# On Deterministic Finite Automata and Syntactic Monoid Size, Continued

Markus Holzer and Barbara König

Institut für Informatik, Technische Universität München,
Boltzmannstraße 3, D-85748 Garching bei München, Germany
email: {holzer,koenigb}@informatik.tu-muenchen.de

**Abstract.** We continue our investigation on the relationship between regular languages and syntactic monoid size. In this paper we confirm the conjecture on two generator transformation semigroups. We show that for every prime $n \geq 7$ there exist natural numbers $k$ and $\ell$ with $n = k + \ell$ such that the semigroup $U_{k,\ell}$ is maximal w.r.t. its size among all (transformation) semigroups which can be generated with two generators. This significantly tightens the bound on the syntactic monoid size of languages accepted by $n$-state deterministic finite automata with binary input alphabet. As a by-product of our investigations we are able to 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.

## 1 Introduction

Finite automata are used in several applications and implementations in software engineering, programming languages and other practical areas in computer science. They are one of the first and most intensely investigated computational models. Since regular languages have many representations in the world of finite automata it is natural to investigate the succinctness of their different representations. Recently, the size of the syntactic monoid as a natural measure of descriptive complexity for regular languages was proposed in [3] and studied in detail. Recall, that the syntactic monoid of a language $L$ 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 $\Sigma^*$ 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 particular, the size of transformation monoids of $n$-state (minimal) deterministic finite automata was investigated in [3]. In most cases tight upper bounds on the syntactic monoid size were obtained. It was proven 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, 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 $\ell$ close to $\frac{n}{2}$, and a trivial non-matching upper bound of $n^n - n! + g(n)$, where $g(n)$ denotes Landau's function [5–7], which gives the maximal order of all permutations in $S_n$, for the size of the syntactic monoid of a language accepted by an $n$-state deterministic finite automaton was given. 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, and is the starting point of our investigations.

In this paper we tighten the bound on the syntactic monoid size on two generators, confirming the conjecture, that for every prime $n \geq 7$ there exist natural numbers $k$ and $\ell$ with $n = k + \ell$ such that the semigroup $U_{k,\ell}$ as introduced in [3] is maximal w.r.t. its size among all (transformation) semigroups which can be generated with two generators. Since $U_{k,\ell}$, for suitable $k$ and $\ell$ is a syntactic monoid, this sharpens the above given bound for syntactic monoids induced by $n$-state deterministic finite automata with binary input alphabet. In order to show that there is no larger subsemigroup 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.

In the forthcoming we will show that for a large enough $n$ the maximal subsemigroup is of type (3) and that whenever $n$ is *prime* the semigroup is isomorphic to some $U_{k,\ell}$. 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. Then in Section 3 we start our investigations with 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 deals with the most complicated case, where the permutation contains two or more cycles, and Section 6 is devoted to the main result of this paper, on the size maximality of the semigroup under consideration. 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] and [9]. 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., first $\alpha$, then $\beta$. 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 $\alpha$ in $T(E)$ is defined as $img(\alpha) = \{\, (i)\alpha \mid i \in E \,\}$ and the kernel of $\alpha$ 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 $T_n$.

The semigroup we are interested in is defined below and was introduced in [3] in order to study the relation between $n$-state deterministic finite automata with binary input alphabet and the size of syntactic monoids.

**Definition 1.** *Let $n \geq 2$ such that $n = k + \ell$ for some natural numbers $k$ and $\ell$. 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 the semigroup $U_{k,\ell}$ as a subset of $T_n$ as follows: A transformation $\gamma$ 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 $\gamma$ 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 $h \notin img(\gamma)$.*

Observe, that it is always better to choose the element $h$ which is missing in the image of $\gamma$ from the larger cycle of $\alpha$ since this yields a larger semigroup $U_{k,\ell}$. Therefore we can safely assume that $k \leq \ell$.

