most the transformations specified in Definition 1. Let γ therefore be an element generated by α and β. If no β was used in the generation of γ, then $\gamma = \alpha^m$, for some natural number m. Otherwise $\gamma = \alpha^m\beta\gamma'$ for some natural number m (possibly $m = 0$) and some transformation γ'. By definition $(1)\beta = (n)\beta$. We set $i = (1)\alpha^{-m}$ and $j =$

$(n)\alpha^{-m}$. Since the element 1 is located in the first cycle of α and the element n is located in the second cycle of α it follows that $i \in \{1,\ldots,k\}$ and $j \in \{k+1,\ldots,n\}$. Furthermore, $(i)\gamma = (i)\alpha^m\beta\gamma' = (1)\beta\gamma' = (n)\beta\gamma' = (j)\alpha^m\beta\gamma = (j)\gamma$. On the other hand γ can be written as $\gamma = \gamma''\beta\alpha^r$, for some $r \geq 0$. Since n is not in the image of β, the same is true for the image of $\gamma''\beta$. This implies that $h = (n)\alpha^r$ is not in the image of γ and since n is an element of the second cycle of α, this implies $h \in \{k+1,\ldots,n\}$.

Conversely, we show that α and β generate at least the transformations specified in Definition 1. Clearly transformations of the form $\gamma = \alpha^m$, for some $m \geq 1$, can be generated easily. Now let γ be a transformation such that $(i)\gamma = (j)\gamma$ and $h \notin img(\gamma)$ for $i \in \{1,\ldots,k\}$ and $h, j \in \{k+1,\ldots,n\}$. Since k and ℓ do not have a common divisor, the cycles of α can be "turned" independently and therefore there exists a natural number $r \in \{1,\ldots,k\ell\}$ such that $(i)\alpha^r = 1$ and $(j)\alpha^r = n$. And there exists a number p such that $\alpha^p = (1\,2\,\ldots\,k)$. Furthermore there exists a number s such that $(n)\alpha^s = h$.

We are now looking for a transformation γ' such that $\gamma = \alpha^r\beta\gamma'\alpha^s$ and γ' can be generated from α and β. This condition can be rewritten to $\gamma\alpha^{-s} = \alpha^r\beta\gamma'$. Both transformation $\gamma\alpha^{-s}$ and $\alpha^r\beta$ do not have the element n in their image. So it suffices to show that for every transformation δ on $\{1,\ldots,n-1\}$ we can generate a transformation γ' on $\{1,\ldots,n\}$ such that $\gamma'|_{\{1,\ldots,n-1\}} = \delta$. Observe, that the transformations α^p and β (see the definition of β) act as permutations on the set $\{1,\ldots,n-1\}$ and their restrictions to this set are generators of S_{n-1}.

We can also generate the transformation η that maps $(1)\eta = (2)\eta = 1$ and is the identity on $\{3,\ldots,n-1\}$. This can be done by first creating a transformation with the same kernel as η. The kernel of β partitions the set $\{1,\ldots,n\}$ into $\{\{1,n\},\{2\},\ldots,\{n-1\}\}$. We can now construct a transformation σ that acts as a permutation on $\{1,\ldots,n-1\}$ and that maps $(2)\beta \mapsto n-1$ and $(1)\beta \mapsto k$. Therefore the transformation $\beta\sigma\alpha$ maps 2 to n, and 1 to itself, and has the same kernel as β. Consequently the transformation $\beta\sigma\alpha\beta$ has the kernel $\{\{1,2,n\},\{3\},\ldots,\{n-1\}\}$ and all its images are contained in $\{1,\ldots,n-1\}$. Therefore there exists a permutation σ' that acts on $\{1,\ldots,n-1\}$ and for which $\beta\sigma\alpha\beta\sigma' = \eta$. Since this gives us three generators for T_{n-1}, it is clear that with these three transformations α^p, β, and η we can construct a transformation γ' such that $\gamma'|_{\{1,\ldots,n-1\}} = \delta$ for every transformation $\delta \in S_{n-1}$. □

Before we continue our investigations estimating the size of $U_{k,\ell}$, we show that $U_{k,\ell}$ is in fact a syntactic monoid of a regular language accepted by some n-state deterministic finite automaton.

