Available online at www.sciencedirect.com
SCIENCE DIRECT®
Theoretical Computer Science 327 (2004) 319–347
Theoretical Computer Science
www.elsevier.com/locate/tcs

On deterministic finite automata and syntactic monoid size☆

Markus Holzer[a,*], Barbara König[b,1]

[a] *Institut für Informatik, Technische Universität München, Boltzmannstraße 3, 85748 Garching bei München, Germany*

[b] *Institut für Formale Methoden der Informatik, Universität Stuttgart, Universitätsstraße 38, 70569 Stuttgart, Germany*

Received 7 October 2003; received in revised form 1 April 2004; accepted 1 April 2004

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 and lower bounds on the syntactic monoid size depending on the number of generators (input alphabet size) used. It turns out, that the two generator case is the most involved one. There we show a lower bound of $n^n\left(1-\frac{2}{\sqrt{n}}\right)$ for the size of the syntactic monoid of a language accepted by an n-state deterministic finite automaton with binary input alphabet. Moreover, we prove that for every prime $n \geqslant 7$, the maximal size semigroup w.r.t. its size among all (transformation) semigroups which can be generated with two generators, is generated by a permutation with two cycles (of appropriate lengths) and a non-bijective mapping merging elements from these two cycles. As a by-product of our investigations we determine the maximal size among all semigroups generated by two transformations, where one is a permutation with a single cycle and the other is a non-bijective mapping.

Keywords: Automata theory; Deterministic finite automata; Syntactic monoids

☆ This paper is a completely revised and expanded version of two papers presented at the 6th and 7th Conference on Developments in Language Theory (DLT) held in Kyoto, Japan, September 18–21, 2002 and in Szeged, Hungary, July 7–11, 2003, respectively.

* Corresponding author.
E-mail addresses: holzer@informatik.tu-muenchen.de (M. Holzer), koenigba@fmi.uni-stuttgart.de (B. König).

[1] Part of the work was done while the author was at Institut für Informatik, Technische Universität München, Boltzmannstraße 3, D-85748 Garching bei München, Germany.

0304-3975/$ - see front matter © 2004 Elsevier B.V. All rights reserved.
doi:10.1016/j.tcs.2004.04.010

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 [1,17]. 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 [5] 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 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 $uv_1w \in L \iff uv_2w \in L$ for every $u, w \in \Sigma^*$. 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. Recently, this was also proposed in [6].

For most cases, we show tight upper bounds on the syntactic monoid size, 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 maximal size is linear, while for regular languages over an input alphabet with at least three letters the maximal size n^n is reached. The challenging part is to determine the size of the syntactic monoid for regular languages over a binary alphabet. Obviously, $n!$ is a lower bound for the maximal size, which is induced by the two generators of S_n. Compared to this obvious bound we can do much better. We show a lower bound of $n^n\left(1-\frac{2}{\sqrt{n}}\right)$ and a trivial non-matching upper bound of $n^n - n! + g(n)$, where $g(n)$ denotes Landau's function [7,9,10], for the size of the syntactic monoid of a language accepted by an n-state deterministic finite automaton with binary input alphabet. 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.

To obtain the lower bound $n^n\left(1-\frac{2}{\sqrt{n}}\right)$ in the binary input alphabet case we introduce a semigroup which can be generated by a permutation with two cycles (of appropriate lengths) and a non-bijective mapping merging elements from these two cycles. Moreover, we can prove that, for prime $n \geqslant 7$, this semigroup is indeed maximal in size among all (transformation) semigroups that can be generated with two generators. In order to show that there is no larger sub-semigroup of T_n with two generators, we investigate all possible combinations of generators. In principle the following situations for generators appear:

(1) two permutations,
(2) a permutation with one cycle and a non-bijective transformation,

(3) a permutation with two or more cycles and a non-bijective transformation—the semigroup under consideration is of this type, and
(4) two non-bijective transformations.

We will investigate these cases in order to show maximality of the size of the semigroup under consideration in the case of prime numbers. The entire argument relies on a series of lemmata covering the above-mentioned cases, where the second case plays a major role. In fact, as a by-product, we are able to determine the maximal size among all semigroups generated by two transformations, where one transformation is a permutation with a single cycle and the other is a non-bijective mapping. In order to achieve our goal we use diverse techniques from algebra, analysis, and even computer-verified results for a finite number of cases.

The paper is organized as follows. In the next section we introduce the necessary notations. In Section 3 we prove the easy cases on syntactic monoid size and devote Section 4 to the study of binary regular languages. Then in Section 5 we come to the main result of this paper, on the size maximality of the semigroup under consideration. To this end, we investigate in Subsection 5.1 the case where one is a permutation with a single cycle and the other is a non-bijective mapping. Next, two permutations and two non-bijective mappings are considered (Section 5.2). Then Subsection 5.3 deals with the most complicated case, where the permutation contains two or more cycles, which then leads to the main result of the paper. 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 [4,12]. In this paper, we are dealing with regular languages and their syntactic monoids. A *semigroup* is a non-empty 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., in $\alpha\beta$ first α is applied, 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 denoted by S_n trivially is a sub-monoid of T_n, and contains $n!$ elements.

A transformation $\alpha \in T_n$ will be written as

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & \ldots & n-1 & n \\ (1)\alpha & (2)\alpha & (3)\alpha & \ldots & (n-1)\alpha & (n)\alpha \end{pmatrix}.$$

A permutation $\alpha \in S_n$ can also be represented by its cycles, i.e., by

$$(m_1^1 \ldots m_1^{t_1}) \ldots (m_k^1 \ldots m_k^{t_k}),$$

where the $m_i^j \in \{1,\ldots,n\}$ are pairwise different natural numbers. This denotes a permutation α where $(m_i^j)\alpha = m_i^{j+1}$ for $1 \leqslant i \leqslant k$, $1 \leqslant j < t_i$, $(m_i^{t_i})\alpha = m_i^1$, for $1 \leqslant i \leqslant k$, and $(m)\alpha = m$ for all other $m \in \{1,\ldots,n\}$.

Throughout the paper we use the following version of Stirling's approximation for the factorial given in [2,14]:

$$\sqrt{2\pi n}\left(\frac{n}{\mathrm{e}}\right)^n \mathrm{e}^{\frac{1}{12n+1}} < n! < \sqrt{2\pi n}\left(\frac{n}{\mathrm{e}}\right)^n \mathrm{e}^{\frac{1}{12n}}.$$

We need some additional notation. If A is an arbitrary non-empty subset of a semigroup S, then the family of sub-semigroups of S containing A is non-empty, since S itself is one such semigroup; it holds that the intersection of the family is a sub-semigroup of S containing A, which is denoted by $\langle A\rangle$. It is characterized within the set of sub-semigroups of S by the properties: (1) $A \subseteq \langle A\rangle$ and (2) if U is a sub-semigroup of S containing A, then $\langle A\rangle \subseteq U$. The semigroup $\langle A\rangle$ consists of all elements of S that can be expressed as finite products of elements in A. If $\langle A\rangle = S$, then we say that A is a set of generators for S. If $A = \{\alpha, \beta\}$ we simply write $\langle A\rangle$ as $\langle \alpha, \beta\rangle$.

Finally, 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 deterministic finite automata.

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.

Regard, for instance the minimal deterministic finite automaton A over the alphabet $\Sigma = \{a, b\}$ depicted in Fig. 1. The two letters of the alphabet correspond to two transformations

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{pmatrix} \quad \text{and} \quad \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 4 & 2 & 1 \end{pmatrix},$$

which generate the transformation monoid $M(A)$. In this case, $M(A)$ contains exactly 1857 elements. Later, this monoid will be referred to as $U_{2,3}$.

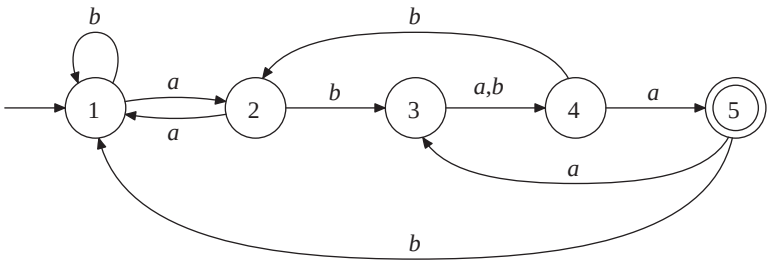

Fig. 1. A minimal deterministic finite automaton.

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. First, we consider unary regular languages, where we can profit from the following result on monogenic (sub)semigroups, which can be found in [4].

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

A single permutation $\alpha \in S_n$ can generate up to $g(n)$ elements, where $g(n)$ is Landau's function—see [7,9,10]. It holds that

$$g(n) = \max\{\mathrm{lcm}\{i_1, \ldots, i_k\} \mid i_1 + \cdots + i_k = n\}$$

and $\lim_{n\to\infty} \frac{\log g(n)}{\sqrt{n \log n}} = 1$. See also [16]. It turns out that the values of Landau's function cannot be reached in the case of syntactic monoids.

When estimating the syntactic monoid size of regular languages over a unary input alphabet we find the following situation.