In [3] it was shown that if $\gcd\{k, \ell\} = 1$, then the semigroup $U_{k,\ell}$ can be generated by two generators only. Moreover, in this case, $U_{k,\ell}$ is the syntactic monoid of a language accepted by an $n$-state deterministic finite automaton, where $n = k + \ell$.

Finally, we need some additional notation. If $A$ is an arbitrary non-empty subset of a semigroup $S$, then the family of subsemigroups of $S$ containing $A$ is non-empty, since $S$ itself is one such semigroup; hence the intersection of the family is a subsemigroup of $S$ containing $A$. We denote it by $\langle A\rangle$. It is characterized within the set of subsemigroups of $S$ by the properties: (1) $A \subseteq \langle A\rangle$ and (2) if $U$ is a subsemigroup 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 $\langle \alpha, \beta\rangle$.

## 3 Semigroup Size—The Single Cycle Case

In this section 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 section 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 2.** *Let $n \geq 2$ and $1 \leq d < n$. 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 $\gamma$ 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 $n$.*

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 $\beta$ which maps two elements $1 \leq i < j \leq n$ onto the same image one can infer that every transformation $\gamma$ generated by $\alpha$ and $\beta$ is either a multiple of $\alpha$ or maps two elements of distance $d := j - i$ to the same value. Next 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. We omit the proof of the following lemma.

**Lemma 1.** *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 $d = \gcd\{n, d'\}$.*

Before we can prove that $V_n^d$ can be generated by two elements of $T_n$ we need a result, which constitutes how to find a complete basis for the symmetric group $S_n$. The result given below was shown in [8].

**Theorem 1.** *Given a non-identical element $\alpha$ in $S_n$, then there exists $\beta$ such both generate the symmetric group $S_n$, provided that it is not the case that $n = 4$ and $\alpha$ 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 the semigroup $V_n^d$. Due to the lack of space we omit the proof of the following theorem, which is heavily based on Theorem 1.

**Theorem 2.** *Let $n \geq 2$ and $1 \leq d < n$. 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 $\beta$ of kernel size $n - 1$.*[1]

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.

[1] Observe, that 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 $L(A)$. Since this statement can be easily seen, we omit its proof.

**Theorem 3.** *Let $n \geq 2$ and $1 \leq d < n$ with $d \mid n$. 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 subsemigroup $V_n^d$ can be obtained from $T_n$ by removing all transformations not satisfying the second part of Definition 2 and by adding the $n$ multiples of $\alpha$ afterwards. The number of the former transformations can be determined as follows: Assume that a graph $G$ has nodes $V = \{1, \dots, n\}$ where a circle $C_k$ consists of nodes $\{k, k+d, \dots, k+id, \dots, k+n-d\}$, for $1 \leq k \leq d$. Then one can easily verify that the colourings of $G$ are exactly the transformations which do not satisfy the second part of Definition 2. The number of colourings of a graph $G$ with $k$ colours is described by its chromatic polynomial, see, e.g. [10]. Since the chromatic polynomial of a circle $C_n$ with $n$ nodes is $(k-1)^n + (-1)^n(k-1)$ 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 4.** *The size of $V_n^d$ is maximal whenever*

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

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

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

*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

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

The additional index $k$ is present for later use—see Lemma 5. For now we assume that $k = n$.

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

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

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

So if there exist divisors $d'$ such that $\frac{n}{d'}$ is odd, the semigroup $V_n^d$ is maximal w.r.t. its size 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 $1 \leq d < n$. From our previous investigations one can infer that the following inequalities hold:

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

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

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

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

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

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

**Theorem 5.** *There exists a natural number $N$ such that for every $n \geq N$, there exist $k$ and $\ell$ 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 Theorem 4 and a result from [3], which state that

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

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 2 (A cycle and a non-bijective transformation).** *If $\alpha \in S_n$ such that $\alpha$ consists of a single cycle and $\beta \in T_n \backslash S_n$, then $|\langle \alpha, \beta \rangle| \leq |V_n|$.*