Theorem 7. *Let $k, \ell \in \mathbb{N}$ be two natural numbers with $k < \ell$ and $\gcd\{k,\ell\} = 1$, and set $n = k+\ell$. Then there is an n-state minimal deterministic finite automaton A with binary input alphabet the transition monoid of which equals $U_{k,\ell}$. Hence, $U_{k,\ell}$ is the syntactic monoid of $L(A)$.*

Proof. By Theorem 6 the semigroup $U_{k,\ell}$ is generated the permutation $\alpha = (1\,2\,\ldots\,k)(k+1\,k+2\,\ldots\,n)$ and by an element β of kernel size $n-1$. Define the deterministic finite automaton $A = (Q, \{a,b\}, \delta, 1, F)$, where $Q = \{1,\ldots,n\}$,

$F = \{k, n\}$, and $\delta(i, a) = (i)\alpha$ and $\delta(i, b) = (i)\beta$ for all $i \in Q$. In order to show that $U_{k,\ell}$ is the syntactic monoid of $L(A)$ we have to prove that all states are reachable and belong to different equivalence classes. For reachability we argue as follows: Obviously, the transition monoid of A equals $U_{k,\ell}$ by construction. Thus, all states are reachable since $U_{k,\ell}$ contains all constant functions. For the second claim we distinguish three cases:

1. Let $i, j \in \{1, \ldots, k\}$ with $i < j$. Then $\delta(i, a^{k-j}) \notin F$ and $\delta(j, a^{k-j}) = k \in F$. Thus, states i and j are inequivalent.
2. Let $i, j \in \{k+1, \ldots, n\}$ with $i < j$. Then a similar argumentation as above shows that both states are not equivalent.
3. Finally, let $i \in \{1, \ldots, k\}$ and $j \in \{k+1, \ldots, n\}$. Here we can not exclude that $k - i = n - j$. Nevertheless, since $\gcd\{k, \ell\} = 1$ it follows in that case that $\delta(i, a^{k-i}a^k) = k$ and $k \in F$, while $\delta(j, a^{k-i}a^k) \notin F$. This implies that both states are inequivalent, too.

This completes our proof and shows that A is a minimal deterministic finite automaton. Hence, A's transition monoid equals the syntactic monoid of $L(A)$. □

In order to determine the size of $U_{k,\ell}$ the following lemma, relating size and number of colourings of a particular graph, is very useful in the sequel.

Lemma 2. *Let $n = k + \ell$ for some naturals numbers k and ℓ satisfying $k < \ell$ and $\gcd\{k, \ell\} = 1$. Denote the complete bipartite graph with two independent sets C and D having k and ℓ nodes, respectively, by $K_{k,\ell}$. Then*

$$|U_{k,\ell}| = k\ell + N,$$

where N is the number of invalid colourings of $K_{k,\ell}$ with colours from $\{1, \ldots, n\}$, such that at least one colour from the set $\{k+1, \ldots, n\}$ is missing.

Proof. We assume, without loss of generality, that $V = \{1, \ldots, n\}$ is the set of nodes of $K_{k,\ell}$ and that $C = \{1, \ldots, k\}$ and $D = \{k+1, \ldots, n\}$. Thus every (valid or invalid) colouring of $K_{k,\ell}$ can be considered as a transformation of T_n and *vice versa*. It is rather straightforward to see that the transformations of $U_{k,\ell}$ satisfying the second part of Definition 1 coincide exactly with the invalid colourings of $K_{k,\ell}$, where at least one colour from the set $\{k+1, \ldots, n\}$ is missing. □

Now we are ready to estimate the size of $U_{k,\ell}$ and prove some asymptotics for particular values of k and ℓ.