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 at 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 as well. On the other hand, if A was chosen to be an arbitrary 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* $|\Sigma| \geqslant 2$, *or* (iii) $n \geqslant 3$ *and* $|\Sigma| \geqslant 3$.

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 $\delta(i, c) = (i)\gamma$ for all $i \in Q$. 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 theorem above can be improved with respect to the alphabet size. By some 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 $n \geqslant 3$ the following completeness theorem for functions of one argument given in [15], shows that an improvement is also not possible. The completeness result reads as follows.

Theorem 4. *Assume $n \geqslant 3$. 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 monoids 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 show some results concerning its size, including a lower bound and some facts concerning asymptotics. Section 5 will then determine under which circumstances the semigroup defined below is maximal in size among all semigroups generated by two generators.

The advantage of the explicit definition of the semigroup is that we do not 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 5. Let $n \geqslant 2$ 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 are coprime, there are $k\ell$ possible pairs to choose from. And if k and ℓ are chosen close to $\frac{n}{2}$, then $k\ell > n$.

Since β is non-bijective, at least one index h will be missing from the image of β. Even after subsequent applications of α, the missing index, will never leave the cycle of α it is contained in. Note that in order to maximize $U_{k,\ell}$ we should pick h from the larger of the two cycles of α, since this gives us more indices to choose from. So, in the following we will often demand that $k < \ell$.

4.1. The Syntactic semigroup $U_{k,\ell}$

Next, we have to show that $U_{k,\ell}$ is indeed a semigroup. Moreover, we prove that there is a regular language whose syntactic monoid equals $U_{k,\ell}$, for suitable k and ℓ.

Lemma 6. *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 $m_1, m_2 \geqslant 1$. 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 $m \geqslant 1$, and γ_2 satisfies Condition (2) of Definition 5, 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 Condition (2) of Definition 5.

(3) Assume that $\gamma_2 = \alpha^m$, for some $m \geqslant 1$, and γ_1 satisfies Condition (2) of Definition 5, 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 $h' = (h)\gamma_2 \in \{k+1, \ldots, k+\ell\}$ and $h' \notin img(\gamma_1\gamma_2)$, 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 Condition (2) of Definition 5. 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 $1 \leqslant r \leqslant 2$.

By setting $i = i_1$, $j = j_1$, and $h = h_2$, it is easy to see that $\gamma_1\gamma_2$ satisfies Condition (2) of Definition 5. □

Before we can prove that $U_{k,\ell}$ is generated by two elements of $T_{k+\ell}$ we need a result, which states how to find a complete basis for the symmetric group S_n. The theorem given below was shown in [11].

Theorem 7. *Given a non-identical element α in S_n, then there exists an element β of S_n such that 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 8. *Let $k, \ell \in \mathbb{N}$ be two natural numbers with $k \neq 1$, $k < \ell$, 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 5. 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 7, 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 $1 \leqslant i \leqslant n-1$ and $(n)\beta = (1)\pi_2$. Hence β has kernel size $n-1$.

We will first show that α and β generate at most the transformations specified in Definition 5. 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 $r \geqslant 0$. 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 5. Clearly transformations of the form $\gamma = \alpha^m$, for some $m \geqslant 1$, 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 and $\alpha^r\beta$ has kernel size $n-1$. 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 the values $(2)\beta \mapsto n-1$ 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 $\beta\sigma\alpha\beta\sigma'|_{\{1,\ldots,n\}} = \eta$. 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 9. *Let $k, \ell \in \mathbb{N}$ be two natural numbers with $k \neq 1$, $k < \ell$, 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 8 the semigroup $U_{k,\ell}$ is generated by 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 cannot 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 $L(A)$. □

4.2. On the size and asymptotics of the $U_{k,\ell}$ semigroup

In order to determine the size of $U_{k,\ell}$ it turned out to be very useful to show a connection between the number of elements of the semigroup and the number of invalid colourings of a graph. An transformation $\gamma \in T_n$ is a mapping from the set $\{1,\ldots,n\}$ into the set $\{1,\ldots,n\}$ and in the following we identify the pre-image set with the set of n nodes of a graph and the image set with a set of n colours. According to Condition (2) of Definition 5, a transformation γ is contained in $U_{k,\ell}$ whenever there are suitable indices i, j such that $\gamma(i) = \gamma(j)$ and some more conditions are satisfied. So if we consider a graph with an edge connecting the nodes i and j, γ is an invalid colouring of such a graph.

The following theorem determines the exact size of the semigroups $U_{k,\ell}$ by using results from graph theory.

Theorem 10. *Let $n = k + \ell$ for some naturals numbers k and ℓ. Denote the complete bipartite graph with two independent sets V_1 and V_2 having k and ℓ nodes, respectively, by $K_{k,\ell}$. Then*

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

where

$$N = \sum_{i=1}^{n} \left(\binom{n}{i} - \binom{k}{i-\ell} \right) \left(\left\{ {n \atop i} \right\} - \sum_{r=1}^{i} \left\{ {k \atop r} \right\} \left\{ {\ell \atop i-r} \right\} \right) i!$$

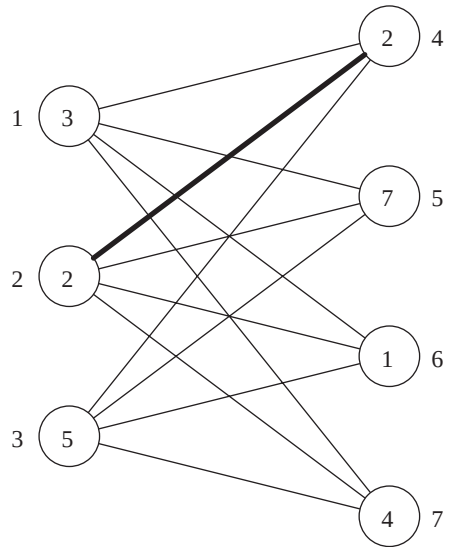

Fig. 2. An invalid colouring of the bipartite graph $K_{3,4}$.

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. Here $\left\{{n \atop i}\right\}$ stands for the Stirling numbers of the second kind and denotes the number of possibilities to partition an n-element set into i non-empty subsets.

Proof. We assume, without loss of generality, that $V = \{1,\ldots,n\}$ is the set of nodes of $K_{k,\ell}$ and that $V_1 = \{1,\ldots,k\}$ and $V_2 = \{k+1,\ldots,n\}$. Thus every (valid or invalid) colouring of $K_{k,\ell}$ can be considered as a transformation of T_n and *vice versa*. To illustrate this, consider the transformation

$$\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 5 & 2 & 7 & 1 & 4 \end{pmatrix} \in U_{3,4}.$$

In a graph colouring the upper row corresponds to nodes and the lower row to colours (see Fig. 2, where colours are written inside the nodes and numbers are besides each node). The colouring is invalid—see the edge which is emphasized—and one colour out of $\{4, 5, 6, 7\}$ is missing, namely colour 6.

It is rather straightforward to see that the transformations of $U_{k,\ell}$ satisfying the second part of Definition 5 coincide exactly with the invalid colourings of $K_{k,\ell}$, where at least one colour from the set $\{k+1,\ldots,n\}$ is missing.

The chromatic polynomial $\chi(G,\lambda)$ of a graph $G = (V,E)$ with $V = \{1,\ldots,n\}$ and $E \subseteq \{\{v,w\} \mid v,w \in V \text{ and } v \neq w\}$ gives the number of valid colourings of G with at most λ colours—we refer to [13] for an introduction to chromatic polynomials. It can be

written as

$$\chi(G,\lambda) = \sum_{i=1}^{\lambda} \binom{n}{i} p(G,i) i!,$$

where $p(G,i)$ is the number of possibilities to partition V into i non-empty independent sets. The above formula can easily be verified with the following considerations: In order to colour a graph with *exactly* i colours, one first chooses i of n colours, then partitions the nodes into i independent sets and finally assigns colours to sets of nodes.

With the above consideration, we can deduce that the number of invalid colourings of a graph G, with colours from $\{1,\ldots,n\}$, where at least one colour from the set $\{k+1,\ldots,n\}$ is missing is equal to

$$\sum_{i=1}^{n} \binom{n}{i} - \binom{n-\ell}{i-\ell}\left(\left\{ {n \atop i} \right\} - p(G,i)\right) i!. \tag{1}$$

This follows from the fact that $\binom{n-\ell}{i-\ell} = \binom{k}{i-\ell}$ is the number of possibilities to choose colours in such a way that all colours of $\{k+1,\ldots,n\}$ are present. Note that $\left\{ {n \atop i} \right\} - p(G,i)$ is the number of possibilities to partition the nodes of G into sets such that at least one set is not independent.

In the case of $G = K_{k,\ell}$ we find that

$$p(K_{k,\ell}, i) = \sum_{r=1}^{i} \left\{ {k \atop r} \right\} \left\{ {\ell \atop i-r,} \right\},$$

where r is the number of subsets, into which the set V_1 is partitioned. Clearly no independent set can contain elements of both $\{1,\ldots,k\}$ and $\{k+1,\ldots,n\}$. Substituting $p(G,i)$ in Eq. (1) by the value computed above and adding $\operatorname{lcm}\{k,\ell\}$, which is the order of α and therefore the number of permutations in $U_{k,\ell}$, one obtains the claimed formula for the size of $U_{k,\ell}$. □

Now we are ready to prove some asymptotics for the $U_{k,\ell}$ semigroup for particular values of k and ℓ. Since the following theorem requires the existence of some k, ℓ such that $\ell - k \leqslant 4$, i.e., k and ℓ are close to $\frac{n}{2}$, we will first show that coprime k, ℓ with this property always exist and that $U_{k,\ell}$ can thus be generated with two generators in this case.

