On the Height of Towers of Subsequences and Prefixes

Stěpán Holub, Tomáš Masopust, Michaël Thomazo

▶ **To cite this version:**

Stěpán Holub, Tomáš Masopust, Michaël Thomazo. On the Height of Towers of Subsequences and Prefixes. Information and Computation, 2019, 10.1016/j.ic.2019.01.004 . hal-02269576

HAL Id: hal-02269576
https://inria.hal.science/hal-02269576

Submitted on 23 Aug 2019

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

On the Height of Towers of Subsequences and Prefixes☆

Štěpán Holub[a,1,*], Tomáš Masopust[b,2], Michaël Thomazo[c,3]

[a]*Charles University, Sokolovská 83, 175 86 Praha, Czech Republic*
[b]*Institute of Mathematics, Czech Academy of Sciences, Žižkova 22, 616 62 Brno, Czechia*
[c]*Inria, France*

Abstract

A tower is a sequence of words alternating between two languages in such a way that every word is a subsequence of the following word. The height of the tower is the number of words in the sequence. If there is no infinite tower (a tower of infinite height), then the height of all towers between the languages is bounded. We study upper and lower bounds on the height of maximal finite towers between two regular languages with respect to the size of the NFA (respectively the DFA) representation. Our motivation to study the bounds on maximal finite towers comes from a method to compute a piecewise testable separator of two regular languages. We show that the upper bound is polynomial in the number of states and exponential in the size of the alphabet, and that it is asymptotically tight if the size of the alphabet is fixed. If the alphabet may grow, then, using an alphabet of size approximately the number of states of the automata, the lower bound on the height of towers is exponential with respect to that number. In this case, there is a gap between the lower and upper bound, and the asymptotically optimal bound remains an open problem. Since, in many cases, the constructed towers are sequences of prefixes, we also study towers of prefixes.

Keywords: Automata, languages, alternating towers, subsequences, prefixes, upper and lower bounds
2010 MSC: 68R05, 68Q45

1. Introduction

A *tower* between two languages is a sequence of words alternating between the languages in such a way that every word is a subsequence of the following word. The number of words in a tower is the height of the tower. As a consequence of a more general result [3, Lemma 6], the existence of towers of arbitrary height implies the existence of an infinite tower. Therefore, if there is no infinite tower, the height of all towers is bounded.

Although we believe that the maximal height of towers between two regular languages is an interesting topic on its own, our motivation comes from the construction of a piecewise testable separator of two regular languages [3, 6, 12]. It was independently shown by Czerwiński et al. [3] and Place et al. [12] that the *non*-separability by piecewise testable languages is equivalent to the existence of a common pattern in the two automata (called an $(\mathbf{u}, \mathbf{B})$-*path* in Place et al. [12] and *synchronized languages* in Czerwiński et al. [3]). This pattern is further equivalent to the existence of an infinite tower between the languages [3], and its existence can be detected in polynomial time. Deciding piecewise testable separability is thus in PTime. The problem is also hard for PTime [10]. A similar pattern has recently been identified for general word languages [4].

To actually construct a separator is a more difficult problem. Place et al. [12] construct the separator as a union of $\sim_\kappa$-equivalence classes, where $u \sim_\kappa v$ if and only if the words u and v have the same set of subsequences of length up to

☆A preliminary version of this work was presented at the MFCS 2014 conference [6].

*Corresponding author
Email addresses: holub@karlin.mff.cuni.cz (Štěpán Holub), masopust@math.cas.cz (Tomáš Masopust), michael.thomazo@inria.fr (Michaël Thomazo)

[1]Research supported by the Czech Science Foundation grant number 13-01832S
[2]Research supported by the by DFG in Emmy Noether grant KR 4381/1-1 (DIAMOND), and by RVO 67985840.
[3]Research supported by the Alexander von Humboldt Foundation

	Upper bound	Lower bound	
		$\lvert\Sigma\rvert = k$	$\lvert\Sigma\rvert \geq n + m$
NFAs	$\frac{\mu^{\lvert\Sigma\rvert+1} - 1}{\mu - 1}$	$\Theta\left(\mu^k\right)$	$\Omega\left(2^{n+m}\right)$
DFAs			

(a) Towers of subsequences over Σ; $\mu = \max(n, m)$

	Upper bound	Lower bound	
		$\lvert\Sigma\rvert = 2$	$\lvert\Sigma\rvert \geq n + m$
NFAs	$\frac{(2^n-1)(2^m-1)+1}{2}$	$\Omega\left(2^{\sqrt{\frac{2\nu}{\log 2\nu}}}\right)$	2^{n+m-2}
DFAs	$\frac{nm}{2} + 1$	$\frac{nm}{2} + 1$	$\frac{nm}{2} + 1$

(b) Towers of prefixes; $\nu = \min(n, m)$

Table 1: Upper and lower bounds on the height of towers of subsequences and prefixes for automata with n and m states

κ. The difficult part is to find a suitable κ. Place et al. [12] find such a κ that is exponential in the size of the automaton and doubly exponential in the size of the alphabet. The separator is then κ-piecewise testable and it can be constructed as the union of $\sim_\kappa$ classes that cover one of the languages. Our present research is motivated by a different approach, which we briefly describe in Subsection 2.1. The relation between the maximal height of towers and the number κ of Place et al. is an interesting question. The number of classes of the equivalence relation $\sim_\kappa$ indeed depends on κ and was investigated by Karandikar et al. [9]. In Subsection 2.2, we show that, in some sense, κ provides an upper bound on the maximal height of towers, and that κ can be arbitrarily larger than the maximal height of towers.

Not much is known about the upper bound on the height of towers between two regular languages if no infinite tower exists. The only result we are aware of is a result by Stern [13] giving an exponential upper bound $2^{|\Sigma|^2 n}$ on the height of towers between a piecewise testable language over an alphabet Σ represented by an n-state minimal DFA and its complement. In this paper, we give a better bound that holds in a general setting of two arbitrary regular languages (having no infinite tower) represented by NFAs. We show in Theorem 1 that the upper bound on the height of towers between two regular languages represented by NFAs is polynomial with respect to the depth of the NFAs and exponential with respect to the size of the alphabet.

Considering the lower bound, in Theorem 2 we first improve an existing bound for binary regular languages [6]. Theorems 4 and 5 and Corollary 6 then show that the upper bound is asymptotically tight if the alphabet is fixed, for both NFAs and DFAs. If the alphabet may grow with the depth of the automata, Theorem 4 shows that we can achieve an exponential lower bound for NFAs with respect to the number of states. The same is shown for DFAs in Theorem 7. Notice that it does not contradict the polynomiality of the upper bound with respect to the number of states because the automata require an alphabet of size approximately the number of states. These lower bounds are not asymptotically equal to the upper bound and it is not known what the (asymptotically) tight bound is, cf. Open Problem 1. Specifically, we do not know whether an alphabet of size greater than the number of states may help to build higher towers. In Theorems 8 and 9, we show how to transform general NFAs to DFAs preserving the height of towers.

Surprisingly, it turns out that the towers we construct to demonstrate lower bounds are mostly sequences of prefixes. Therefore, we also investigate *towers of prefixes*. We provide a pattern that characterizes the existence of an infinite tower of prefixes in Theorem 10. We further prove tight bounds on the height of towers of prefixes in Theorem 13 for DFAs and in Theorem 16 for NFAs. We then discuss towers of prefixes between two binary NFAs in Corollary 17.

Our main results are summarized in Table 1. We also formulate the following two open problems:

1. What is the tight bound on the height of towers of subsequences for two NFAs (DFAs) over an alphabet that may grow with the number of states? See Open Problem 1 below.

2. What is the tight bound on the height of towers of prefixes for NFAs over a fixed (binary) alphabet? See Open Problem 2.

2. Preliminaries

The cardinality of a set Σ is denoted by $|\Sigma|$ and its power set by 2^Σ. The free monoid generated by Σ is denoted by Σ^*. An element of Σ^* is called a *word*; the empty word is denoted by ε. For a word $w \in \Sigma^*$, $\mathrm{alph}(w) \subseteq \Sigma$ denotes the set of all letters occurring in w, and $|w|_a$ denotes the number of occurrences of letter a in w.

A *nondeterministic finite automaton* (NFA) is a quintuple $\mathcal{A} = (Q, \Sigma, \delta, I, F)$, where Q is the finite nonempty set of states, Σ is the alphabet, $I \subseteq Q$ is the set of initial states, $F \subseteq Q$ is the set of accepting states, and $\delta\colon Q \times \Sigma \to 2^Q$ is the transition function that can be extended to the domain $2^Q \times \Sigma^*$ in the usual way. The language *accepted* by $\mathcal{A}$ is the set $L(\mathcal{A}) = \{w \in \Sigma^* \mid \delta(I, w) \cap F \neq \emptyset\}$. A *path* π from a state q_0 to a state q_n under a word $a_1a_2\cdots a_n$, for some $n \geq 0$, is a sequence of states and input letters $q_0, a_1, q_1, a_2, \ldots, q_{n-1}, a_n, q_n$ such that $q_{i+1} \in \delta(q_i, a_{i+1})$ for all $i = 0, 1, \ldots, n-1$. The path π is *accepting* if $q_0 \in I$ and $q_n \in F$, and it is *simple* if the states $q_0, q_1, \ldots, q_n$ are pairwise distinct. The number of states on the longest simple path in $\mathcal{A}$ is called the *depth* of $\mathcal{A}$. We write $q \xrightarrow{w} q'$ to denote that $q' \in \delta(q, w)$ and say that there exists a path from state q to state q' under the word w, or labeled by the word w. The NFA $\mathcal{A}$ has a *cycle over an alphabet* $\Gamma \subseteq \Sigma$ if there exists a state q and a word w over Γ such that $q \xrightarrow{w} q$. A path π *contains a cycle over* Γ if $q \xrightarrow{w} q$ is a subpath of π for some state q and $\mathrm{alph}(w) = \Gamma$.