Theorem 8. *Assume $n \geq 3$. Let $n = k + \ell$ for some natural numbers k and ℓ obeying $k < \ell$ and $\gcd\{k, \ell\} = 1$. Then*

$$|U_{k,\ell}| \geq n^n - \binom{n}{\ell}\ell! n^k - \binom{n}{\ell}k^k \ell^\ell.$$

Moreover, for every n there exists $k(n)$ and $\ell(n)$ satisfying the above properties and $\ell(n) - k(n) \leq 4$, such that

$$\lim_{n\to\infty} \frac{|U_{k(n),\ell(n)}|}{n^n} = 1.$$

Proof. By our previous investigation on the relationship between the size of $U_{k,\ell}$ and the number of (in)valid colourings of the complete bipartite graph $K_{k,\ell}$ we have

$$U_{k,\ell} \supseteq T_n - \underbrace{\{\, \gamma \in T_n \mid \{k+1,\ldots,n\} \subseteq img(\gamma) \,\}}_{A} - \underbrace{\{\, \gamma \in T_n \mid \gamma \text{ is a valid colouring of the graph } K_{k,\ell} \,\}}_{B}.$$

This is also due to the fact that every permutation is a valid colouring of $K_{k,\ell}$.

Thus, in order to determine $|U_{k,\ell}|$ it is sufficient to estimate the size of A and B. We over-estimate both sets in the forthcoming. Let

$$A' = \{\, (\gamma, a_1, \ldots, a_\ell) \mid \gamma \in A \text{ and } \gamma(a_i) = k+i, \text{ for } 1 \leq a_i \leq n \,\}.$$

It is easy to see that that $|A| \leq |A'|$ and furthermore $|A'| = \binom{n}{\ell}\ell! n^k = n^{\underline{\ell}} n^k$ where $n^{\underline{\ell}} = n(n-1)\cdots(n-\ell+1)$ denotes the falling factorial. We first choose the values of the a_i, then assign a different element of $\{k+1,\ldots,k+\ell\}$ to each of them and finally assign an arbitrary element to each of the remaining k pre-images. For B we argue as follows: Let

$$B' = \{\, (\gamma, X, Y) \mid \gamma \in B,\, X \uplus Y = \{1,\ldots,n\},\, |X| = k,\, |Y| = \ell, \\ (\{1,\ldots,k\})\gamma \subseteq X, \text{ and } (\{k+1,\ldots,n\})\gamma \subseteq Y \,\}.$$

One observes, that $|B| \leq |B'|$ and furthermore $|B'| = \binom{n}{\ell} k^k \ell^\ell$, since we first choose the elements of Y (which gives us automatically the elements of X), then we assign a colour from X to the nodes in $\{1,\ldots,k\}$, and afterwards we assign a colour from Y to the nodes in $\{k+1,\ldots,k+\ell\}$. This shows that

$$|U_{k,\ell}| \geq n^n - \binom{n}{\ell}\ell! n^k - \binom{n}{\ell} k^k \ell^\ell.$$

For the asymptotic result, we first show the following claim: Assume $n \geq 3$. Then there exists $k, \ell \in \mathbb{N}$ such that $n = k + \ell$, $\ell - k \leq 4$, and $\gcd\{k, \ell\} = 1$.

We argue as follows: Whenever $n = 2m+1$ then set $k = m$ and $\ell = m+1$. If n is even, we have to distinguish the following two cases: Either $n = 4m$, then we can set $k = 2m-1$ and $\ell = 2m+1$, both can not be divided by 2 and since $\ell - k = 2$ there is no other candidate for a common divisor. If $n = 4m+2$, then we can set $k = 2m-1$ and $\ell = 2m+3$. Since $\ell - k = 4$, the only candidates for common divisors are 2 and 4, but clearly k and ℓ are not divisible by any of them. This proves the existence of some k and ℓ, which are close to $\frac{n}{2}$.

Then the asymptotic result is seen by using Stirling's approximation for the factorials, proving that both $\frac{|A|}{n^n}$ and $\frac{|B|}{n^n}$ converge to 0 whenever n goes to infinity. Let A' and B' be the sets defined above. We obtain

$$\begin{aligned}\frac{|A|}{n^n} \leq \frac{|A'|}{n^n} = \frac{n^\ell n^k}{n^n} = \frac{n!}{\ell! n^{n-k}} = \frac{1}{n^{n-k}} \cdot \frac{\sqrt{2\pi n}\left(\frac{n}{e}\right)^n (1+\Theta(\frac{1}{n}))}{\sqrt{2\pi\ell}\left(\frac{\ell}{e}\right)^\ell (1+\Theta(\frac{1}{\ell}))} \\ = \sqrt{\frac{n}{\ell}}\left(\frac{n}{e}\right)^k \frac{1}{\ell^\ell} \frac{1+\Theta(\frac{1}{n})}{1+\Theta(\frac{1}{\ell})}\end{aligned}$$