Lemma 11. *For every $n \geqslant 2$ there exists $k(n)$ and $\ell(n)$ satisfying $n = k(n) + \ell(n)$, $k(n) < \ell(n)$ and $\gcd\{k(n),\ell(n)\} = 1$ such that $\ell(n) - k(n) \leqslant 4$.*

Proof. Whenever $n = 2m+1$ for some m, i.e., n is odd, 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 cannot 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 $\frac{n}{2}$. □

Theorem 12. *Assume $n \geqslant 3$. Let $n = k + \ell$ for some natural numbers k and ℓ. Then*

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

If $\ell - k \leqslant 4$ we can simplify this to

$$|U_{k,\ell}| \geqslant n^n \left(1 - \frac{2}{\sqrt{n}}\right).$$

Moreover, if we choose for every n numbers $k(n)$ and $\ell(n)$ satisfying $\ell(n) - k(n) \leqslant c$ for some constant c, then

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

Proof. By our previous investigation on the relationship between the size of the $U_{k,\ell}$ semigroup 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 find a lower bound for $|U_{k,\ell}|$ it is sufficient to estimate the size of A and B. We over-estimate both sets in the following. Let

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

It is easy to see that $|A| \leqslant |A'|$ and furthermore $|A'| = \binom{n}{\ell}\ell! n^k$. 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 $|B| \leqslant |B'|$ and furthermore $|B'| = \binom{n}{\ell} k^k \ell^\ell$, since we first choose the elements of Y (which automatically gives us 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

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

We use Stirling's approximation in the version

$$\sqrt{2\pi n}\left(\frac{n}{\mathrm{e}}\right)^n < n! < \sqrt{2\pi n}\left(\frac{n}{\mathrm{e}}\right)^n \mathrm{e}^{\frac{1}{12}}.$$

It holds that

$$|A'| = \binom{n}{\ell}\ell! n^k = \frac{n!}{k!}n^k < n^k \frac{\sqrt{2\pi n}\left(\frac{n}{\mathrm{e}}\right)^n \mathrm{e}^{\frac{1}{12}}}{\sqrt{2\pi k}\left(\frac{k}{\mathrm{e}}\right)^k} = n^n \sqrt{\frac{n}{k}}\left(\frac{n}{k}\right)^k \left(\frac{1}{\mathrm{e}}\right)^\ell \mathrm{e}^{\frac{1}{12}}$$

Since $\ell - k \leqslant c$ and $k < \ell$, it follows that $\frac{n-c}{2} \leqslant k \leqslant \frac{n}{2}$ and $\ell \geqslant \frac{n}{2}$ and therefore:

$$|A'| < n^n \sqrt{\frac{2n}{n-c}}\left(\frac{2n}{n-c}\right)^{\frac{n}{2}}\left(\frac{1}{\mathrm{e}}\right)^{\frac{n}{2}} \mathrm{e}^{\frac{1}{12}} = n^n \sqrt{\frac{2n}{n-c}}\left(\frac{2n}{(n-c)\mathrm{e}}\right)^{\frac{n}{2}} \mathrm{e}^{\frac{1}{12}}.$$

If we assume that $\ell - k \leqslant 4 = c$ and $n \geqslant 32$, we can infer that $c \leqslant \frac{n}{8}$ and hence

$$|A'| < n^n \sqrt{\frac{16}{7}}\left(\frac{16}{7\mathrm{e}}\right)^{\frac{n}{2}} \mathrm{e}^{\frac{1}{12}}.$$

This term is strictly smaller than $n^n \frac{1}{\sqrt{n}}$ for $n \geqslant 32$. This can be shown with the following consideration:

$$\sqrt{\frac{16}{7}}\left(\frac{16}{7\mathrm{e}}\right)^{\frac{n}{2}} \mathrm{e}^{\frac{1}{12}} \leqslant \frac{1}{\sqrt{n}} \iff \frac{16}{7}\left(\frac{16}{7\mathrm{e}}\right)^n \mathrm{e}^{\frac{1}{6}} \leqslant \frac{1}{n} \iff \frac{16}{7}\mathrm{e}^{\frac{1}{6}} n \leqslant \left(\frac{7\mathrm{e}}{16}\right)^n.$$

This inequality holds for $n = 32$ and it can be shown that the derivation of the left-hand side—which is $\frac{16}{7}\mathrm{e}^{\frac{1}{6}}$—is strictly smaller than the derivation of the right-hand side—which is $\left(\frac{7\mathrm{e}}{16}\right)^n \ln\left(\frac{7\mathrm{e}}{16}\right)$—for $n \geqslant 32$.

A lower bound for the size of B' can be obtained as follows:

$$|B'| = \frac{n!}{k!\ell!}k^k \ell^\ell < \frac{\sqrt{2\pi n}\left(\frac{n}{\mathrm{e}}\right)^n \mathrm{e}^{\frac{1}{12}}}{\sqrt{2\pi k}\left(\frac{k}{\mathrm{e}}\right)^k \sqrt{2\pi\ell}\left(\frac{\ell}{\mathrm{e}}\right)^\ell} k^k \ell^\ell = \frac{n^n}{\sqrt{2\pi}}\sqrt{\frac{n}{k\ell}}\,\mathrm{e}^{\frac{1}{12}}.$$

Since $\frac{n-c}{2} \leqslant k \leqslant \frac{n}{2}$ and $l \geqslant \frac{n}{2}$, we obtain

$$|B'| < \frac{n^n}{\sqrt{2\pi}}\sqrt{\frac{n}{\frac{n-c}{2}\,\frac{n}{2}}}\,\mathrm{e}^{\frac{1}{12}} = n^n \sqrt{\frac{2}{\pi(n-c)}}\mathrm{e}^{\frac{1}{12}}.$$

Again, if we assume $\ell - k \leqslant 4$ and $n \geqslant 32$, we obtain $c \leqslant \frac{n}{8}$ and

$$|B'| < n^n \sqrt{\frac{16}{7\pi n}}\,\mathrm{e}^{\frac{1}{12}} \approx n^n\, 0.85292\, \frac{1}{\sqrt{n}} \leqslant n^n\, \frac{1}{\sqrt{n}}.$$

Combined, we obtain

$$|U_{k,\ell}| \geqslant n^n \left(1 - \frac{2}{\sqrt{n}}\right)$$

for $n \geqslant 32$. By checking all other cases, we can infer that the inequality holds for all n.

Then, the asymptotic result can be easily seen. If we divide the last term above by n^n, it is obvious that it converges to 1. □

Now we come to the main result of this section. Recall that $g(n)$ denotes Landau's function [7,9,10], which gives the maximal size of a subgroup of S_n which can be generated by one generator.

Theorem 13. *Assume $n \geqslant 3$ and let A be an n-state deterministic finite automaton with binary input alphabet. Then a monoid of size $n^n - n! + g(n)$ is sufficient to recognize the language $L(A)$ and a monoid of size at least*

$$n^n \left(1 - \frac{2}{\sqrt{n}}\right)$$

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 from Lemma 11 and Theorems 9 and 12. □

Observe, that in [6] a lower bound of $n^n\left(1 - \frac{4}{n}\right)$, for odd $n \geqslant 70$, was shown for the largest sub-semigroup of T_n that can be generated by two generators. This lower bound is slightly better then ours, since the authors have used a more elaborate counting argument for the number of proper vertex colourings of a bipartite graph, which is due to [8].

Finally, we obtain the following corollary:

Corollary 14. *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. On the maximality of $U_{k,\ell}$ semigroups

Extending the asymptotic result shown in the last section, we now address the question of obtaining an exact characterization of a subgroup of T_n of maximal size that can be generated with two generators. Although this problem is not fully solved yet, we can show that one of the semigroups $U_{k,\ell}$ is indeed maximal in size whenever $k+\ell$ is a prime number. The rest of this section will be concerned with establishing the following result:

Theorem 15. *Let $n \geqslant 7$ be a prime number. Then a semigroup $U_{k,\ell}$, for some k and ℓ with $n = k + \ell$, $k < \ell$ and $k \neq 1$, is maximal w.r.t. its size among all semigroups which can be generated with two generators.*

In order to show that there is no larger sub-semigroup of T_n with two generators, we investigate all possible combinations of generators. In principle, the following situations for generators appear:

(1) two permutations,

(2) a permutation with one cycle and a non-bijective transformation,
(3) a permutation with two or more cycles and a non-bijective transformation—the semigroup $U_{k,\ell}$ is of this type, and
(4) two non-bijective transformations.

The rest of this section is organized as follows: We deal with the four cases, mentioned above, starting with Case (2), which is particularly interesting and which can be characterized completely. We then continue by showing that choosing two generators according to Case (1) or (4) cannot result in a semigroup of maximal size. Then we consider Case (3) and finally summarize all these cases, which leads to Theorem 15 above.