*Proof.* Since the permutation $\alpha$ consists of a single cycle, there is a permutation $\pi$ 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 $\pi$ 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 $\alpha'$ and $\beta'$ generate at most the transformations specified in Definition 2. Therefore we conclude that $|\langle\alpha', \beta'\rangle| \leq |V_n|$. □

Observe, that because of Theorem 5, Lemma 2 implies that there exists a natural number $N$ such that for every $n \geq N$ there exist $k$ and $\ell$ with $n = k + \ell$ such that $|\langle\alpha, \beta\rangle| < |U_{k,\ell}|$, for every $\alpha \in S_n$ such that $\alpha$ consists of a single cycle and $\beta \in T_n \backslash S_n$.

## 4 Semigroup Size—Two Permutations or Non-Bijective Mappings

In this section 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 3 (Two permutations).** *Let $n \geq 2$. If $\alpha, \beta \in S_n$, then $|\langle\alpha, \beta\rangle| < |V_n|$.*

*Sketch of Proof.* Obviously, for permutations $\alpha$ and $\beta$ we have $|\langle\alpha, \beta\rangle| \leq n!$. In order to prove the stated inequality it suffices to show that $n! < |V_n^1|$. The details are left to the reader. □

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

**Lemma 4 (Two non-bijective transformations).** *Let $n \geq 2$. If both $\alpha$ and $\beta$ in $T_n \setminus S_n$, then $|\langle\alpha, \beta\rangle| < |V_n|$.*

*Proof.* Since $\alpha$ and $\beta$ 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 $\pi$ such that $(i_1)\pi = j_1$, $(i_1 +_n 1)\pi = k_1$ for some index $i_1$ and $(i_2)\pi = j_2$, $(i_2 +_n 1)\pi = k_2$ for some index $i_2$. If $j_1 = j_2$, then it is the case that $i_1 = i_2$, similarly if $j_1 = k_2$, then $i_1 = i_2 +_n 1$, etc. This means that all transformations generated by $\pi\alpha\pi^{-1}$ and $\pi\beta\pi^{-1}$ satisfy the second part of Definition 2 for $d = 1$. According to Definition 2 the set $\langle\pi\alpha\pi^{-1}, \pi\beta\pi^{-1}\rangle$, and therefore also $\langle\alpha, \beta\rangle$ which is isomorphic, have less elements than $V_n^1$, since at least the permutations are missing. Thus, the stated claim follows. □

## 5 Semigroup Size—Two and More Cycles

Finally we consider the case where one of the generators is a permutation $\alpha$ 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 $\beta$ merges elements from the same or different cycles of $\alpha$. 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 $\alpha$.

**Lemma 5 (An arbitrary permutation and a non-bijective mapping merging elements from the same cycle).** *There exists a natural number $N$ such that for every $n \geq N$ the following holds: Let $\alpha, \beta \in T_n$ be transformations where $\alpha$ is a permutation. Furthermore let $\beta$ be a non-bijective transformation such that $(i)\beta = (j)\beta$ and both $i$ and $j$ are located in the same cycle of $\alpha$. Then there exist $k$ and $\ell$ with $n = k + \ell$ 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 1.

With a similar argument as in the proof of Theorem 3 we can deduce that the semigroup generated by $\alpha$ and $\beta$ contains at most some permutations and the invalid colourings of a graph $G$, where $G$ consists of $d$ circles of length $\frac{m}{d}$ 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 $|\langle \alpha, \beta \rangle| \leq n^n + n! - \left((n-1)^{\frac{m}{d}} + (-1)^{\frac{m}{d}}(n-1)\right)^d n^{n-m}$. Similar reasoning as in the proof of Theorem 4 shows that

$$n^n + n! - \left((n-1)^{\frac{m}{d}} + (-1)^{\frac{m}{d}}(n-1)\right)^d n^{n-m} \leq n^n + n! - n^n \left(\frac{(n-1)(n-2)}{n^2}\right)^{\frac{n}{3}}$$

and

$$\lim_{n\to\infty} \frac{n^n + n! - n^n \left(\frac{(n-1)(n-2)}{n^2}\right)^{\frac{n}{3}}}{n^n} = 1 - \frac{1}{e}.$$