Since both k and ℓ are close to $\frac{n}{2}$ as shown above, we can infer that the last factor converges to 1 whenever n goes to infinity. Furthermore, since $k \leq \frac{n}{2} \leq \ell$, it follows that

$$\sqrt{\frac{n}{\ell}}\left(\frac{n}{e}\right)^k \frac{1}{\ell^\ell} \leq \sqrt{2}\left(\frac{n}{e}\right)^{\frac{n}{2}} \frac{1}{\left(\frac{n}{2}\right)^{\frac{n}{2}}} \leq \sqrt{2}\left(\frac{2}{e}\right)^{\frac{n}{2}}.$$

Thus, the last term obviously converges to 0 whenever n goes to infinity. For the fraction of $|B|$ and n^n we do similar. We find

$$\begin{aligned}\frac{|B|}{n^n} \leq \frac{|B'|}{n^n} &= \frac{1}{n^n}\frac{n!}{k!\ell!}k^k\ell^\ell \\ &= \frac{1}{n^n}\frac{\sqrt{2\pi n}\left(\frac{n}{e}\right)^n}{\sqrt{2\pi k}\left(\frac{k}{e}\right)^k\sqrt{2\pi\ell}\left(\frac{\ell}{e}\right)^\ell}k^k\ell^\ell\frac{1+\Theta(\frac{1}{n})}{(1+\Theta(\frac{1}{k}))(1+\Theta(\frac{1}{\ell}))} \\ &= \frac{1}{\sqrt{2\pi}}\sqrt{\frac{n}{k\ell}}\frac{1+\Theta(\frac{1}{n})}{(1+\Theta(\frac{1}{k}))(1+\Theta(\frac{1}{\ell}))}\end{aligned}$$

Again the last factor converges to 1. Now it holds that

$$\sqrt{\frac{n}{k\ell}} = \sqrt{\frac{n}{kn-k^2}} = \frac{1}{\sqrt{k-\frac{k^2}{n}}} \overset{\frac{3n}{8}\leq k\leq\frac{n}{2}}{\leq} \frac{1}{\sqrt{\frac{3n}{8}-\frac{n}{4}}} = \sqrt{\frac{8}{n}},$$

where $\frac{3n}{8} \leq k \leq \frac{n}{2}$ follows for large enough n, since k and $\frac{n}{2}$ differ only by a constant. And the last term converges to 0 whenever n goes to infinity. This proves the second statement of our result. □

Now we come to the main result of this section. Recall that $g(n)$ denotes Landau's function [4–6], which gives the size of the maximal subgroup of S_n which can be generated by one generator.

Theorem 9. *Assume $n \geq 3$ and let A be a n-state deterministic finite automata. Then a monoid of size $n^n - n! + g(n)$ is sufficient to recognize the language $L(A)$ and a monoid of size*

$$n^n - \binom{n}{\ell}\ell! n^k - \binom{n}{\ell}k^k\ell^\ell,$$

where $n = k+\ell$, $\ell - k \leq 4$, and $\gcd\{k,\ell\} = 1$ for some natural numbers k and ℓ, is necessary in the worst case.

Proof. The upper bound $n^n - n! + g(n)$ is immediate, since we assume that only one of the two generators is a permutation and the lower bound follows by Theorems 7 and 8. □

Moreover, we obtain the following corollary, which we state without proof:

Corollary 1. *There is a sequence $L_1, L_2, \ldots$ of binary regular languages such that*

$$\lim_{n\to\infty} \frac{|M(L_i)|}{n^n} = 1,$$

and each L_i is accepted by a minimal deterministic finite automaton with exactly n states. □

5 Conclusions

We have studied the relationship between the size of a deterministic finite automaton A and the size of the syntactic monoid, which is necessary to recognize the language $L(A)$.