The NFA $\mathcal{A}$ is *deterministic* (DFA) if $|I| = 1$ and $|\delta(q, a)| \leq 1$ for every q in Q and a in Σ. Note that we allow some transitions to be undefined. In the sequel, we consider only automata without useless states, that is, automata where every state appears on an accepting path. In other words, if it is necessary to add a sink state in order to obtain a complete automaton, such a sink state is not considered when counting the number of states.

For two words $v = a_1a_2\cdots a_n$ and $w \in \Sigma^*a_1\Sigma^*a_2\Sigma^*\cdots\Sigma^*a_n\Sigma^*$, we say that v is a *subsequence* of w or that v can be *embedded* into w, denoted by $v \preccurlyeq w$. A word $v \in \Sigma^*$ is a prefix of $w \in \Sigma^*$, denoted by $v \leq w$, if $w = vu$ for some $u \in \Sigma^*$.

We define towers of subsequences as a generalization of Stern's alternating towers between a language and its complement [13]. For two languages L and R, a sequence $(w_i)_{i=1}^r$ of words is a *tower of subsequences* between L and R if $w_1 \in L \cup R$ and, for all $i < r$,

1. $w_i \preccurlyeq w_{i+1}$,
2. $w_i \in L$ implies $w_{i+1} \in R$, and
3. $w_i \in R$ implies $w_{i+1} \in L$.

Similarly, a sequence $(w_i)_{i=1}^r$ of words is a *tower of prefixes* between L and R if $w_1 \in L \cup R$ and, for all $i < r$, $w_i \leq w_{i+1}$, $w_i \in L$ implies $w_{i+1} \in R$, and $w_i \in R$ implies $w_{i+1} \in L$.

The number of words in the sequence, r, is the *height* of the tower. If $r = \infty$, then we speak about an *infinite tower* between L and R. The languages L and R are not necessarily disjoint. However, if there is a word $w \in L \cap R$, then there is a trivial infinite tower $w, w, w, \ldots$. If the languages are clear from the context, we usually omit them. By a *tower between two automata*, we mean a tower between their languages.

In what follows, if we talk about towers without a specification, we mean towers of subsequences. If we mean towers of prefixes, we always specify it explicitly.

2.1. Computing a piecewise testable separator

In this section, we briefly describe our approach to compute a piecewise testable separator that motivates the investigation of this paper.

For a word $w = a_1a_2\cdots a_\ell$, where $a_i \in \Sigma$, let $\mathrm{up}(w)$ denote the language $\Sigma^*a_1\Sigma^*a_2\Sigma^*\cdots\Sigma^*a_\ell\Sigma^*$ of all supersequences of w (the *upward closure*). For a language L, let $\mathrm{up}(L) = \bigcup_{w\in L} \mathrm{up}(w)$. Then $\mathrm{up}(L) = \bigcup_{w\in M_L} \mathrm{up}(w)$, where M_L is the set of minimal elements of L with respect to $\preccurlyeq$, which is finite by Higman's Lemma [5]. A regular language is *piecewise testable* if it is a finite boolean combination of upward closures of some words. Then, $\mathrm{up}(L)$ is piecewise testable for any L. If the words used in the boolean combination are of length at most k, then the language is called k-piecewise testable.

Let L and R be two disjoint languages over Σ. To construct a piecewise testable language $K \supseteq L$ disjoint from R (called a piecewise testable separator), we choose $\mathrm{up}(L)$ as the first approximation of K. Typically, $\mathrm{up}(L)$ is not disjoint from R and, therefore, we try to fix it by putting $R_1 = \mathrm{up}(L) \cap R$ and taking $K_0 = \mathrm{up}(L) \setminus \mathrm{up}(R_1)$. Although

K_0 is obviously disjoint from R, it may not be a superset of L, namely if $L_1 = L \cap \mathsf{up}(R_1)$ is not empty. We therefore repeat the construction for L_1, and construct another "layer" of K defining $R_2 = \mathsf{up}(L_1) \cap R$ and $K_1 = \mathsf{up}(L_1) \setminus \mathsf{up}(R_2)$. In this way, we obtain a sequence $K_0, K_1, K_2, \ldots$ of piecewise testable sets defined by $L_0 = \mathsf{up}(L)$ and by

$$\begin{aligned} R_{i+1} &= \mathsf{up}(L_i) \cap R, \\ L_{i+1} &= \mathsf{up}(R_{i+1}) \cap L, \\ K_i &= \mathsf{up}(L_i) \setminus \mathsf{up}(R_{i+1}) \,. \end{aligned}$$

Finally we define $K = \bigcup_{i \geq 0} K_i$. Definitions imply that $w \in R_{i+1}$ if and only if there is a tower $w_1 \preccurlyeq w'_1 \preccurlyeq w_2 \preccurlyeq w'_2 \preccurlyeq \cdots \preccurlyeq w_i \preccurlyeq w'_i = w$ between L and R. Therefore, if the maximum height of a tower between L and R is $r \leq 2j - 1$, then R_{j+1} is empty. Then $K_j = \mathsf{up}(L_j)$ and $K = \bigcup_{i=0}^{j} K_i$ is the piecewise testable separator we are looking for. Notice that the complexity of the above construction depends on the maximal height of the tower between L and R, which motivates our study on the upper and lower bounds on the height of finite towers.

2.2. The height of towers versus the number κ

Recall that Place et al. [12] construct a number κ for which the separator is κ-piecewise testable. In this section, we show that the number κ provides, in some sense, an upper bound on the maximal height of towers, and that κ can be arbitrarily larger than the maximal height of towers.

We first show that the maximal height of finite towers is bounded by the number of classes of the relation $\sim_\kappa$. Let L and R be two separable regular languages, and let κ be such that every class of the relation $\sim_\kappa$ has a nonempty intersection with at most one of the languages L and R. Let $w_1 \preccurlyeq w_2 \preccurlyeq w_3$ be a part of a tower, where $w_1, w_3 \in L$, $w_2 \in R$, and $w_1 \sim_\kappa w_3$ be two elements of the tower that belong to the same $\sim_\kappa$-class. Let $sub_\kappa(w)$ denote all subsequences of w of length up to κ. Then $sub_\kappa(w_1) \subseteq sub_\kappa(w_2) \subseteq sub_\kappa(w_3) = sub_\kappa(w_1)$ implies that $w_1 \sim_\kappa w_2$. This means that both w_1 and w_2 belong to the same class of the $\sim_\kappa$ relation, and hence this class has a nonempty intersection with both L and R, which is a contradiction. Thus, every $\sim_\kappa$-class contains at most one element of the tower.

To show that κ can be arbitrarily larger than the height of the maximal finite tower, let c be a constant, and let $L_1 = \{w \mid |w| = c\}$ and $L_2 = \{w \mid |w| = 2c\}$ be two languages over $\{0, 1\}$, where the DFA representations have $c + 1$ and $2c + 1$ states. Then the height of the maximal tower is two and our algorithm computes a piecewise testable separator $K = \{w \mid c \leq |w| < 2c\} = \mathsf{up}(L_1) \setminus \mathsf{up}(L_2)$ in one step using time that is easily seen to be polynomial in c. On the other hand, the optimal κ is $c + 1$. Therefore, the method of Place et al. [12] needs to check $2^{\Theta(c \log c)}$ classes in order to construct the separator [9]. This also illustrates the fact that L_1 being piecewise testable itself is not helpful in general. Indeed, deciding whether the language of an NFA is κ-piecewise testable is a PSpace-complete problem even if the NFA is of a very restricted form [11].

2.3. The height of towers versus the number of words in the boolean combination defining separators

The complexity of a separator K can also be measured by the number of elementary languages of the form $\mathsf{up}(w)$ needed in the boolean expression defining K. Let F be the set of words such that K is a boolean combination of languages $\mathsf{up}(w)$, where $w \in F$. For each word $u \in \Sigma^*$, the truth value of $u \in K$ is determined by the set $\sigma(u) = \{w \in F \mid u \in \mathsf{up}(w)\}$. In particular, $\sigma(u) = \sigma(v)$ implies that $u \in K$ if and only if $v \in K$. Observe that $u \preccurlyeq u'$ implies that $\sigma(u) \subseteq \sigma(u')$. We now deduce that $\sigma(w_1) \subsetneq \sigma(w_2) \subsetneq \cdots \subsetneq \sigma(w_r) \subseteq F$ for any tower $(w_i)_{i=1}^r$ between two languages L and R, and hence $|F| \geq r - 1$.[4] This means that any such a boolean expression requires at least as many elements as is the height of the maximal tower. The required number of elements then follows from our lower-bound results.

3. Upper bound on the height of towers of subsequences

Let two languages over Σ be given, represented as NFAs with n and m states. As already mentioned in the introduction, it is known that there is either an infinite tower between the languages, or the height of towers is bounded [3].