5.1. Semigroup size—the single cycle case

In this subsection, we consider the case where one generator is a permutation containing a single cycle and the other is a non-bijective transformation. This situation is of particular interest, since it allows us to completely characterize this case and moreover it is very helpful in the sequel when dealing with two permutations or two non-bijective transformations.

The outline of this subsection is as follows: First we define a subset of T_n by some easy properties—as in the case of the $U_{k,\ell}$ semigroup, verify that it is a semigroup and that it is generated by two generators. The subset of T_n we are interested in, is defined as follows:

Definition 16. Let $n \geqslant 2$ and $1 \leqslant d < n$. Furthermore, let $\alpha = (1\,2\,3\,\ldots\,n)$ be a permutation of S_n consisting of one cycle. We define V_n^d as a subset of T_n as follows: A transformation γ is an element of V_n^d if and only if
(1) there exists a natural number $m \in \mathbb{N}$ such that $\gamma = \alpha^m$ *or*
(2) there exists an $i \in \{1, \ldots, n\}$ such that $(i)\gamma = (i +_n d)\gamma$, where $+_n$ denotes the addition modulo n in the set $\{1, \ldots, n\}$.

The intuition behind choosing this specific semigroup V_n^d is the following: Without loss of generality we can assume that $\alpha = (1\,2\,3\,\ldots\,n)$. By choosing a non-bijective transformation β which maps two elements $1 \leqslant i < j \leqslant n$ onto the same image one can infer that every transformation γ generated by α and β is either a multiple of α or maps two elements of distance $d := j - i$ to the same value.

5.1.1. The set V_n^d is a syntactic semigroup

In this subsection we show that V_n^d is indeed a semigroup and that V_n^d is isomorphic to $V_n^{d'}$ if $\gcd\{n, d\} = \gcd\{n, d'\}$. Therefore, it will be sufficient to consider only divisors of n in the following.

Lemma 17. *The set V_n^d is closed under composition and is therefore a* (*transformation*) *semigroup. Moreover, V_n^d is isomorphic to $V_n^{d'}$ whenever $d' = \gcd\{n, d\}$.*

Proof. The proof that V_n^d is a transformation semigroup is similar to the proof of Lemma 6 and is thus left to the reader. To show that V_n^d is isomorphic to $V_n^{d'}$ we argue as follows. Consider the equation $x \cdot d \equiv d' (\mathrm{mod}\, n)$. It has a solution if and only if $x \cdot \frac{d}{d'} \equiv 1 \pmod{\frac{n}{d'}}$ has a solution. A solution x_0 exists since $\frac{d}{d'}$ and $\frac{n}{d'}$ are coprime. If

x_0 is an arbitrary solution of the latter equation, then all numbers of the form $x_0 + k\,\frac{n}{d'}$ are solutions as well. The question is whether any of these numbers is relatively prime to n. Since $\gcd\{x_0, \frac{n}{d'}\} = 1$, Dirichlet's Theorem [3] implies that there are infinitely many primes of the form $x_0 + k\,\frac{n}{d'}$. Any such prime p which does not divide n is the solution we are looking for. Now define a permutation $\pi \in S_n$ with $(i)\pi = p^{-1} \cdot_n i$, for all $1 \leqslant i \leqslant n$, where $\cdot_n$ denotes the binary multiplication modulo n in the set $\{1, \ldots, n\}$. Observe that π is a bijection since $\gcd\{p, n\} = 1$. Then define the mapping $\phi : T_n \to T_n$ by $\gamma \mapsto \pi\gamma\pi^{-1}$, for $\gamma \in T_n$. Observe, that whenever $(i)\gamma = (i +_n d)\gamma$, then

$$\begin{aligned}(p \cdot_n i)\pi\gamma\pi^{-1} = (i)\gamma\pi^{-1} = (i +_n d)\gamma\pi^{-1} = (p \cdot_n (i +_n d))\pi\gamma\pi^{-1} \\ = (p \cdot_n i +_n p \cdot_n d)\pi\gamma\pi^{-1} = (p \cdot_n i +_n d')\pi\gamma\pi^{-1}.\end{aligned}$$

It remains to prove that ϕ is an isomorphism from V_n^d to $V_n^{d'}$. This is left to the reader. □

Now we are ready for the proof that two elements are enough to generate all of the semigroup V_n^d.

Theorem 18. *Let $n \geqslant 2$ and $1 \leqslant d < n$. The semigroup V_n^d can be generated by two elements of T_n, where one element is the permutation $\alpha = (1\ 2\ 3\ \ldots\ n)$ and the other is an element β of kernel size $n - 1$.*

Proof. The first generator of V_n^d is the permutation α of Definition 16. We now construct a second generator β such that $(n - d)\beta = (n)\beta$ and furthermore $\beta|_{\{1,\ldots,n-1\}}$, which is β restricted to the set $\{1, \ldots, n - 1\}$, is a permutation.

Observe that

$$\begin{aligned}\alpha^{n-d}\beta &= \begin{pmatrix} 1 & \cdots & d-1 & d & d+1 & \cdots & n \\ n-d+1 & \cdots & n-1 & n & 1 & \cdots & n-d \end{pmatrix}\beta \\ &= \underbrace{\begin{pmatrix} 1 & \cdots & d-1 & d & d+1 & \cdots & n \\ n-d+1 & \cdots & n-1 & n-d & 1 & \cdots & n-d \end{pmatrix}}_{\rho}\beta.\end{aligned}$$

The last equation holds because of $(n - d)\beta = (n)\beta$. We set $\pi_1 = \rho|_{\{1,\ldots,n-1\}}$, which is a permutation of S_{n-1}, and with Theorem 7 we can infer the existence of a permutation $\pi_2 \in S_{n-1}$ such that π_1 and π_2 generate S_{n-1}. This is true since in the case of $n = 5$ when we let d vary over $\{1, 2, 3, 4\}$, we obtain the permutations (1 4 3 2), (1 4 2 3), (1 3 2 4), and (1 2 3 4) for π_1, each of them consisting of a single cycle. None of these is one of the exceptional cases. Now define the second generator β of V_n^d as follows: Let $(i)\beta = (i)\pi_2$ whenever $1 \leqslant i \leqslant n - 1$ and $(n)\beta = (n - d)\pi_2$. Hence β has kernel size $n - 1$ and n is not in the image of β.

We will first show that α and β generate at most the transformations specified in Definition 16. 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 $(n - d)\beta = (n)\beta$. We set $j = (n - d)\alpha^{-m}$ and $k = (n)\alpha^{-m}$. Since the application of α basically amounts to addition of 1 (modulo n) it holds that $j +_n d = k$ and furthermore $(j)\gamma = (j)\alpha^m\beta\gamma' = (n - d)\beta\gamma' = (n)\beta\gamma' = (k)\alpha^m\beta\gamma' = (j +_n d)\gamma$.

Conversely, we show that α and β generate at least the transformations specified in Definition 16. Clearly transformations of the form $\gamma = \alpha^m$, for some $m \geqslant 1$, can be generated easily. Now let γ be a transformation such that $(j)\gamma = (j +_n d)\gamma$ for some j. This implies also that at least one element $h \in \{1, \ldots, n\}$ is missing from the image of γ.

We are now looking for a transformation γ' such that $\gamma = \alpha^{(n-d)-_n j}\beta\gamma'\alpha^h$ and γ' can be generated from α and β. This condition can be rewritten to $\gamma\alpha^{-h} = \alpha^{(n-d)-_n j}\beta\gamma'$. Both transformations $\gamma\alpha^{-h}$ and $\alpha^r\beta$ where $r = (n-d) -_n j$ do not have the element n in their image. Furthermore, it holds that $(j)\gamma\alpha^{-h} = (j +_n d)\gamma\alpha^{-h}$ and $(j)\alpha^{(n-d)-_n j}\beta = (n-d)\beta = (n)\beta = (j +_n d)\alpha^{(n-d)-_n j}\beta$. Additionally, $\alpha^r\beta$ has kernel size $n-1$.

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 $\alpha^{n-d}\beta$ and β (see the definition of β) act as permutations on the set $\{1, \ldots, n-1\}$ and their restrictions to this set are $\pi_1\pi_2$ and π_2. This allows us to construct π_1. Since π_1 and π_2 are generators of S_{n-1}, the same holds for $\pi_1\pi_2$ and π_2.

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 $\{\{n-d, n\}, \{1\}, \ldots, \{n-d-1\}, \{n-d+1\}, \ldots, \{n-1\}\}$. We can now construct a transformation σ that acts as a permutation on $\{1, \ldots, n-1\}$ and that maps $(1)\beta \mapsto n-d-1$ and $(2)\beta \mapsto n-1$. Therefore the transformation $\beta\sigma\alpha$ maps 1 to $n-d$, and 2 to n, and has the same kernel as β. Consequently, the transformation $\beta\sigma\alpha\beta$ has the kernel $\{\{n-d, n\}, \{1, 2\}, \{3\} \ldots, \{n-d-1\}, \{n-d+1\}, \ldots, \{n-1\}\}$ and all its images are contained in $\{1, \ldots, n-1\}$. Therefore there exists a transformation σ' that acts as a permutation 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 $\alpha^{n-d}\beta$, β, and η we can construct a transformation γ' such that $\gamma'|_{\{1,\ldots,n-1\}} = \delta$ for every $\delta \in T_{n-1}$. □

Finally, we show that V_n^d is indeed a syntactic monoid.