n	$\lvert S_n\rvert = n!$	k	ℓ	$\lvert U_{k,\ell}\rvert$	$max(n)$	$n^n - n! + g(n)$	$\lvert T_n\rvert = n^n$
3	6	1	2	13	24	24	27
4	24	1	3	133	176	236	256
5	120	2	3	1857	2110	3011	3125
		1	4	1753			
6	720	1	5	27311	32262 (?)	45942	46656
7	5040	3	4	607285	610871 (?)	818515	823543
		2	5	610871			
		1	6	492637			
8	40320	3	5	13492007	13492007 (?)	16736911	16777216
		1	7	10153599			
9	362880	4	5	323534045	323534045 (?)	387057629	387420489
		2	7	306605039			
		1	8	236102993			
10	3628800	3	7	8678434171	8678434171 (?)	9996371230	10000000000
		1	9	6122529199			
11	39916800	5	6	256163207631	258206892349 (?)	285271753841	285311670611
		4	7	258206892349			
		3	8	251856907425			
		2	9	231326367879			
		1	10	175275382621			

Table 1. Sizes of some investigated semigroups.

In most cases, we were able to prove tight upper bounds. The only exception are binary regular languages were we have presented a non-matching upper and lower bound. We summarize some computed values on the size of some of the semigroups (monoids) involved in Table 1.

There, the number $max(n)$ denotes the size of the maximal transformation semigroup (monoid) with two generators, which might not coincide with the size of some $U_{k,\ell}$. A table entry with a question mark indicates that the precise value is not known and thus is a conjecture. The generators for the groups with 24, 176, 2110, and 32262 elements all contain a single cycle permutation $(1\,2\,\ldots\,n)$. However, already for $n = 7$, the case where one of the generators is the cycle is beat by our semigroup $U_{k,\ell}$.

It remains to tighten the bound on the syntactic monoid size on two generators in future research. To understand the very nature of this question it seems to be very important, to precisely characterize the maximal size transformation semigroup on two generators, in a similar way as the generators for T_n and S_n are characterized in Theorems 4 and 5. We conjecture, that for every $n \geq 7$, there exists natural numbers k and ℓ with $n = k + \ell$ such that the semigroup $U_{k,\ell}$ is maximal under all two generator transformation semigroups (monoids).

Acknowledgments

Thanks to J. M. Howie and J.-E. Pin for some fruitful discussions on the subject.

References

1. J.-M. Champarnaud, D. Maurel, and D. Ziadi, editors. *Automata Implementation, Proceedings of the* 3*rd International Workshop on Implementing Automata*, number 1660 in LNCS, Rouen, France, September 1998. Springer.
2. J. M. Howie. *An Introduction to Semigroup Theory*, volume 7 of *L. M. S. Monographs*. Academic Press, 1976.
3. S. C. Kleene. Representation of events in nerve nets and finite automata. In C. E. Shannon and J. McCarthy, editors, *Automata studies*, volume 34 of *Annals of mathematics studies*, pages 2–42. Princeton University Press, 1956.
4. E. Landau. Über die Maximalordnung der Permutationen gegebenen Grades. *Archiv der Mathematik und Physik*, 3:92–103, 1903.
5. J.-L. Nicolas. Sur l'ordre maximum d'un élément dans le groupe s_n des permutations. *Acta Arithmetica*, 14:315–332, 1968.
6. J.-L. Nicolas. Ordre maximum d'un élément du groupe de permutations et highly composite numbers. *Bulletin of the Mathematical Society France*, 97:129–191, 1969.
7. S. Piccard. *Sur les bases du groupe symétrique et les couples de substitutions qui engendrent un groupe régulier*. Librairie Vuibert, Paris, 1946.
8. J.-E. Pin. *Varieties of formal languages*. North Oxford, 1986.
9. A. Salomaa. On the composition of functions of several variables ranging over a finite set. *Annales Universitatis Turkuensis*, 41, 1960. Series AI.
10. D. Wood and S. Yu, editors. *Automata Implementation, Proceedings of the* 2*nd International Workshop on Implementing Automata*, number 1436 in LNCS, London, Canada, September 1997. Springer.