[4] We thank an anonymous reviewer of an earlier version of this paper for pointing this out.

We now estimate that bound in terms of $\mu = \max\{n, m\}$ and $k = |\Sigma|$. Stern's bound for minimal DFAs is $2^{k^2\mu}$. Our new bound is $O\left(\mu^k\right) = O\left(2^{k \log \mu}\right)$ and holds for NFAs. Consequently, if the alphabet is fixed, our bound is polynomial with respect to the number of states; otherwise, it is exponential in the size of the alphabet.

Before stating our upper-bound result, we recall that the depth of an automaton is the number of states on the longest simple path, and hence it is bounded by the number of states of the automaton.

Theorem 1. *Let $\mathcal{A}_0$ and $\mathcal{A}_1$ be NFAs with n and m states, respectively, over an alphabet Σ. Assume that there is no infinite tower between the languages $L(\mathcal{A}_0)$ and $L(\mathcal{A}_1)$, and let $(w_i)_{i=1}^r$ be a tower between the languages such that $w_i \in L(\mathcal{A}_{i \bmod 2})$. Let $1 < \mu \leq \max(n, m)$ denote the maximum of the depths of $\mathcal{A}_0$ and $\mathcal{A}_1$. Then $r \leq \frac{\mu^{|\Sigma|+1}-1}{\mu-1}$.*

Proof. To prove the upper bound, we assign to each w_i of the tower an integer W_i in such a way that $0 \leq W_1 < W_2 < \cdots < W_r < \frac{\mu^{|\Sigma|+1}-1}{\mu-1}$. To this aim, we define a factorization of w_r using an accepting path of w_r in $\mathcal{A}_{r \bmod 2}$. Then we inductively define factorizations of all w_i, $1 \leq i < r$, depending on an accepting path of w_i in $\mathcal{A}_{i \bmod 2}$ and on the factorization of w_{i+1}. The value of W_i is derived from these factorizations.

We now define the concepts we need in the proof. We say that a sequence $(v_1, v_2, \ldots, v_k)$ of nonempty words is a *cyclic factorization* of $w = v_1 v_2 \cdots v_k$ with respect to some path π from a state q to a state q' under w in an automaton $\mathcal{A}$ if π can be decomposed into $q_{i-1} \xrightarrow{v_i} q_i$, $i = 1, 2, \ldots k$, and either v_i is a letter, or the path $q_{i-1} \xrightarrow{v_i} q_i$ contains a cycle over $\mathrm{alph}(v_i)$. We call v_i a *letter factor* if it is a letter and $q_{i-1} \neq q_i$, and a *cycle factor* otherwise. Note that our cyclic factorization is closely related to the factorization by Almeida [1], see also Almeida [2, Theorem 8.1.11], and also to factorizations used in [12].

We now show that if π is a path $q \xrightarrow{w} q'$ in some automaton $\mathcal{A}$ with depth μ, then w has a cyclic factorization $(v_1, v_2, \ldots, v_k)$ with respect to π that contains at most μ cycle factors and at most $\mu - 1$ letter factors. Moreover, if $k > 1$, then $\mathrm{alph}(v_i)$ is a strict subset of $\mathrm{alph}(w)$ for each cyclic factor v_i, $i = 1, 2, \ldots, k$. We call such a cyclic factorization *nice*. By convention, the empty sequence is a nice cyclic factorization of the empty word with respect to the empty path.

Consider a path π of the automaton $\mathcal{A}$ from q to q' labeled by a word w. Let $q_0 = q$ and define the factorization $(v_1, v_2, \ldots, v_k)$ inductively by the following greedy strategy. Assume that we have defined the factors $v_1, v_2, \ldots, v_{i-1}$ such that $w = v_1 \cdots v_{i-1} w'$ and $q_0 \xrightarrow{v_1 v_2 \cdots v_{i-1}} q_{i-1}$. The factor v_i is defined as the label of the longest possible initial segment π_i of the path $q_{i-1} \xrightarrow{w'} q'$ such that either π_i contains a cycle over $\mathrm{alph}(v_i)$ or $\pi_i = q_{i-1}, a, q_i$, where $v_i = a$ is a letter. Such a factorization is well defined, and it is a cyclic factorization of w.

Let p_i, for $i = 1, 2, \ldots, k$, be a state such that the path $q_{i-1} \xrightarrow{v_i} q_i$ contains a cycle $p_i \to p_i$ over the alphabet $\mathrm{alph}(v_i)$ if v_i is a cycle factor, and $p_i = q_{i-1}$ if v_i is a letter factor. If $p_i = p_j$ with $i < j$ such that v_i and v_j are cycle factors, then we have a contradiction with the maximality of v_i since $q_{i-1} \xrightarrow{v_i v_{i+1} \cdots v_j} q_j$ contains a cycle $p_i \to p_i$ from p_i to p_i over the alphabet $\mathrm{alph}(v_i v_{i+1} \cdots v_j)$. Therefore, the factorization contains at most μ cycle factors.

Note that v_i is a letter factor only if the state p_i, which is equal to q_{i-1} in such a case, has no reappearance in the path $q_{i-1} \xrightarrow{v_i \cdots v_k} q'$. This implies that there are at most $\mu - 1$ letter factors. Finally, if $\mathrm{alph}(v_i) = \mathrm{alph}(w)$ for a cyclic factor v_i, then $v_i = v_1 = w$ follows from the maximality of v_1. Therefore $(v_1, v_2, \ldots, v_k)$ is a nice cyclic factorization of w.

We are now ready to execute the announced strategy. Let $(v_{r,1}, v_{r,2}, \ldots, v_{r,k_r})$ be a nice cyclic factorization of w_r with respect to some accepting path in the automaton $\mathcal{A}_{r \bmod 2}$. Given a (not necessarily nice) cyclic factorization $(v_{i,1}, v_{i,2}, \ldots, v_{i,k_i})$ of w_i, $i = 2, 3, \ldots, r$, the factorization $(v_{i-1,1}, v_{i-1,2}, \ldots, v_{i-1,k_{i-1}})$ of w_{i-1} is defined as follows. Let $w_{i-1} = v'_{i,1} v'_{i,2} \cdots v'_{i,k_i}$, where $v'_{i,j} \preccurlyeq v_{i,j}$ for each $j = 1, 2, \ldots, k_i$. Such words (possibly empty) exist, since we have that $w_{i-1} \preccurlyeq w_i$. Let $\pi_{i,j}$ be paths under $v'_{i,j}$ that together form an accepting path of w_{i-1} in $\mathcal{A}_{i-1 \bmod 2}$. Then

$$(v_{i-1,1}, v_{i-1,2}, \ldots, v_{i-1,k_{i-1}}) = \prod_{j=1}^{k_i} \left(v''_{i,j,1}, v''_{i,j,2}, \ldots, v''_{i,j,m_{i,j}}\right),$$

where $\left(v''_{i,j,1}, v''_{i,j,2}, \ldots, v''_{i,j,m_{i,j}}\right)$ is a nice cyclic factorization of $v'_{i,j}$ with respect to $\pi_{i,j}$ and the product denotes the concatenation of sequences. Note that if $v_{i,j}$ is a letter factor of w_i then either $m_{i,j} = 0$ (if $v'_{i,j}$ is empty) or $m_{i,j} = 1$ and $v''_{i,j,1}$ is a letter factor of w_{i-1}.

To define W_i, let g be the function $g(x) = \mu\frac{\mu^x-1}{\mu-1}$, and let $f(v_{i,j}) = 1$ if $v_{i,j}$ is a letter factor, and $f(v_{i,j}) = g\left(\left|\mathrm{alph}(v_{i,j})\right|\right)$ if $v_{i,j}$ is a cycle factor. We now set

$$W_i = \sum_{j=1}^{k_i} f\left(v_{i,j}\right).$$

The key property of g is that $g(x+1) = \mu \cdot g(x) + (\mu - 1) + 1$. (In fact, this equality and $g(0) = 0$ defines g.) The definition of a nice factorization implies that if $(v_1, v_2, \ldots, v_k)$ is a nice factorization of w with $k > 1$, then

$$\sum_{i=1}^{k} f(v_i) \le \mu \cdot g\left(\left|\mathrm{alph}(w)\right| - 1\right) + (\mu - 1) < g\left(\left|\mathrm{alph}(w)\right|\right).$$

Applying this to the nice factorizations defined above, we obtain

$$\sum_{\ell=1}^{m_{i,j}} f\left(v''_{i,j,\ell}\right) \le f\left(v_{i,j}\right) \tag{1}$$

for all $i = 2, 3, \ldots, r$ and $j = 1, 2, \ldots, k_i$. In particular,

$$W_r = \sum_{\ell=1}^{k_r} f(v_{r,\ell}) \le g\left(\left|\mathrm{alph}(w_r)\right|\right) \le g(|\Sigma|) < g(|\Sigma|) + 1 = \frac{\mu^{|\Sigma|+1} - 1}{\mu - 1}. \tag{2}$$

Moreover, we have equality in (1) if and only if $m_{i,j} = 1$, $\mathrm{alph}\left(v_{i,j}\right) = \mathrm{alph}\left(v''_{i,j,1}\right)$, and both $v_{i,j}$ and $v''_{i,j,1}$ are either letter factors, or cyclic factors. We deduce that $W_{i-1} \le W_i$, $i = 2, 3, \ldots, r$, and, moreover, $W_{i-1} = W_i$ if and only if

- $k_{i-1} = k_i$,
- $\mathrm{alph}(v_{i,j}) = \mathrm{alph}(v_{i-1,j})$ for all $j = 1, 2, \ldots, k_i$, and
- for all $j = 1, 2, \ldots, k_i$, $v_{i,j}$ is a letter factor if and only if $v_{i-1,j}$ is a letter factor.