Hence, a similar asymptotic argument as in the proof of Theorem 5 shows that there is a natural number $N$ such for every $n \geq N$ the size of the semigroups on $n$ elements under consideration is strictly less than the size of $U_{k,\ell}$, for suitable $k$ and $\ell$ with $n = k + \ell$. □

Finally, we consider the case where the non-bijective transformation $\beta$ merges elements from different cycles of the permutation $\alpha$. In the remainder of this section we assume $n = k + \ell$ to be a prime number. The reasons for this assumption is that $k$ and $\ell$ are always coprime, which guarantees that $U_{k,\ell}$ can be generated by two generators only.

**Lemma 6 (A permutation with two or more cycles and a non-bijective mapping merging elements from different cycles).** *Let $n$ be a prime number and let $\alpha, \beta \in T_n$ be transformations where $\alpha$ is a permutation consisting of $m \geq 2$ cycles. Furthermore let $\beta$ be a non-bijective transformation such that $(i)\beta = (j)\beta$ and $i$ and $j$ are located in different cycles of $\alpha$. Then there exist $k$ and $\ell$ with $n = k + \ell$ such that $|\langle \alpha, \beta \rangle| \leq |U_{k,\ell}|$.*

*Proof.* We define $U := \langle \alpha, \beta \rangle$ and show that $|U| \leq |U'|$, where $U'$ is generated by a two-cycle permutation $\alpha'$ and a non-bijective mapping $\beta'$ that merges elements of different cycles, as described below in detail.

Now assume that the $m$ cycles in $\alpha$ have lengths $k_1, \ldots, k_m$, i.e., $n = \sum_{i=1}^{m} k_i$. Furthermore the sets of elements of the $m$ cycles are denotes by $C_1, \ldots, C_m$ and $|C_i| = k_i$. Without loss of generality we may assume that $\beta$ 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 $\beta$:

1. There is an element $h$ which is not contained in the image of $\beta$ and moreover, $h$ is not located in the first two cycles of $\alpha$. So let us assume that it is located in the third cycle $C_3$. Let $\alpha'$ be a permutation with two cycles, where the elements of the first cycle are $C'_1 = C_2 \cup \bigcup_{i=4}^{m} C_i$ and the elements of the second cycle are $C'_2 = C_1 \cup C_3$. In the cycles these elements can be arranged in an arbitrary way. We now set $k = k_2 + \sum_{i=4}^{m} k_i$ and $\ell = k_1 + k_3$ . Since $n = k + \ell$ and $n$ is prime, it follows that $\gcd\{k, \ell\} = 1$. Similar to the construction for the $U_{k,\ell}$ one can now find a transformation $\beta'$ such that $\alpha'$ and $\beta'$ generate a semigroup $U'$ isomorphic to $U_{k,\ell}$. That means, the elements of $U'$ are exactly the multiples of $\alpha'$ and all transformations $\gamma$ which satisfy $(i)\gamma = (j)\gamma$, for $i \in C'_1$ and $j \in C'_2$, and where at least one element of $C'_2$ is missing in the image of $\gamma$.

   Now let us compare the sizes of $U$ and $U'$. First consider only the non-bijective transformations of $U'$. This includes at least all non-bijective transformations generated by $\alpha$ and $\beta$, since the first cycle of $\alpha'$ includes $C_2$ and the second cycle of $\alpha'$ includes $C_1$ and $C_3$. So for any non-bijective $\gamma$ generated by $\alpha$ and $\beta$ there are indices $i \in C_1$, $j \in C_2$, $h \in C_3$ such that $(i)\gamma = (j)\gamma$ and $h \notin \mathit{img}(\gamma)$. This implies that $\gamma$ can be generated by $\alpha'$ and $\beta'$ as well. However, $U$ may contain more permutations than $U'$. 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 $U'$ 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 $k_1 k_2 k_3 (n-1)!$ mappings with image size $n - 1$. We first choose the two elements which are in the same kernel equivalence class, for which there are $k_1 k_2$ 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

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

Therefore $U'$ 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 $\beta$ is located in one of the first two cycles. Then an analogous construction as in (1) shows how to construct suitable $\alpha'$ and $\beta'$ such that $|U| \leq |\langle \alpha', \beta' |$. Due to the lack of space the details are left to the reader.