Theorem 19. *Let $n \geqslant 2$. Then there is an n-state minimal deterministic finite automaton A with binary input alphabet the transition monoid of which equals V_n^d. Hence, V_n^d is the syntactic monoid of $L(A)$.*

Proof. By Theorem 18 the semigroup V_n^d is generated by the permutation $\alpha = (1\,2\,\ldots\,n)$ and by an element β of kernel size $n-1$. Define the deterministic finite automaton $A = (Q, \{a, b\}, \delta, 1, F)$, where $Q = \{1, \ldots, n\}$, $F = \{n\}$, and $\delta(i, a) = (i)\alpha$ and $\delta(i, b) = (i)\beta$ for all $i \in Q$. In order to show that V_n^d 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 V_n^d by construction. Thus, all states are reachable since V_n^d contains all powers of α. The second claim also easily follows since for $i, j \in \{1, 2, \ldots, n\}$ with $i < j$ we find $\delta(i, a^{n-j}) \notin F$ and $\delta(j, a^{n-j}) = n \in F$. Thus, states i and j are inequivalent. This completes our proof and shows that A is a minimal deterministic finite automaton. Hence, A's transition monoid equals the syntactic monoid of $L(A)$. □

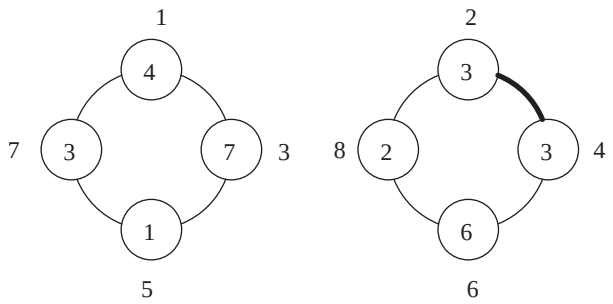

Fig. 3. An invalid colouring of a family of circles $C_4 \oplus C_4$, where $\oplus$ denotes disjoint union of two graphs.

5.1.2. On the size and asymptotics of the V_n^d semigroup

In order to determine the size of V_n^d, the following theorem, relating size and number of colourings of a particular graph, is very useful in the sequel.

Theorem 20. *Let $n \geqslant 2$ and $1 \leqslant d < n$ with $d|n$. Denote the undirected graph consisting of d circles, each of length $\frac{n}{d}$, by G. Then*

$$|V_n^d| = n + N,$$

where $N = n^n - \left((n-1)^{\frac{n}{d}} + (-1)^{\frac{n}{d}}(n-1)\right)^d$ is the number of invalid colourings of G with n colours.

Proof. The sub-semigroup V_n^d can be obtained from T_n by removing all transformations not satisfying the second part of Definition 16 and by adding the n multiples of α afterwards. The number of the former transformations can be determined as follows: Assume that a graph G has nodes $V = \{1, \ldots, n\}$ where a circle C_k consists of nodes $\{k, k+d, \ldots, k+i \cdot d, \ldots, k+n-d\}$, for $1 \leqslant k \leqslant d$. Then one can easily verify that the colourings of G are exactly the transformations which do not satisfy the second part of Definition 16. To illustrate this, regard the transformation

$$\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 3 & 7 & 3 & 1 & 6 & 3 & 2 \end{pmatrix} \in V_8^2.$$

The corresponding graph consists of two circles, both of length 4 (see Fig. 3, where colours are written inside the nodes and node numbers are besides each node). The invalid colouring is marked by emphasizing the corresponding edge.

The number of colourings of a graph G with λ colours is described by its chromatic polynomial, see, e.g. [13]. Since the chromatic polynomial of a circle C_n with n nodes is $(\lambda-1)^n + (-1)^n(\lambda-1)$ and the chromatic polynomial of a graph consisting of disconnected components is the product of the chromatic polynomials of its components, the desired result follows. □

Now we are ready to prove some asymptotics on the size of V_n^d for some particular values of d, which are determined first.

Theorem 21. *The size of V_n^d is maximal whenever*

$$d = \max(\{1\} \cup \{\, d' \mid d' \text{ divides } n \text{ and } \frac{n}{d'} \text{ is odd}\}).$$

Let V_n denote the semigroup V_n^d of maximal size. Then

$$\lim_{n\to\infty} \frac{|V_n|}{n^n} = 1 - \frac{1}{\mathrm{e}},$$

where e *is the base of the natural logarithm.*

Proof. The maximality of V_n^d w.r.t. its size is seen as follows. We first define two real-valued functions

$$u_{n,k}^{\text{even}}(x) = \left((n-1)^{\frac{k}{x}} + (n-1)\right)^x \quad \text{and} \quad u_{n,k}^{\text{odd}}(x) = \left((n-1)^{\frac{k}{x}} - (n-1)\right)^x.$$

The additional index k is present for later use—see Lemma 26. For now we assume that $k = n$.

By Theorem 20 we have $|V_n^d| = n^n + n - u_{n,n}^{\text{even}}(d)$ whenever $\frac{n}{d}$ is even and $|V_n^d| = n^n + n - u_{n,n}^{\text{odd}}(d)$ whenever $\frac{n}{d}$ is odd. Obviously $u_{n,k}^{\text{odd}} < u_{n,k}^{\text{even}}$. First we show that $u_{n,k}^{\text{even}}$ is strictly monotone by taking the first derivation of $\ln u_{n,k}^{\text{even}}(x)$. We obtain

$$\begin{aligned}
\frac{\mathrm{d}}{\mathrm{d}x} \ln u_{n,k}^{\text{even}}(x) &= \ln\left((n-1)^{\frac{k}{x}} + (n-1)\right) + x\,\frac{(n-1)^{\frac{k}{x}} \ln(n-1)\left(-\frac{k}{x^2}\right)}{(n-1)^{\frac{k}{x}} + (n-1)} \\
&> \ln\left((n-1)^{\frac{k}{x}}\right) - \frac{k}{x}\,\frac{(n-1)^{\frac{k}{x}} \ln(n-1)}{(n-1)^{\frac{k}{x}}} \\
&= \frac{k}{x}\ln(n-1) - \frac{k}{x}\ln(n-1) = 0.
\end{aligned}$$

Analogously one can show that $u_{n,k}^{\text{odd}}$ is strictly antitone.

So if there exist divisors d' such that $\frac{n}{d'}$ is odd, the size of semigroup V_n^d is maximal whenever we choose the largest such d'. Otherwise there are only divisors d' such that $\frac{n}{d'}$ is even and we choose the smallest of these divisors, which is 1.

Next consider the semigroup $V_n = V_n^d$, for some $1 \leqslant d < n$. From our previous investigations one can infer that the following inequalities hold:

$$\begin{aligned}
n^n + n - (n-1)^n - (n-1) &\leqslant n^n + n - \left((n-1)^{\frac{n}{d}} + (-1)^{\frac{n}{d}}(n-1)\right)^d \\
&\leqslant n^n + n - \left((n-1)^3 - (n-1)\right)^{\frac{n}{3}}.
\end{aligned}$$

The second half of the inequality follows since the size of V_n^d is maximal whenever $\frac{n}{d}$ is odd and $1 \leqslant d < n$ is maximal. This is achieved ideally whenever $\frac{n}{d} = 3$. The rest follows with the monotonicity and antitonicity of the functions $u_{n,n}^{\text{even}}$ and $u_{n,n}^{\text{odd}}$, respectively.

We now determine the limits of the lower and upper bounds. There we find that

$$\begin{aligned}\lim_{n\to\infty}\frac{n^n+n-(n-1)^n-(n-1)}{n^n} &= \lim_{n\to\infty}\left(1+\frac{1}{n^n}-\left(\frac{n-1}{n}\right)^n\right)\\ &= 1-\lim_{n\to\infty}\left(\frac{n-1}{n}\right)^{n-1}\lim_{n\to\infty}\frac{n-1}{n}\\ &= 1-\frac{1}{\mathrm{e}},\end{aligned}$$

since $\lim_{n\to\infty}(1+\frac{1}{n})^n = \mathrm{e}$, and the limit of the upper bound tends also to $1-\frac{1}{\mathrm{e}}$ by similar reasons as above. Hence $\lim_{n\to\infty}\frac{|V_n|}{n^n} = 1-\frac{1}{\mathrm{e}}$. □

From the asymptotic behaviour of the semigroups V_n and $U_{k,\ell}$ we immediately infer the following theorem.