We show that if these conditions are met for some i, then there is an infinite tower between $\mathcal{A}_0$ and $\mathcal{A}_1$. Let Z be the language of words $z_1 z_2 \cdots z_{k_i}$ such that $z_j = v_{i,j}$ if $v_{i,j}$ is a letter factor, and $z_j \in (\mathrm{alph}(v_{i,j}))^*$ if $v_{i,j}$ is a cycle factor. In particular, $w_i, w_{i-1} \in Z$. Since $w_i \in L(\mathcal{A}_{i \bmod 2})$ and $w_{i-1} \in L(\mathcal{A}_{i-1 \bmod 2})$, the definition of a cycle factor implies that, for each $z \in Z$, there exist $z' \in L(\mathcal{A}_0) \cap Z$ such that $z \preccurlyeq z'$ and $z'' \in L(\mathcal{A}_1) \cap Z$ such that $z \preccurlyeq z''$. The existence of an infinite tower follows.

As a trivial case, consider the situation where all factors in question are letter factors. Then $w_i = w_{i-1}$, and the languages are not disjoint, which yields the infinite tower consisting of the shared word. As a more complicated example, assume that $k_{i-1} = k_i = 2$, and let $w_{i-1} = cab \cdot b$, $w_i = aabbcc \cdot b$ be the corresponding nice factorizations where factors cab and $aabbcc$ are cyclic with cycles labeled with cab and $abbc$. Then $(cab)^*b \subseteq L(\mathcal{A}_{i-1 \bmod 2})$ and $a(abbc)^*c\,b \subseteq L(\mathcal{A}_{i \bmod 2})$. The infinite tower is now for example $cabb \preccurlyeq a(abbc)^3cb \preccurlyeq (cab)^{13}b \preccurlyeq a(abbc)^{39}cb \preccurlyeq \cdots$.

We have therefore proved that $W_{i-1} < W_i$, which together with (2) completes the proof. □

The question is how good this bound is. We study this question next and show that it is tight if the alphabet is fixed. If the alphabet grows with the number of states of the automata, then we can construct a tower of exponential height with respect to the number of states of the automata (as well as with respect to the size of the alphabet). However, we do not know whether this bound is tight. We formulate this question as the following open problem asking how much the size of the alphabet can increase the height of the tower, given the number of states (or the depth). In Theorem 1, the alphabet plays an important role. It is a natural and very intriguing question, what the potential of the alphabet really is.

Open Problem 1. Let $\mathcal{A}_0$ and $\mathcal{A}_1$ be NFAs with n and m states, respectively, over an alphabet Σ with $|\Sigma| \ge n + m$. Let μ be the maximum depth of $\mathcal{A}_0$ and $\mathcal{A}_1$. Assume that there is no infinite tower between the languages $L(\mathcal{A}_0)$ and $L(\mathcal{A}_1)$, and let $(w_i)_{i=1}^r$ be a tower between them. Is it true that $r \le \frac{\mu^{n+m+1}-1}{\mu-1}$ or even that $r \le 2^{n+m}$?

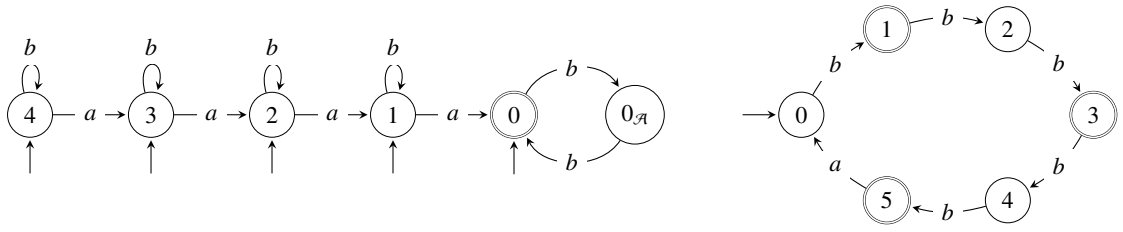

Figure 1: Automata $\mathcal{A}_d$ and $\mathcal{B}_e$ of Theorem 2 for $d = e = 5$

4. Lower bounds on the height of towers

The upper bound of Theorem 1, as well as its proof, indicate that the size of the alphabet is significant for the height of towers. This is confirmed by lower bounds considered in this section. We consider two cases, namely (i) the size of the alphabet is fixed and (ii) the size of the alphabet may grow with the size of the automata. We show that the upper bound of Theorem 1 is asymptotically tight if the size of the alphabet is fixed, and that the lower bound may be exponential with respect to the size of the automata if the alphabet may grow. In this case, the size of the alphabet is approximately the number of states of the automata. However, the precise upper bound for this case is left open, cf. Open Problem 1.

To warm up, we start with the binary alphabet. The upper bound of Theorem 1 gives $n^2 + n + 1$ in this case, and it is known to be tight up to a linear factor [6]. Namely, for every odd positive integer n, there are two binary NFAs with $n - 1$ and n states having a tower of height $n^2 - 4n + 5$ and no infinite tower. We now improve this bound.

Theorem 2. *For every positive integer d and every odd positive integer e, there exists a binary NFA with $d + 1$ states and a binary DFA with $e + 1$ states having a tower of height $d(e + 1) + 2$ and no infinite tower.*

Proof. We define the automata $\mathcal{A}_d$ and $\mathcal{B}_e$ with $d + 1$ and $e + 1$ states, respectively, as depicted in Figure 1 for $d = e = 5$. The NFA $\mathcal{A}_d = (\{0, 1, \ldots, d-1\} \cup \{0_{\mathcal{A}}\}, \{a, b\}, \delta_d, \{0, 1, \ldots, d-1\}, \{0\})$ consists of an a-path through the states $d - 1, \ldots, 0$, of self-loops under b in all states $1, \ldots, d - 1$, and of a b-cycle from 0 to $0_{\mathcal{A}}$ and back to 0. The DFA $\mathcal{B}_e = (\{0, 1, \ldots, e\}, \{a, b\}, \delta_e, 0, \{i \mid 1 \leq i \leq e \text{ and } i \text{ is odd}\})$ consists of a b-path through the states $0, 1, \ldots, e$ and of an a-transition from state e to state 0. All odd states are accepting.

Consider the word $w = (b^e a)^{d-1} b^{e+1}$. Note that $\mathcal{A}_d$ accepts all prefixes of w ending with an even number of b's, including those ending with a, and the empty prefix. On the other hand, the automaton $\mathcal{B}_e$ accepts all prefixes of w ending with an odd number of b's. Moreover, the automaton $\mathcal{B}_e$ accepts the word $(b^e a)^{d-1} b^e ab$. Hence the sequence $(w_i)_{i=1}^{|w|+2}$, where, for $i = 1, 2, \ldots, |w| + 1$, w_i is the prefix of w of length $i - 1$, and $w_{|w|+2} = (b^e a)^{d-1} b^e ab$ is a tower between $\mathcal{A}_d$ and $\mathcal{B}_e$ of height $|w| + 2 = (e + 1)(d - 1) + e + 1 + 2 = d(e + 1) + 2$.

We show that there is no higher tower between the languages, in particular, there is no infinite tower. Notice that any word in $L(\mathcal{B}_e)$ is a prefix of a word in $(b^e a)^*$. As the languages are disjoint (they require a different parity of the b-tail), any tower $(w_i)_{i=1}^r$ is strictly increasing with respect to $\preccurlyeq$ and thus $|w_i| \geq i - 1$. Thus if the height of $(w_i)_{i=1}^r$ is larger than $d(e + 1) + 2$ the word $w_{d(e+1)+1}$ or $w_{d(e+1)+2}$ is in $L(\mathcal{B}_e)$ and therefore contains at least d occurrences of letter a. However, no such word can be embedded into a word of $L(\mathcal{A}_d)$, since each word of $L(\mathcal{A}_d)$ contains at most $d - 1$ occurrences of letter a. □

As a consequence of Theorem 2, we obtain the following lower bound on the height of binary towers.

Corollary 3. *For every even positive integer n, there exists a binary NFA with n states and a binary DFA with n states having a tower of height $n^2 - n + 2$ and no infinite tower.*

Proof. Set $d = e = n - 1$ in Theorem 2. □

The construction used in Theorem 2 reveals the main mechanism behind high towers. The automaton $\mathcal{A}_d$ bounds the number of possible occurrences of letter a (by $d - 1$) but it is very generous concerning letter b. On the other hand, the automaton $\mathcal{B}_e$ requires at least one a for each sequence of e occurrences of letter b. This general strategy is

employed in a more complicated way in the following two theorems, which eventually allow to show that the upper bound from Theorem 1 is asymptotically tight, even for deterministic automata.