This completes our proof and shows that $|\langle \alpha, \beta \rangle| \leq |U_{k,\ell}|$, because in both cases semigroup $U'$ is isomorphic to some $U_{k,\ell}$, for appropriate $k$ and $\ell$. □

## 6 On the Maximality of $U_{k,\ell}$ Semigroups

Now we are ready to prove the main theorem of this paper, namely that the size maximal semigroup has $|U_{k,\ell}|$ elements, for some $k$ and $\ell$, whenever $n = k + \ell$ is a prime greater or equal than 7. Observe, that the following theorem strengthens Lemma 5.

**Theorem 6.** *Let $n \geq 7$ be a prime number. Then the semigroup $U_{k,\ell}$, for some $k$ and $\ell$ with $n = k + \ell$, is maximal w.r.t. its size among all semigroups which can be generated with two generators.*

*Proof.* Since all other cases have already been treated in the Lemmata 3, 4, and 6, it is left to show that $U_{k,\ell}$ has more elements than the semigroup $V$, where $V$ is generated by $\alpha$ and $\beta$ and latter mapping merges elements located in the same cycle of $\alpha$. Note that $k$ and $\ell$ are trivially coprime whenever $n = k + \ell$ is a prime.

We have shown in Lemma 5 that

$$|V| \leq n^n + n! - n^n \left( \frac{n(n-1)(n-2)}{n^3} \right)^{\frac{n}{3}} = n^n + n! - (n(n-1)(n-2))^{\frac{n}{3}} .$$

Furthermore from [3] it follows that

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

We use Stirling's approximation in the version

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

given in [1, 11]. In this way we obtain an upper bound for $|V|$ and a lower bound for $|U_{k,\ell}|$ , see the proof in [3], as follows:

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

and

$$|U_{k,\ell}| \geq n^n - \left(\sqrt{2}\left(\frac{2}{e}\right)^{\frac{n}{2}} e^{\frac{1}{12}} + \sqrt{8}\frac{1}{\sqrt{n}}e^{\frac{1}{12}}\right) n^n.$$

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

$$\sqrt{2}\left(\frac{2}{e}\right)^{\frac{n}{2}} e^{\frac{1}{12}} + \sqrt{8}\frac{1}{\sqrt{n}}e^{\frac{1}{12}} < \underbrace{\left(\frac{(n-1)(n-2)}{n^2}\right)^{\frac{n}{3}}}_{A(n)} - \underbrace{\sqrt{2\pi n}\left(\frac{1}{e}\right)^{n} e^{\frac{1}{12}}}_{B(n)}.$$

The function $A(n)$ is monotone and converges to $\frac{1}{e} \approx 0.3678794412$ while the function $B(n)$ is antitone and converges to 0. For $n \geq 20$ we have $A(n) > 0.358$ and $B(n) < 10^{-7}$, and therefore $A(n) - B(n) > 0.35 =: c$. We set $c_1 = 0.01$ and $c_2 = 0.34$ and solve the equations

$$\sqrt{2}\left(\frac{2}{e}\right)^{\frac{n}{2}} e^{\frac{1}{12}} < c_1 \quad \text{and} \quad \sqrt{8}\frac{1}{\sqrt{n}}e^{\frac{1}{12}} < c_2.$$

These equations are satisfied if

$$n > 2\frac{\log\left(c_1\frac{1}{\sqrt{2}}e^{-\frac{1}{12}}\right)}{\log\frac{2}{e}} \approx 32.81753852 \quad \text{and} \quad n > \left(\frac{\sqrt{8}}{c_2}e^{\frac{1}{12}}\right)^2 \approx 81.75504594,$$

i.e., whenever $n \geq 82$.