Theorem 22. *There exists a natural number N such that for every $n \geqslant N$, there exist k and ℓ with $n = k+\ell$ such that $|V_n| < |U_{k,\ell}|$.*

Proof. The existence of a natural number N satisfying the requirements given above follows from Theorems 12 and 21, which state that

$$\lim_{n\to\infty}\frac{|V_n|}{n^n} = 1-\frac{1}{\mathrm{e}} \quad\text{and}\quad \lim_{n\to\infty}\frac{|U_{k(n),\ell(n)}|}{n^n} = 1,$$

for suitable $k(n)$ and $\ell(n)$. □

The following lemma shows that whenever we have a permutation consisting of a single cycle and a non-bijective transformation, we obtain at most as many elements as contained in V_n.

Lemma 23 (*A cycle and a non-bijective transformation*). *Let $n \geqslant 2$. If α is in S_n such that α consists of a single cycle and $\beta \in T_n \setminus S_n$, then $|\langle\alpha,\beta\rangle| \leqslant |V_n|$.*

Proof. Since the permutation α consists of a single cycle, there is a permutation π such that $\pi\alpha\pi^{-1} = (1\,2\,3\,\ldots\,n)$. We set $\alpha' = \pi\alpha\pi^{-1}$ and $\beta' = \pi\beta\pi^{-1}$. Because π is a bijection, we can infer that $|\langle\alpha,\beta\rangle| = |\langle\alpha',\beta'\rangle|$. There are two elements $i < j$ such that $(i)\beta' = (j)\beta'$. We define $d = j-i$. It can be easily seen that α' and β' generate at most the transformations specified in Definition 16. Therefore we conclude that $|\langle\alpha',\beta'\rangle| \leqslant |V_n|$. □

Observe, that because of Theorem 22, Lemma 23 implies that there exists a natural number N such that for every $n \geqslant N$ there exist k and ℓ with $n = k+\ell$ such that $|\langle\alpha,\beta\rangle| < |U_{k,\ell}|$, for every $\alpha \in S_n$ such that α consists of a single cycle and $\beta \in T_n \setminus S_n$.

5.2. Semigroup size—two permutations or two non-bijective mappings

In this subsection, we show that two permutations or two non-bijective transformation are inferior in size to an $U_{k,\ell}$ semigroup, for large enough $n = k+\ell$. Here it turns out, that

the semigroup V_n is very helpful in both cases. If we take two permutations as generators, then we can at most obtain the symmetric group S_n.

Lemma 24 (*Two permutations*). *Let $n \geqslant 2$. If both α and β are in S_n, then $|\langle \alpha, \beta \rangle| < |V_n|$.*

Proof. Obviously, for permutations α and β we have $|\langle \alpha, \beta \rangle| \leqslant n!$. In order to prove the stated inequality it suffices to show that $n! < |V_n^1|$. We determine the number of transformations in V_n^1, the image of which is the set $\{1, \ldots, n-1\}$. First, there are n possibilities to choose the pair $(j, j +_n 1)$ of indices that should be mapped to the same value. And, second, there are $(n-1)!$ possibilities to assign an image to each element of the kernel. In total, there are already $n!$ transformations of this kind. Since V_n^1 contains additional elements, e.g., permutations, it follows that $n! < |V_n^1|$. Hence $|\langle \alpha, \beta \rangle| < |V_n|$. □

Next we consider the case of two non-bijective transformations.

Lemma 25 (*Two non-bijective transformations*). *Let $n \geqslant 2$. If both α and β in $T_n \setminus S_n$, then $|\langle \alpha, \beta \rangle| < |V_n|$.*

Proof. Since α and β are both non-bijective, there are indices $j_1 < k_1$ and $j_2 < k_2$ such that $(j_1)\alpha = (k_1)\alpha$ and $(j_2)\beta = (k_2)\beta$. In this case we can construct a permutation π such that $\pi\alpha\pi^{-1}$, $\pi\beta\pi^{-1}$, and all transformations generated by them satisfy the second part of Definition 16 for $d = 1$. In this way we show that the set $\langle \pi\alpha\pi^{-1}, \pi\beta\pi^{-1} \rangle$, and therefore also $\langle \alpha, \beta \rangle$ which is isomorphic, has less elements than V_n^1, since at least the permutations are missing.

In order to construct π we have to distinguish several cases: Whenever all indices j_1, k_1, j_2, k_2 are pairwise different, we choose a permutation π such that $(1)\pi = j_1$, $(2)\pi = k_1$, $(3)\pi = j_2$, $(4)\pi = k_2$. In this case $\pi\alpha\pi^{-1}$ merges the indices 1 and 2, whereas $\pi\beta\pi^{-1}$ merges the indices 3 and 4. All other cases can be treated similarly. For instance if $k_1 = j_2$ we set $(1)\pi = j_1$, $(2)\pi = k_1 = j_2$, $(3)\pi = k_2$, and if $j_1 = j_2$ and $k_1 \neq k_2$ we set $(1)\pi = k_1$, $(2)\pi = j_1 = j_2$, $(3)\pi = k_2$. □

5.3. Semigroup size—two and more cycles

Finally, we consider the case where one of the generators is a permutation α consisting of two or more cycles and the other is a non-bijective transformation. In this case we distinguish two sub-cases, according to whether the non-bijective transformation β merges elements from the same or different cycles of α. We start our investigation with the case where there are i and j such that $(i)\beta = (j)\beta$ and both are located within the same cycle of α.

Lemma 26 (An arbitrary permutation and a non-bijective mapping merging elements from the same cycle). *For every $n \geqslant 7$ the following holds*: *Let $\alpha, \beta \in T_n$ be transformations where α is a permutation. Furthermore, let β be a non-bijective transformation such that $(i)\beta = (j)\beta$ and both i and j are located in the same cycle of α. Then there exist $k \neq 1$ and ℓ with $n = k + \ell$, $k < \ell$ and $\gcd\{k, \ell\} = 1$ such that $|\langle \alpha, \beta \rangle| < |U_{k,\ell}|$.*

Proof. We assume that i and j are located in the same cycle of length m with distance d w.r.t. their location within the cycle. We can assume that d divides m, otherwise we can find an isomorphic semigroup where this is the case, following the ideas of the proof of Lemma 17.

With a similar argument as in the proof of Theorem 20 we can deduce that the semigroup generated by α and β contains at most some permutations and the invalid colourings of a graph G, where G consists of d circles of length m/d and $n-m$ isolated nodes. The number of valid colourings of such a graph equals

$$((n-1)^{\frac{m}{d}} + (-1)^{\frac{m}{d}}(n-1))^d n^{n-m}.$$

Therefore we conclude $|\langle\alpha,\beta\rangle| \leqslant n^n + n! - \left((n-1)^{\frac{m}{d}} + (-1)^{\frac{m}{d}}(n-1)\right)^d n^{n-m}$. Similar reasoning as in the proof of Theorem 21 shows that

$$\begin{aligned}
|V| &\leqslant n^n + n! - \left((n-1)^{\frac{m}{d}} + (-1)^{\frac{m}{d}}(n-1)\right)^d n^{n-m} \\
&\leqslant n^n + n! - \left((n-1)^3 - (n-1)\right)^{\frac{m}{3}} n^{n-m} \\
&= n^n + n! - n^n \left(\frac{n(n-1)(n-2)}{n^3}\right)^{\frac{m}{3}} \\
&\leqslant n^n + n! - n^n \left(\frac{n(n-1)(n-2)}{n^3}\right)^{\frac{n}{3}} \\
&= n^n + n! - (n(n-1)(n-2))^{\frac{n}{3}}.
\end{aligned}$$

By using Stirling's approximation we obtain

$$|V| \leqslant n^n + \sqrt{2\pi n}\left(\frac{n}{\mathrm{e}}\right)^n \mathrm{e}^{\frac{1}{12}} - (n(n-1)(n-2))^{\frac{n}{3}}.$$

Furthermore, from Theorem 12 and Lemma 11 it follows that we can choose k, ℓ satisfying the above properties such that:

$$|U_{k,\ell}| \geqslant n^n \left(1 - \frac{2}{\sqrt{n}}\right).$$

The upper bound for $|V|$ is smaller than the lower bound for $|U_{k,\ell}|$ whenever

$$\frac{2}{\sqrt{n}} < \underbrace{\left(\frac{(n-1)(n-2)}{n^2}\right)^{\frac{n}{3}}}_{A(n)} - \underbrace{\sqrt{2\pi n}\left(\frac{1}{\mathrm{e}}\right)^n \mathrm{e}^{\frac{1}{12}}}_{B(n)}.$$

The function $A(n)$ is monotone and converges to $\frac{1}{\mathrm{e}} \approx 0.36788$ while the function $B(n)$ is antitone and converges to 0. For $n \geqslant 20$ we have $A(n) > 0.358$ and $B(n) < 10^{-7}$, and therefore $A(n) - B(n) > 0.35 =: c$.

We solve the equation $\frac{2}{\sqrt{n}} < c$, which is satisfied whenever $n > \left(\frac{2}{c}\right)^2 \approx 32.65306$, i.e., whenever $n \geqslant 33$.

The remaining cases for $7 \leqslant n \leqslant 32$ have been checked with the help of computer algebra software. To this end we have verified that $|V| \leqslant |U_{k,\ell}|$, for some k and ℓ, where the upper bound for $|V|$ from Lemma 26 and the exact value of $|U_{k,\ell}|$ from Theorem 10 was used. It turned out that $|V_n|$ is maximal w.r.t. size for all V semigroups.