Theorem 4. *For all integers $n, m \geq 2$ there exist two NFAs with n and m states over an alphabet of cardinality $n+m-2$ having a tower of height $2^{n+m-2} - 2^{m-2} + 1$ and no infinite tower.*

Proof. For $k \geq 0$, let $\Sigma_k = \{b, a_1, a_2, \ldots, a_k\}$ and $\Gamma_k = \{c_1, c_2, \ldots, c_k\}$ be alphabets (with $\Sigma_0 = \{b\}$ and $\Gamma_0 = \emptyset$). We define two NFAs $\mathcal{A}_{n,m}$ and $\mathcal{B}_{n,m}$ over $\Sigma_{n-1} \cup \Gamma_{m-2}$ as follows.

The set of states of the NFA $\mathcal{A}_{n,m}$ is $Q_n = \{0, 1, 2, \ldots, n-1\}$. All states are initial, and state 0 is the unique accepting state. The transition function of $\mathcal{A}_{n,m}$ consists of

- a self-loop under Σ_{j-1} for all states j with $j > 0$,
- an a_i-transition i to j if $0 \leq j < i$, and
- transitions under Γ_{m-2} from state 0 to each state $j > 0$.

The NFA $\mathcal{A}_{5,m}$ is shown in Figure 2.

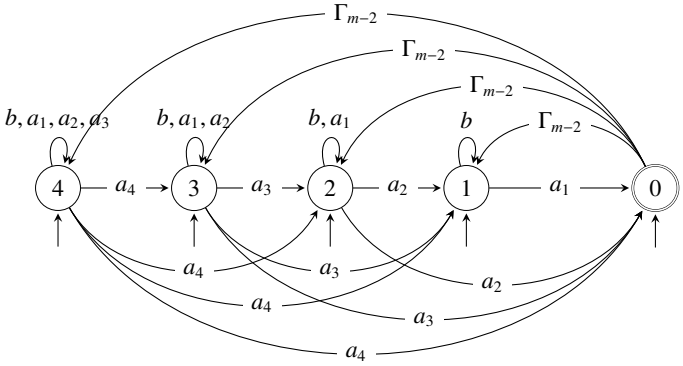

Figure 2: Automaton $\mathcal{A}_{5,m}$ of Theorem 4

The NFA $\mathcal{B}_{n,m}$ has the state set $Q_m = \{0, 1, 2, \ldots, m-2\} \cup \{0_B\}$. All states are initial, except for state 0_B, which, in turn, is the unique accepting state. The transitions of $\mathcal{B}_{n,m}$ consist of

- self-loops under $\Sigma_{n-1} \cup \Gamma_{j-1}$ for all states j with $j > 0$, and of self-loops under Σ_{n-1} in state 0,
- a c_i-transition from i to j if $0 \leq j < i$, and from i to 0_B, and
- transitions under $\Gamma_{m-2} \cup \{b\}$ from 0 to 0_B.

The NFA $\mathcal{B}_{n,6}$ is shown in Figure 3.

We now define a word $u_{n+m-3}b$ such that all its prefixes form a tower. To do this, we first inductively define a word u_{n-1} so that $u_0 = \varepsilon$ and $u_k = u_{k-1}ba_ku_{k-1}$ for $0 < k < n$. Then $u_k \in \Sigma_k^*$ and $|u_k| = 2^{k+1} - 2$. We now use the word u_{n-1} to define, for $0 < p \leq m-2$, a word $u_{n+p-1} = u_{n+p-2}c_pu_{n+p-2}$. Then $u_{n+p-1} \in (\Sigma_{n-1} \cup \Gamma_p)^*$ and $|u_{n+p-1}| = 2^{n+p} - 2^p - 1$. Finally, the word $u_{n+m-3}b$ is of length $2^{n+m-2} - 2^{m-2}$, therefore it has $2^{n+m-2} - 2^{m-2} + 1$ prefixes.

We now show that the prefixes of $u_{n+m-3}b$ form a tower between the languages. Namely, we show by induction on p that every prefix v of $u_{n+p-1}b$ is accepted by $\mathcal{A}_{n,m}$ if it ends with a letter from $\Sigma_{n-1} \setminus \{b\}$, and it is accepted by $\mathcal{B}_{n,m}$ from a state smaller than $p+1$ if it ends with a letter from $\Gamma_{m-2} \cup \{b\}$.

For $p = 0$, any prefix v of $u_{n-1}b$ ending with b is accepted by $\mathcal{B}_{n,m}$ from state 0. The empty word is accepted by $\mathcal{A}_{n,m}$ in 0. If v is nonempty and ending with a letter from $\Sigma_{n-1} \setminus \{b\}$, then it is of the form $v = u_{k-1}ba_kv'$ with $k > 0$

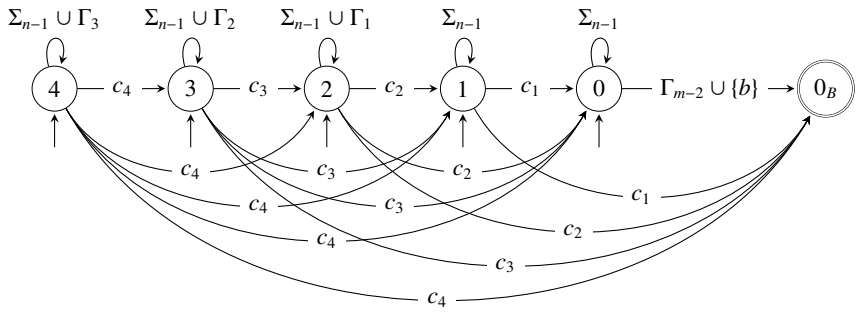

Figure 3: Automaton $\mathcal{B}_{n,6}$ of Theorem 4

where v' is a prefix of u_{k-1}. We show by induction on $|v|$ that v is accepted by $\mathcal{A}_{n,m}$ from state k. By the induction hypothesis, v' is accepted by $\mathcal{A}_{n,m}$ from some state $k' < k$. Then v is accepted by $\mathcal{A}_{n,m}$ by the path

$$k \xrightarrow{u_{k-1}b} k \xrightarrow{a_k} k' \xrightarrow{v'} 0\,.$$

In particular, u_{n-1} is accepted by $\mathcal{A}_{n,m}$ from the state $n-1$.

Let now $p \geq 1$ and consider the word $u_{n+p-1}b$. By induction, the claim holds for prefixes of $u_{n+p-2}b$ and u_{n+p-2} is accepted in $\mathcal{A}_{n,m}$ from state $n-1$. Let v be a prefix of $u_{n+p-1}b$ of the form $u_{n+p-2}c_p v'$ where v' is a prefix (possibly empty) of $u_{n+p-2}b$. If v' ends with a letter from $\Sigma_{n-1} \setminus \{b\}$, then $\mathcal{A}_{n,m}$ accepts v' from a state k' by the induction hypothesis. Then the whole prefix v is accepted in $\mathcal{A}_{n,m}$ by the path

$$n-1 \xrightarrow{u_{n+p-2}} 0 \xrightarrow{c_p} k' \xrightarrow{v'} 0\,.$$

If v' ends with a letter from $\Gamma_p \cup \{b\}$, then it is accepted by $\mathcal{B}_{n,m}$ from a state $p' < p$ by the induction hypothesis. Then the whole prefix v is accepted by $\mathcal{B}_{n,m}$ by the path

$$p \xrightarrow{u_{n+p-2}} p \xrightarrow{c_p} p' \xrightarrow{v'} 0\,.$$

This shows the claimed height of the tower.

It remains to show that there is no infinite tower. We first show that there is no infinite tower over the alphabet Σ_{n-1} and then that there is no infinite tower over the alphabet $\Sigma_{n-1} \cup \Gamma_{m-2}$. Suppose the contrary, and let $k \geq 0$ be the smallest integer such that there is an infinite tower over Σ_k. Since ε, b is the highest tower over Σ_0, we have $k \geq 1$. Since every word of $L(\mathcal{A}_{n,m}) \cap \Sigma_k^*$ contains at most one occurrence of the letter a_k, we can consider, without loss of generality, an infinite tower $(w_i)_{i=1}^{\infty}$ in which every w_i contains exactly one occurrence of a_k. Let $w_i = w_i'' a_k w_i'$, where $w_i', w_i'' \in \Sigma_{k-1}^*$. Since all transitions under a_k lead to an initial state in both automata, the word w_i' is accepted by $\mathcal{A}_{n,m}$ (by $\mathcal{B}_{n,m}$ resp.) if w_i is accepted by $\mathcal{A}_{n,m}$ (by $\mathcal{B}_{n,m}$ resp.). Then $(w_i')_{i=1}^{\infty}$ is an infinite tower over Σ_{k-1}; a contradiction. Thus, let $p \geq 1$ be the smallest integer such that there is an infinite tower over $\Sigma_{n-1} \cup \Gamma_p$. Similarly as above, since each word from $(\Sigma_{n-1} \cup \Gamma_p)^*$ accepted by the automaton $\mathcal{B}_{n,m}$ contains at most one occurrence of c_p, we can choose an infinite tower $(w_i)_{i=1}^{\infty}$ such that all words have exactly one occurrence of the letter c_p. Let $w_i = w_i'' c_p w_i'$ with $w_i', w_i'' \in (\Sigma_{n-1} \cup \Gamma_{p-1})^*$. A direct inspection of the automata yields that w_i' is accepted by $\mathcal{A}_{n,m}$ (by $\mathcal{B}_{n,m}$ resp.) if w_i is accepted by $\mathcal{A}_{n,m}$ (by $\mathcal{B}_{n,m}$ resp.). Then $(w_i')_{i=1}^{\infty}$ is an infinite tower over $\Sigma_{n-1} \cup \Gamma_{p-1}$; a contradiction. □

Remark 1. As pointed out, the tower constructed in the previous proof is actually a tower of prefixes. Theorem 4 therefore still holds if "tower" is replaced with "tower of prefixes".