The remaining cases for $7 \leq n \leq 81$ have been checked with the help of the Groups, Algorithms and Programming (GAP) system for computational discrete algebra. To this end we have verified that $|V| \leq |U_{k,\ell}|$, for some $k$ and $\ell$, where the upper bound for $|V|$ from Lemma 5 and the exact value of $|U_{k,\ell}|$ was used.[2] It turned out that $|V_n|$ is maximal w.r.t. size for all $V$ semigroups. □

## 7 Conclusions

We have confirmed the conjecture in [3] on the size of two generator semigroups. In the end, we have shown that for prime $n$, such that $n \geq 7$, the semigroup generated by two generators with maximal size can be characterized in a very nice and accurate way. The cases $2 \leq n \leq 6$ are not treated in this paper, but we

[2] The formula given below did not appear in [3] and gives the exact size of the $U_{k,\ell}$ semigroup: Let $k, \ell \in \mathbb{N}$ such that $\gcd\{k,\ell\} = 1$. The semigroup $U_{k,\ell}$ contains exactly

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

elements, where $n = k + \ell$. 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.

were able to show that in all these cases the semigroup $V_n$ contains a maximal number of elements. Here $2 \leq n \leq 5$ were done by brute force search using the GAP system and $n = 6$ by additional quite involved considerations, which we have to omit to due the lack of space. 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 $n \geq 7$ is not a prime number. We conjecture, that Theorem 6 also holds in this case, but we have no proof yet. Also, the question how to choose $k$ and $\ell$ properly remains unanswered. In order to maximize the size of $U_{k,\ell}$ one has to minimize the number of valid colourings—see [3]—which is minimal if $k$ and $\ell$ are close to $\frac{n}{2}$. This clashes with the observation that the cycle $\alpha$ from which an element in the image of $\beta$ 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 $\ell$ are as close to $\frac{n}{2}$ as the condition that $k$ and $\ell$ should be coprime allows. Again a proof of this statement is still missing. In order to understand the very nature of the question much 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.

## 8 Acknowledgments

Thanks to Rob Johnson, and Paul Pollack, and John Robertson for their help in managing the essential step in the proof of Lemma 1.

## References

1. W. Feller. Stirling's formula. In *An Introduction to Probability Theory and Its Applications*, volume 1, chapter 2.9, pages 50–53. Wiley, 3rd edition, 1968.
2. G. H. Hardy and E. M. Wright. *An Introduction to the Theory of Numbers.* Clarendon, 5th edition, 1979.
3. M. Holzer and B. König. On deterministic finite automata and syntactic monoid size. In M. Ito and M. Toyama, editors, *Preproceedings of the 6th International Conference on Developments in Language Theory*, pages 229–240, Kyoto, Japan, September 2002. Kyoto Sangyo University. To appear in LNCS.
4. J. M. Howie. *An Introduction to Semigroup Theory*, volume 7 of *L. M. S. Monographs.* Academic Press, 1976.
5. E. Landau. Über die Maximalordnung der Permutationen gegebenen Grades. *Archiv der Mathematik und Physik*, 3:92–103, 1903.
6. J.-L. Nicolas. Sur l'ordre maximum d'un élément dans le groupe $s_n$ des permutations. *Acta Arithmetica*, 14:315–332, 1968.
7. 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.
8. S. Piccard. *Sur les bases du groupe symétrique et les couples de substitutions qui engendrent un groupe régulier.* Librairie Vuibert, Paris, 1946.
9. J.-E. Pin. *Varieties of formal languages.* North Oxford, 1986.
10. R. C. Read. An introduction to chromatic polynomials. *Journal of Combinatorial Theory*, 4:52–71, 1968.
11. H. Robbins. A remark of Stirling's formula. *American Mathematical Monthly*, 62:26–29, 1955.