Hence, this shows that for every $n \geqslant 7$ the size of the semigroups on n elements under consideration is strictly less than the size of $U_{k,\ell}$, for suitable $k \neq 1$ and ℓ with $n = k + \ell$ and $\gcd\{k, \ell\} = 1$. □

Finally, we consider the case where the non-bijective transformation β merges elements from different cycles of the permutation α. Observe, that it might be the case the $U_{k,\ell}$ semigroup in the lemma stated below cannot be generated with two generators, since k might be equal to 1 and k, ℓ are not necessarily coprime.

Lemma 27 (A permutation with two or more cycles and a non-bijective mapping merging elements from different cycles). *Let $\alpha, \beta \in T_n$ be transformations where α is a permutation consisting of $m \geqslant 2$ cycles. Furthermore let β be a non-bijective transformation such that $(i)\beta = (j)\beta$ and i and j are located in different cycles of α. Then there exist k and ℓ with $n = k + \ell$ such that $|\langle \alpha, \beta \rangle| \leqslant |U_{k,\ell}|$.*

Proof. We first define the following auxiliary notion: Let c and c' be two sequences of numbers which contain exactly the elements of a two-cycle permutation $\pi \in S_n$ in the correct order. Note that for a given π the sequences c and c' are not unique, since the first element of a cycle is not fixed. Specifically, the elements of c and c' are pairwise different, and the underlying sets form a partition of $\{1, \ldots, n\}$. Given, two sequences c and c', we denote the corresponding permutation by $\pi(c, c')$.

By $U(c, c')$ be denote that set of all transformations γ satisfying:

(1) γ is a multiple of $\pi(c, c')$ or
(2) there exists an index i contained in c and an index j contained in c' such that $(i)\gamma = (j)\gamma$ and there exists an index h contained in c' such that $h \notin img(\gamma)$.

It is easy to see that $U(c, c')$ is isomorphic to $U_{|c|,|c'|}$. We define $U := \langle \alpha, \beta \rangle$ and show that $|U| \leqslant |U(c, c')|$ for suitable sequences c and c'.

Now assume that the m cycles in α have lengths $k_1, \ldots, k_m$, i.e., $n = \sum_{i=1}^{m} k_i$. Furthermore the (non-unique) sequences of elements of the m cycles are denoted by $c_1, \ldots, c_m$ and $|c_i| = k_i$. Without loss of generality we may assume that β merges elements of the first two cycles c_1 and c_2. We now consider the following two cases according to which element is missing in the image of β:

(1) There is an element h which is not contained in the image of β and moreover, h is not located in the first two cycles of α. So let us assume that it is located in the third cycle c_3. We concatenate the sequences representing cycles and obtain $c'_1 = c_2 c_4 c_5 \ldots c_m$, $c'_2 = c_1 c_3$, $k = k_2 + \sum_{i=4}^{m} k_i$, and $\ell = k_1 + k_3$. From the considerations above it is clear that $|U(c'_1, c'_2)| = |U_{k,\ell}|$.

   Now let us compare the sizes of U and $U(c'_1, c'_2)$. First, consider only the non-bijective transformations. Let $\gamma \in U$ be a transformation which is not a permutation. Since β merges elements of c_1 and c_2 there must be indices i (contained in c_1) and j (contained in c_2) such that $(i)\gamma = (j)\gamma$. Furthermore, since there is an element h contained in c_3

missing in the image of γ. So, clearly, γ is an element of $U(c'_1, c'_2)$. We now consider permutations. The semigroup U may contain more permutations than $U(c'_1, c'_2)$. In the worst case, if $\gcd\{k_i, k_j\} = 1$ for all pairs of cycle lengths with $i \neq j$, then U contains $\prod_{i=1}^{m} k_i$ permutations, whereas $U(c'_1, c'_2)$ contains only $k\ell$ permutations, which might be less. We show that this shortcoming is already compensated by the number of transformations with image size $n-1$.

The semigroup U contains $k_1k_2k_3(n-1)!$ mappings with image size $n-1$. We first choose the two elements which are in the same kernel equivalence class, for which there are k_1k_2 possibilities, then we choose the element of the image that is missing, for which there are k_3 possibilities, and finally we distribute the $n-1$ elements of the image onto the kernel equivalence classes. In the same way we can show that there are $k\ell^2(n-1)!$ transformations with image size $n-1$ in U'. Now define $k' = \sum_{i=4}^{m} k_i$ and observe, that k' might be equal to 0. Then we conclude that

$$\begin{aligned} k\ell^2 - k_1k_2k_3 &= (k_2 + k')(k_1 + k_3)^2 - k_1k_2k_3 \\ &= (k_2 + k')(k_1^2 + 2k_1k_3 + k_3^2) - k_1k_2k_3 \\ &= k_1^2k_2 + k_1k_2k_3 + k_2k_3^2 + k'k_1^2 + 2k'k_1k_3 + k'k_3^2 \\ &\geqslant k_1 + k_2 + k_3 + k' = n. \end{aligned}$$

Therefore $U(c'_1, c'_2)$ contains at least $n!$ more transformations of image size $n-1$ than U. This makes up for the missing permutations, since there are at most $n!$ of them.

(2) The missing element h of the image of β is located in one of the first two cycles. Let us assume that it is located in c_2. If α contains exactly two cycles we are done, since $\langle\alpha, \beta\rangle$ is isomorphic to some $U(c_1, c_2)$. Otherwise permutation α contains at least three cycles and we define $c'_1 = c_1$, $c'_2 = c_2 \dots c_m$. We set $k = k_1$ and $\ell = \sum_{i=2}^{m} k_i$. With the same argument as above, we can conclude that the non-bijective transformations of U are contained in $U(c'_1, c'_2)$. We again have to show that there are sufficiently many transformations of image size $n-1$ in order to make up for the missing permutations of $U(c'_1, c'_2)$. Now the semigroup U contains $k_1k_2^2(n-1)!$ transformations with image size $n-1$, whereas U' has $k\ell^2(n-1)!$ transformations with image size $n-1$. Define $k' = \sum_{i=3}^{m} k_i$. Then we obtain

$$\begin{aligned} k\ell^2 - k_1k_2^2 &= k_1(k_2 + k')^2 - k_1k_2^2 \\ &= k_1(k_2^2 + 2k_2k' + (k')^2) - k_1k_2^2 \\ &= k_1k_2^2 + 2k_1k_2k' + k_1(k')^2 - k_1k_2^2 \\ &= 2k_1k_2k' + k_1(k')^2 \geqslant k_1 + k_2 + k' = n \end{aligned}$$

since $k' > 0$. Therefore $U(c'_1, c'_2)$ contains at least $n!$ more transformations of image size $n-1$ than U. This makes up for the missing permutations, since there are at most $n!$ of them.

This completes our proof and shows that $|\langle\alpha, \beta\rangle| \leqslant |U(c'_1, c'_2)| = |U_{k,\ell}|$ for suitable k and ℓ with $n = k + \ell$. □

Lemma 27 is still insufficient for our purposes, since it is not guaranteed that the semigroup $U_{k,\ell}$ above can be generated by two generators. If we demand that n is a prime number, then we can be sure that k and ℓ are coprime. So in this case, whenever $k \neq 1$, the semigroup

$U_{k,\ell}$ can in fact be generated by two transformations. We will now show that $U_{1,\ell}$ is smaller in size than one of the semigroups we have already considered.

Lemma 28. *Let $n = 1 + \ell$. Then it holds that $|U_{1,\ell}| < |V_n|$.*

Proof. Let us first estimate the number of elements in $U_{1,\ell}$. According to Theorem 10 $|U_{1,\ell}|$ equals $n^n + \ell$ minus the number of transformations that correspond to valid colourings of the complete bipartite graph $K_{1,\ell}$ or that use all colours out of $\{2, \ldots, n\}$. There are $n(n-1)^{n-1}$ valid colourings of $K_{1,\ell}$. Hence we can conclude that

$$|U_{1,\ell}| \leqslant n^n + n - 1 - n(n-1)^{n-1}.$$

On the other hand

$$|V_n| \geqslant n^n + 1 - (n-1)^n$$

by Theorem 21. Thus, in order to show that $|U_{1,\ell}| < |V_n|$, it is sufficient to prove

$$n^n + (n-1) - n(n-1)^{n-1} < n^n + 1 - (n-1)^n,$$

which amounts to showing

$$n - 2 < (n-1)^{n-1},$$

which obviously holds for all n. □

Finally, let us come back to our main Theorem 15, namely that a semigroup of maximal size has $|U_{k,\ell}|$ elements, for some k and ℓ, whenever $n = k + \ell$ is a prime greater or equal than 7.

Proof (Proof of Theorem 15). Let $\alpha, \beta \in T_n$ be two arbitrary transformations. We consider the following cases and show for each of them that $|\langle \alpha, \beta \rangle| \leqslant |U_{k,\ell}|$, where $k \neq 1$ and $k < \ell$. Since n is prime, k and ℓ are trivially coprime. Hence, by Proposition 8, the semigroup $U_{k,\ell}$ can be generated by two transformations.