The following theorem adapts the previous construction for deterministic automata.

Theorem 5. *For all integers $k \geq 1$, $d \geq 2$ and every odd positive integer e, there exist two DFAs with $(k+1)d + k - 1$ and $e+1$ states over an alphabet of cardinality $k+1$ having a tower of height $(e+1)d^k + 2d^{k-1}$ and no infinite tower.*

Proof. For every $k \geq 1$, let $\Sigma_k = \{b, a_1, a_2, \ldots, a_k\}$. We define two DFAs $\mathcal{A}_{k,d}$ and $\mathcal{B}_{k,e}$ over Σ_k as follows. The set of states of the DFA $\mathcal{A}_{k,d}$ is $Q_{k,d} = \{(m, j) \mid m = 1, 2, \ldots, k;\ j = 0, 1, 2, \ldots, d-1\} \cup \{m' \mid m = 2, \ldots, k\} \cup \{(1, i') \mid i = 0, 1, \ldots, d-1\}$. State $(k, d-1)$ is initial, and states $(1, j)$, $j = 0, \ldots, d-1$, are accepting. The transition function of $\mathcal{A}_{k,d}$ consists of

- an a_i-transition from each (i, j) to $(i, j-1)$, and from $(i, 0)$ to states $(i-1, d-1)$ if $i > 1$ and $j > 0$,
- an a_1-transition from $(1, j')$ to $(1, j-1)$ if $1 \leq j \leq d-1$,
- a transition from $(i, d-1)$ to i' and back under a_1 if $i \geq 2$,
- a b-transition from $(1, j)$ to $(1, j')$ and back if $0 \leq j \leq d-1$,
- self-loops in (i, j) under Σ_{i-1} if $i \geq 2$ and $0 \leq j \leq d-2$, and
- self-loops under a_i in states i' if $i \geq 2$.

See Figure 4 for an example.

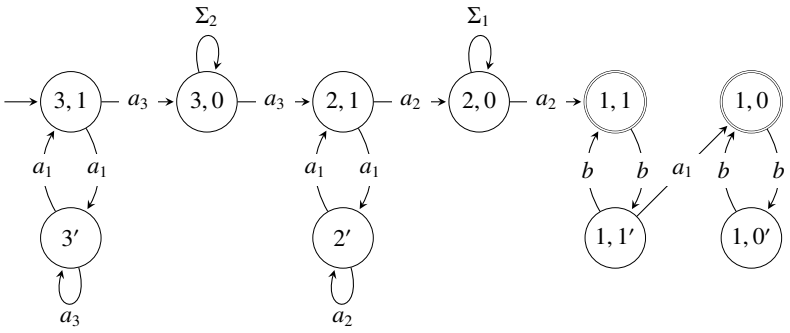

Figure 4: Automaton $\mathcal{A}_{3,2}$ of Theorem 5

The DFA $\mathcal{B}_{k,e}$ has the states $\{0, 1, \ldots, e\}$. State 0 is initial and states with odd numbers are accepting. The transitions of $\mathcal{B}_{k,e}$ contain b-transitions from state i to state $i+1$ for each $0 \leq i \leq e-1$, a transition under $\{a_1, a_2, \ldots, a_k\}$ from state e to state 0, and a self-loop in state 0 under $\{a_1, a_2, \ldots, a_k\}$, see Figure 5 for an illustration.

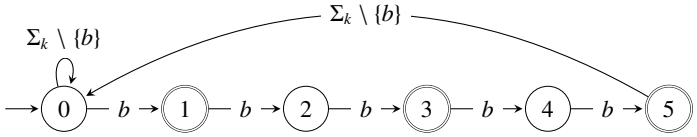

Figure 5: Automata $\mathcal{B}_{k,5}$ of Theorem 5

We now show by induction on k that there is a tower of height $(e+1)d^k + 2d^{k-1}$ between $\mathcal{A}_{k,d}$ and $\mathcal{B}_{k,e}$. For $k = 1$, the automata $\mathcal{A}_{1,d}$ and $\mathcal{B}_{1,e}$ have the tower of prefixes of the word $u = (b^e a_1)^{d-1} b^e$ with two additional words: ub accepted by $\mathcal{A}_{1,d}$, and ua_1b^e accepted by $\mathcal{B}_{1,e}$ in the state e. The tower has the required height $(e+1)d + 2$.

Let now $k \geq 2$ and let $(w_{k-1,i})_{i=1}^{\ell}$, with $\ell = (e+1)d^{k-1} + 2d^{k-2}$, be a tower between the automata $\mathcal{A}_{k-1,d}$ and $\mathcal{B}_{k-1,e}$, where $w_{k-1,1}$ is accepted by $\mathcal{A}_{k-1,d}$ and $w_{k-1,\ell}$ is accepted by $\mathcal{B}_{k-1,e}$ in the state e. Let $u_{k,j} = (a_1 a_k a_1)^j a_k^{d-j} (w_{k-1,\ell} a_k)^j$. We show that $(w_{k,i})_{i=1}^{d\ell}$ with

$$w_{k,j\ell+m} = u_{k,j} w_{k-1,m}, \quad j = 0, 1, \ldots, d-1,\ m = 1, 2, \ldots, \ell,$$

is a tower between the automata $\mathcal{A}_{k,d}$ and $\mathcal{B}_{k,e}$, where $w_{k,1}$ is accepted by $\mathcal{A}_{k,d}$ and $w_{k,d\ell}$ is accepted by $\mathcal{B}_{k,e}$ in the state e.

Since $w_{k-1,\ell} \in \Sigma_{k-1}^*$, it is straightforward to verify that, for each $j = 0, \ldots, d-1$, the word $u_{k,j}$ is a label, in $\mathcal{A}_{k,d}$, of a path from $(k, d-1)$ to $(k-1, d-1)$: if $j = 0$, then

$$(k, d-1) \xrightarrow{a_k^d} (k-1, d-1)\,,$$

and if $0 < j$, then the path is

$$(k, d-1) \xrightarrow{(a_1 a_k a_1)^j} (k, d-1) \xrightarrow{a_k^{d-j}} (k, j-1) \xrightarrow{(w_{k-1,\ell} a_k)^j} (k-1, d-1)\,.$$

In $\mathcal{B}_{k,e}$, each $u_{k,j}$ is a label for a cycle starting and ending in the state 0; namely,

$$0 \xrightarrow{(a_1 a_k a_1)^j a_k^{d-j}} 0 \underbrace{\xrightarrow{w_{k-1,\ell}} e \xrightarrow{a_k} 0}_{j-\text{times}}\,.$$

This implies, by induction and by the construction of the automata, that $w_{k,i}$ are accepted as required. By induction, we have that $w_{k,j\ell+m} \preccurlyeq w_{k,j\ell+m+1}$ for each $1 \leq m < \ell$, and the definition of $u_{k,j}$ implies that also

$$w_{k,j\ell} = (a_1 a_k a_1)^{j-1} a_k^{d-j+1} (w_{k-1,\ell} a_k)^{j-1} w_{k-1,\ell} \preccurlyeq (a_1 a_k a_1)^j a_k^{d-j} (w_{k-1,\ell} a_k)^j w_{k-1,1} = w_{k,j\ell+1}.$$

This completes the proof that $(w_{k,i})_{i=1}^{d\ell}$ is a tower with required properties.

It remains to show that there is no infinite tower. For $k = 1$, the proof is similar to the corresponding part of Theorem 2. Namely, any word from $L(\mathcal{A}_{1,d})$ contains at most d occurrences of a_1. Looking at $\mathcal{B}_{k,e}$, we obtain an upper bound on the length of words in the tower. For the sake of contradiction, let now $k > 1$ be the smallest number such that there exists an infinite tower $(w_i)_{i=1}^{\infty}$ between $\mathcal{A}_{k,d}$ and $\mathcal{B}_{k,e}$ for some d and e. Suppose, first, that for all i, $w_i \in \{a_1, a_k\}^* w_i'$ where $w_i' \in \Sigma_{k-1}^*$. We may assume that a_1 is not the first letter of w_i'. This implies that after reading the $\{a_1, a_k\}^*$ part, $\mathcal{A}_{k,d}$ is in $(k-1, d-1)$ and that $\mathcal{B}_{k,e}$ is in 0. Thus $(w_i')_{i=1}^{\infty}$ is an infinite tower between $\mathcal{A}_{k-1,d}$ and $\mathcal{B}_{k-1,e}$; a contradiction. Let now $t > 1$ be the largest integer such that a word $ca_k^t \preccurlyeq w_i$ for some i, where $c \in \Sigma_k \setminus \{a_1, a_k\}$. It is straightforward to verify that ca_k^d cannot be embedded into any word from $L(\mathcal{A}_{k,d})$, hence $t < d$. Without loss of generality, we can suppose that $ca_k^t \preccurlyeq w_i$ for all i. Let $w_i = w_i'' w_i'$ where w_i'' is the shortest prefix of w_i, such that $ca_k^t \preccurlyeq w_i''$. Then $w_i' \in \Sigma_{k-1}^*$, and $(w_i')_{i=1}^{\infty}$ is again a tower between $\mathcal{A}_{k-1,d}$ and $\mathcal{B}_{k-1,e}$; a contradiction. □

As a corollary, we have that the upper bound of Theorem 1 is tight for a fixed alphabet even for DFAs.

Corollary 6. *Let $k \geq 2$ be a constant. Then the maximum height of a tower between two DFAs with at most n states over an alphabet of cardinality k having no infinite tower is in $\Omega\left(n^k\right)$.*

Proof. For a sufficiently large n, let $k' = k-1$, $d = \left\lfloor \frac{n-k'}{k} \right\rfloor$, and $n-2 \leq e \leq n-1$. Theorem 5 then implies that there exist two DFAs with at most n states having a tower of height at least $(n-1)d^{k'} + 2d^{k'-1} \in \Omega\left(n^k\right)$, and no infinite tower. □

We remark that Corollary 6 in particular improves our former bound $\Omega(n^3)$ for a four-letter alphabet [6, Theorem 3].

Theorem 4 shows that the height of a tower can be exponential in the number of states of NFAs, if the alphabet is allowed to grow with the number of states. For DFAs with at most n states, Theorem 5 yields the height of a tower $\Omega\left((n+1)2^{n/3}\right)$ (for $d = 2$, $k = (n-1)/3$ and $e = n-1$). To obtain a better lower bound for DFAs, we combine Theorem 4 with a "determinization" strategy.

Theorem 7. *For every $n \geq 0$, there exist two DFAs with at most $n+1$ states over an alphabet of cardinality $\frac{n(n+1)}{2} + 1$ having a tower of height 2^n and no infinite tower.*

Proof. For a given integer n, we define a pair of deterministic automata $\mathcal{A}_n$ and $\mathcal{B}_n$ with $n+1$ and two states, respectively, over the alphabet $\Sigma_n = \{b\} \cup \{a_{i,j} \mid i = 1, 2, \ldots, n;\ j = 0, 1, \ldots, i-1\}$ with a tower of height 2^n between $L(\mathcal{A}_n)$

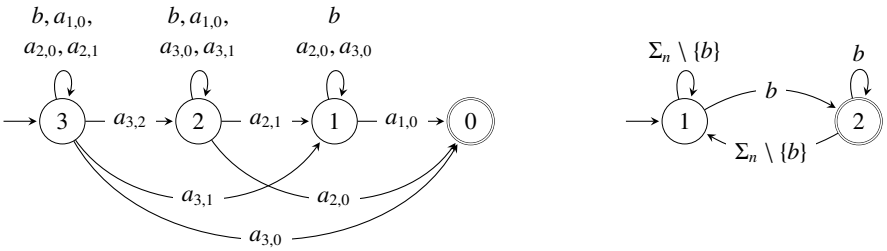

Figure 6: The DFA $\mathcal{A}_3$ (left) and the two-state DFA $\mathcal{B}_n$ (right), $n \geq 0$ of Theorem 7

and $L(\mathcal{B}_n)$, and with no infinite tower. The two-state DFA $\mathcal{B}_n = (\{1,2\}, \Sigma_n, \gamma_n, 1, \{2\})$ accepts all words over Σ_n ending with b and is shown in Figure 6 (right). Note that $\mathcal{B}_n$ is a deterministic version of $\mathcal{B}_{n,0,1}$ of Theorem 4.

The idea of the construction of the DFA $\mathcal{A}_n = (\{0,1,\ldots,n\}, \Sigma_n, \delta_n, n, \{0\})$ is to use the automaton $\mathcal{A}_{n,0,1}$ from the proof of Theorem 4. Since we take $d = 1$, we can denote the state $(i,0)$ simply as i. The nondeterminism is eliminated by relabeling every transition $i \xrightarrow{a_i} j$ with a new unique letter $i \xrightarrow{a_{i,j}} j$. Then the tower of Theorem 4 is modified by relabeling the corresponding letters. However, to preserve embeddability of the new letters, several self-loops must be added.

Formally, the transition function δ_n is defined as follows. For every $a_{i,j} \in \Sigma_n$, we define the transition $\delta_n(i, a_{i,j}) = j$. For every $k = 1,2,\ldots,n$ and $a_{i,j} \in \Sigma_n$ such that $i \neq k$ and $j < k$, we define the self-loop $\delta_n(k, a_{i,j}) = k$. Finally, we add the self-loops $\delta_n(k,b) = k$ to every state $k = 1,2,\ldots,n$, see Figures 6 and 7 for an illustration.

For every $1 \leq k \leq n$ and $0 \leq j < k$, let $\alpha_{k,j} = a_{k,j} a_{k,j-1} \cdots a_{k,0}$, and let the words u_k be defined by $u_0 = \varepsilon$ and $u_k = u_{k-1} b\, \alpha_{k,k-1}\, u_{k-1}$. Note that $u_k b$ contains 2^k letters b.

We first give an informal description of the tower of height 2^n between $\mathcal{A}_n$ and $\mathcal{B}_n$, which relates the construction to Theorem 4. The tower is the sequence $w_n(0), w_n(1), \ldots, w_n(2^n-1)$, where the longest word $w_n(2^n-1)$ is $\alpha_{n,n-1}\, u_{n-1} b \in L(\mathcal{B}_n)$. The word $w_n(2i)$ is obtained from the word $w_n(2i+1)$ by removing the last letter, which is b. The word $w_n(2i-1)$ is obtained from the word $w_n(2i)$ by removing the first letter of some occurrences of $\alpha_{k,j}$ in $w_n(2i)$, see Figure 8 for the case $n = 3$.

We now give a formal definition of $w_n(i)$, which is done recursively. For any $k \geq 1$, we define $w_k(0) = \alpha_{k,0} = a_{k,0}$ and $w_k(1) = a_{k,0}\, b$. For $2 \leq i \leq 2^k - 1$, let

$$w_k(i) = \alpha_{k,\lfloor \log i \rfloor}\, u_{\lfloor \log i \rfloor - 1}\, b\, w_{\lfloor \log i \rfloor}\left(i - 2^{\lfloor \log i \rfloor}\right). \tag{3}$$

We first show that

$$w_k\left(2^\ell - 1\right) = \alpha_{k,\ell-1}\, u_{\ell-1}\, b \tag{4}$$

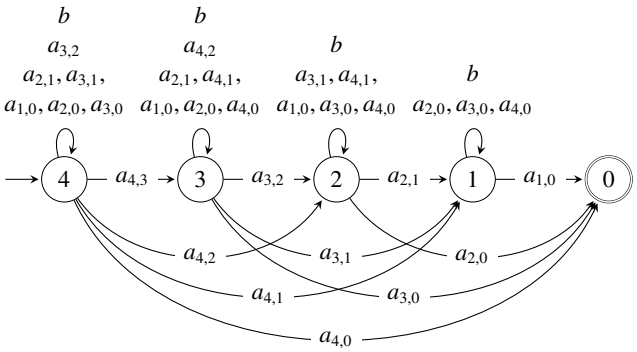

Figure 7: Automaton $\mathcal{A}_4$ of Theorem 7

$$
\begin{aligned}
w_3(0) &= \underline{a_{3,0}} \\
w_3(1) &= \underline{a_{3,0}}\, b \\
w_3(2) &= \underline{a_{3,1}} a_{3,0}\, b\, \underline{a_{1,0}} \\
w_3(3) &= \underline{a_{3,1}} a_{3,0}\, b\, \underline{a_{1,0}}\, b \\
w_3(4) &= \underline{a_{3,2}} a_{3,1} a_{3,0}\, b\, a_{1,0}\, b\, \underline{a_{2,0}} \\
w_3(5) &= \underline{a_{3,2}} a_{3,1} a_{3,0}\, b\, a_{1,0}\, b\, \underline{a_{2,0}}\, b \\
w_3(6) &= \underline{a_{3,2}} a_{3,1} a_{3,0}\, b\, a_{1,0}\, b\, \underline{a_{2,1}} a_{2,0}\, b\, \underline{a_{1,0}} \\
w_3(7) &= \underline{a_{3,2}} a_{3,1} a_{3,0}\, b\, a_{1,0}\, b\, \underline{a_{2,1}} a_{2,0}\, b\, \underline{a_{1,0}}\, b
\end{aligned}
$$

Figure 8: The tower between $L(\mathcal{A}_3)$ and $L(\mathcal{B}_3)$. We underline transitions between different states in $\mathcal{A}_3$.

holds for each k and each $1 \le \ell \le k$. This is true for $\ell = 1$. For $\ell > 1$, we have from (3) and by induction

$$
w_k\left(2^\ell - 1\right) = \alpha_{k,\ell-1}\, u_{\ell-2}\, b\, w_{\ell-1}\left(2^{\ell-1} - 1\right) = \alpha_{k,\ell-1}\, u_{\ell-2}\, b\, \alpha_{\ell-1,\ell-2}\, u_{\ell-2}\, b = \alpha_{k,\ell-1}\, u_{\ell-1}\, b\,.
$$