(1) One of the two transformations is a permutation (without loss of generality we assume this to be α) and the other a transformation (β) merging elements of the same cycle. According to Lemma 26 it holds that $|\langle \alpha, \beta \rangle| \leqslant |U_{k,\ell}|$ where $k \neq 1$ and $k < \ell$.
(2) Both transformations are permutations or both transformations are non-bijective. From Lemmas 24 and 25 it follows that in this case $|\langle \alpha, \beta \rangle| < |V_n|$. By Theorem 18 the semigroup V_n is generated by two transformations which are instances of the previous case (α is a permutation consisting of a single cycle and β is non-bijective). Thus it holds that $|\langle \alpha, \beta \rangle| \leqslant |U_{k,\ell}|$ where $k \neq 1$ and $k < \ell$.
(3) One of the two transformations is a permutation (without loss of generality we assume this to be α) and the other a transformation (β) merging elements of different cycles. By Lemma 27 we know that there exist indices k, ℓ such that $|\langle \alpha, \beta \rangle| \leqslant |U_{k,\ell}|$. Whenever $k \neq 1$ and $k < \ell$ we are done. Otherwise we set $k' = \ell$, $\ell' = k$ whenever $k > \ell$ and $k' = k$, $\ell' = \ell$ otherwise. Obviously $k' < \ell'$. From Theorem 10 it follows that $|U_{k,\ell}| \leqslant |U_{k',\ell'}|$. Now if $k' \neq 1$, we can stop. However, if $k' = 1$, then, according to

Table 1
Sizes of some investigated semigroups

n	$\lvert S_n\rvert = n!$			$\lvert U_{k,\ell}\rvert$		$\lvert V_n^d\rvert$	$\max(n)$	$\lvert T_n\rvert = n^n$
		k	l		d			
3	6	1	2	13	1	24	24	27
4	24	1	3	133	1	176	176	256
					2	116		
5	120	2	3	1857	1	2110	2110	3125
		1	4	1753				
6	720	1	5	27311	1	31032	32262	46656
					2	32262		
					3	19662		
7	5040	3	4	607285	1	543620	610871	823543
		2	5	610871				
		1	6	492637				
8	40320	3	5	13492007	1	11012416	13492007 (?)	16777216
		1	7	10153599	2	10978760		
					4	6942728		
9	362880	4	5	323534045	1	253202778	323534045 (?)	387420489
		2	7	306605039	3	259396434		
		1	8	236102993				
10	3628800	3	7	8678434171	1	6513215600	8678434171 (?)	10000000000
		1	9	6122529199	2	6514278410		
					5	4095100010		
11	39916800	5	6	256163207631	1	185311670632	258206892349	285311670611
		4	7	258206892349				
		3	8	251856907425				
		2	9	231326367879				
		1	10	175275382621				

Lemma 28 it holds that $|\langle\alpha,\beta\rangle| \leqslant |U_{1,\ell'}| < |V_n|$ and from the first case we obtain again the desired result. □

Concluding this section, we present in Table 1 some computed values on the size of some of the semigroups investigated in this paper.

The number $\max(n)$ denotes the size of the maximal transformation semigroup with two generators, which might not coincide with the size of some $U_{k,\ell}$, especially for small n. A table entry with a question mark indicates that the precise value is not known and thus is a conjecture. Also note that semigroups of the form $U_{1,\ell}$ can in general not be generated by two generators. Up to $n = 6$, there is always a group of the form V_n^d which is maximal in size. For instance, the following mappings α and β in T_n generate size maximal semigroups for the value n, where $2 \leqslant n \leqslant 6$:

- $n = 2$:

$$\alpha = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \quad \text{and} \quad \beta = \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}$$

- $n = 3$:

$$\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \text{and} \quad \beta = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 1 & 3 \end{pmatrix}$$

- $n = 4$:

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \quad \text{and} \quad \beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 1 & 4 & 3 \end{pmatrix}$$

- $n = 5$:

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix} \quad \text{and} \quad \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 1 & 4 & 5 & 3 \end{pmatrix}$$

- $n = 6$:

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 5 & 6 & 1 \end{pmatrix} \quad \text{and} \quad \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 1 & 5 & 6 & 2 \end{pmatrix}.$$

All these cases were verified by brute force search using the Groups, Algorithms and Programming (GAP) system.

Coming back to our original question, which was to study the sizes of syntactic monoids, we have now made significant progress in computing the maximal sizes of syntactic monoids for regular languages over a binary alphabet accepted by minimal deterministic automata with n states. The numbers (without question mark) given in column $\max(n)$ in Table 1 are also the maximal sizes of the corresponding syntactic monoids. Furthermore, we have answered the question for n prime. This follows almost directly from Theorems 9, 15, and 19. Both semigroups—V_n^d and $U_{k,\ell}$—contain the identity and are thus monoids. Some of the semigroups we have considered do not contain the identity element (see Lemma 25), but in these cases it is not possible to reach the maximal size, even by adding another element.

6. Conclusion

We have shown that for prime n, such that $n \geqslant 7$, the semigroup generated by two generators with maximal size can be characterized in a very nice and accurate way. The cases $2 \leqslant n \leqslant 6$ are not treated explicitly, but we were able to show that in all these cases the semigroup V_n contains a maximal number of elements. All were done by brute force search using the GAP system. Moreover, we have completely classified the case when one generator is a permutation consisting of a single cycle.

Nevertheless, some questions remain unanswered. First of all, what about the case when $n \geqslant 7$ is not a prime number? We conjecture that Theorem 5 also holds in this case, but we have no proof yet. Also, the question how to choose k and ℓ properly remains unanswered. In order to maximize the size of $U_{k,\ell}$ one has to minimize the number of valid colourings, which is minimal if k and ℓ are close to $n/2$. This clashes with the observation that the cycle α from which an element in the image of β is missing should be as large as possible. Nevertheless, to maximize the size of $U_{k,\ell}$ we conjecture that for large enough n both k and ℓ are as close to $n/2$ as the condition that k and ℓ should be coprime allows. Again a proof of

this statement is still missing. In order to understand the very nature of the question better, a step towards its solution would be to show that the sequence $|U_{k,\ell}|$ for fixed $n = k + \ell$ and varying k is unimodal.

Acknowledgements

Thanks to J.M. Howie and J.-E. Pin for some fruitful discussions on the subject. Also thanks to Rob Johnson, and Paul Pollack, and John Robertson for their help in managing the essential step in the proof of Lemma 17.

References

[1] J.-M. Champarnaud, D. Maurel, D. Ziadi (Eds.), Proc. of the Third Internat. Workshop on Implementing Automata, Lecture Notes in Computer Science, Vol. 1660, Rouen, France, Springer, Verlag, September 1998.
[2] W. Feller, Stirling's formula, in: An Introduction to Probability Theory and Its Applications, 3rd Edition, Vol. 1, Wiley, New York, 1968, pp. 50–53 (chapter 2.9).
[3] G.H. Hardy, E.M. Wright, An Introduction to the Theory of Numbers, 5th Edition, Clarendon, Oxford, 1979.
[4] J.M. Howie, An Introduction to Semigroup Theory, L.M.S. Monographs, Vol. 7, Academic Press, New York, 1976.
[5] S.C. Kleene, Representation of events in nerve nets and finite automata, in: C.E. Shannon, J. McCarthy (Eds.), Automata Studies, Annals of Mathematics Studies, Vol. 34, Princeton University Press, Princeton, NJ, 1956, pp. 2–42.
[6] B. Krawetz, J. Lawrence, J. Shallit, State complexity and the monoid of transformations of a finite set, http://arxiv.org/abs/math.gr/0306416, June 2003.
[7] E. Landau, Über die Maximalordnung der Permutationen gegebenen Grades, Arch. Math. Phys. 3 (1903) 92–103.
[8] F. Lazebnik, New upper bounds for the greatest number of proper vertex colorings of a (V, W)-graph, J. Graph Theory 14 (1) (1990) 25–29.
[9] J.-L. Nicolas, Sur l'ordre maximum d'un élément dans le groupe s_n des permutations, Acta Arith. 14 (1968) 315–332.
[10] J.-L. Nicolas, Ordre maximum d'un élément du groupe de permutations et highly composite numbers, Bull. Math. Soc. France 97 (1969) 129–191.
[11] S. Piccard, Sur les bases du groupe symétrique et les couples de substitutions qui engendrent un groupe régulier, Librairie Vuibert, Paris, 1946.
[12] J.-E. Pin, Varieties of Formal Languages, North Oxford, 1986.
[13] R.C. Read, An introduction to chromatic polynomial, J. Combin. Theory 4 (1968) 52–71.
[14] H. Robbins, A remark of Stirling's formula, Amer. Math. Monthly 62 (1955) 26–29.
[15] A. Salomaa, On the composition of functions of several variables ranging over a finite set, Ann. Univ. Turkuensis 41 (Series AI) (1960).
[16] M. Szalay, On the maximal order in S_n and S_n^*, Acta Arith. 37 (1980) 321–331.
[17] D. Wood, S. Yu (Eds.), Automata implementation, Proc. of the Second Internat. Workshop on Implementing Automata, Lecture Notes in Computer Science, Vol. 1436, London, Canada, Springer, Berlin, September 1997.