By double induction on n and i, we now prove that the sequence $(w_n(i))_{i=0}^{2^n-1}$ is the required tower. For $n = 1$, the claim holds, and the tower is $w_1(0) = a_{1,0}$, $w_1(1) = a_{1,0}\, b$. Let $n > 1$. The definition implies, by induction, that $w_n(i)$ is in $L(\mathcal{B}_n)$ (that is, it ends with b) if and only if i is odd. Consider $w_n(i)$ with even $i \ge 2$. Using (3), we show that there is a path in $\mathcal{A}_n$ labeled by $w_n(i)$ and it can be decomposed as

$$
n \xrightarrow{a_{n,\lfloor \log i \rfloor}} \lfloor \log i \rfloor \xrightarrow{\alpha_{n,\lfloor \log i \rfloor - 1}\, u_{\lfloor \log i \rfloor - 1}\, b} \lfloor \log i \rfloor \xrightarrow{w_{\lfloor \log i \rfloor}\left(i - 2^{\lfloor \log i \rfloor}\right)} 0\,.
$$

For the second segment of the path, note that both the alphabet of $\alpha_{n,\lfloor \log i \rfloor - 1}$ and the alphabet $\{b\} \cup \{a_{m,m'} \mid m \le \lfloor \log i \rfloor - 1, m' < m\}$ of $u_{\lfloor \log i \rfloor - 1}\, b$ are contained in the alphabet of self-loops of state $\lfloor \log i \rfloor$. The last segment exists by induction, since $\lfloor \log i \rfloor < n$, $i - 2^{\lfloor \log i \rfloor} \le 2^{\lfloor \log i \rfloor} - 1$, the automaton $\mathcal{A}_{\lfloor \log i \rfloor}$ is a restriction of $\mathcal{A}_n$, and $i - 2^{\lfloor \log i \rfloor}$ is even.

We show that $w_n(i) \preccurlyeq w_n(i+1)$. This is true for $i = 0$, and follows by induction from (3) if $\lfloor \log(i+1) \rfloor = \lfloor \log i \rfloor$. The latter equality holds unless i is of the form $2^\ell - 1$ for some $\ell > 1$. If $i = 2^\ell - 1$, then $\ell - 1 = \lfloor \log i \rfloor \ne \lfloor \log(i+1) \rfloor = \ell$ and we have from (4)

$$
\begin{aligned}
w_n\left(2^\ell - 1\right) &= \alpha_{n,\ell-1}\, u_{\ell-1}\, b, \\
w_n\left(2^\ell\right) &= \alpha_{n,\ell}\, u_{\ell-1}\, b\, w_\ell(0) = \alpha_{n,\ell}\, u_{\ell-1}\, b\, a_{\ell,0}\,,
\end{aligned}
$$

hence $w_n\left(2^\ell - 1\right) \preccurlyeq w_n\left(2^\ell\right)$ holds.

Finally, observe that if $(v_i)_i$ is a tower between $\mathcal{A}_n$ and $\mathcal{B}_n$, then $(P(v_i)_i)$ is a tower between $\mathcal{A}_{n,0,1}$ and $\mathcal{B}_{n,0,1}$ of Theorem 4, where $P\colon a_{k,j} \mapsto a_k$ is the natural projection. Therefore there is no infinite tower between $\mathcal{A}_n$ and $\mathcal{B}_n$. □

The "determinization" idea of the previous theorem can be generalized. However, compared to the proof of Theorem 7, the general procedure suffers from the increase of states (see Figure 9). The reason why we need not increase the number of states in the proof of Theorem 7 is that the automata we are "determinizing" are such that there is an order in which the transitions/states are used/visited, and that the nondeterministic transitions are acyclic.

Theorem 8. *For every two NFAs $\mathcal{A}$ and $\mathcal{B}$ with at most n states and k input letters, there exist two DFAs $\mathcal{A}'$ and $\mathcal{B}'$ with $O\left(n^2\right)$ states and $O(k+n)$ input letters such that there is a tower of height r between $\mathcal{A}$ and $\mathcal{B}$ if and only if there is a tower of height r between $\mathcal{A}'$ and $\mathcal{B}'$. In particular, there is an infinite tower between $\mathcal{A}$ and $\mathcal{B}$ if and only if there is an infinite tower between $\mathcal{A}'$ and $\mathcal{B}'$.*

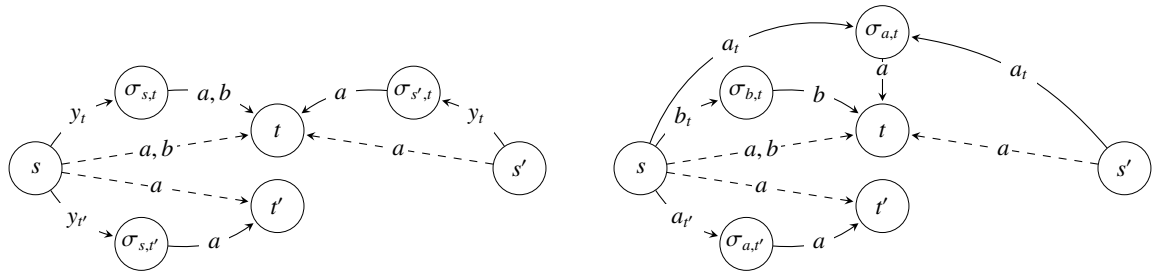

Figure 9: Determinization by Theorem 8 and Theorem 9 respectively. (Self-loops under new letters in σ-states omitted.)

Proof. Let $\mathcal{A}$ and $\mathcal{B}$ be two NFAs with at most n states over an alphabet Σ of cardinality k. We first add a unique initial state, if necessary, to the automata $\mathcal{A}$ and $\mathcal{B}$ and the corresponding transitions in the standard way. Assume now that $\mathcal{A}$ and $\mathcal{B}$ have a unique initial state, and let Q_A and Q_B denote their respective sets of states. We modify the automata $\mathcal{A}$ and $\mathcal{B}$ to obtain the DFAs $\mathcal{A}'$ and $\mathcal{B}'$ as follows. Let $Q_{A'} = Q_A \cup \{\sigma_{s,t} \mid s, t \in Q_A\}$ and $Q_{B'} = Q_B \cup \{\sigma_{s,t} \mid s, t \in Q_B\}$, where $\sigma_{s,t}$ are new states. We introduce a new letter y_t for every state $t \in Q_A \cup Q_B$. It results in $O\left(n^2\right)$ states and $O(k+n)$ letters. The transition function is defined as follows. In both automata, each transition $s \xrightarrow{a} t$ is replaced with two transitions $s \xrightarrow{y_t} \sigma_{s,t}$ and $\sigma_{s,t} \xrightarrow{a} t$. Moreover, self-loops in all new states are added over all new letters. Note that all transitions are deterministic in $\mathcal{A}'$ and $\mathcal{B}'$.

We now prove that if there is a tower of height r between $\mathcal{A}$ and $\mathcal{B}$, then there is a tower of height r between $\mathcal{A}'$ and $\mathcal{B}'$. Informally, given a tower between $\mathcal{A}$ and $\mathcal{B}$, in order to obtain a tower between $\mathcal{A}'$ and $\mathcal{B}'$, a sequence of "directing" symbols is inserted before each letter in the tower. "Directing" symbols record the list of transitions the corresponding letter will be responsible for in the rest of the tower. Formally, let $(w_i)_{i=1}^r$ be a tower between $\mathcal{A}$ and $\mathcal{B}$. Let $\ell = |w_r|$ and

$$w_r = x_{r,1}x_{r,2}\cdots x_{r,\ell}\,,$$

with $x_{r,j} \in \Sigma$. Next, for $i = 1, 2, \ldots, r-1$, let

$$w_i = x_{i,1}x_{i,2}\cdots x_{i,\ell}$$

where $x_{i,j}$ is either a letter or the empty word such that $x_{i,j} \preccurlyeq x_{i+1,j}$ for each $i = 1, 2, \ldots, r-1$ and $j = 1, 2, \ldots, \ell$. For every w_i, we fix an accepting path π_i in the corresponding automaton. Let $p_{i,j}$ be the letter y_t where $s \to t$ is the transition corresponding to $x_{i,j}$ in π_i if $x_{i,j}$ is a letter, and let $p_{i,j}$ be empty if $x_{i,j}$ is empty. We define

$$w'_i = \alpha_{i,1}\alpha_{i,2}\cdots\alpha_{i,\ell}$$

where $\alpha_{i,j} = p_{i,j}p_{i-1,j}\cdots p_{1,j}x_{i,j}$ if $x_{i,j} \neq \varepsilon$, and $\alpha_{i,j} = x_{i,j} = \varepsilon$ otherwise. It is straightforward to verify that $\left(w'_i\right)_{i=1}^r$ is a tower of height r between $\mathcal{A}'$ and $\mathcal{B}'$.

Let now $\left(w'_i\right)_{i=1}^r$ be a tower between $\mathcal{A}'$ and $\mathcal{B}'$. We show that $\left(P\left(w'_i\right)\right)_{i=1}^r$ is a tower between $\mathcal{A}$ and $\mathcal{B}$, where P is a projection erasing all new letters. Obviously, we have $P\left(w'_i\right) \preccurlyeq P\left(w'_{i+1}\right)$. We now show that if a word w' is accepted by $\mathcal{A}'$, then $P(w')$ is accepted by $\mathcal{A}$. Let π' be the path accepting w', and let $\tau'_1, \tau'_2, \ldots, \tau'_d$ denote the sequence of all transitions of π' labeled with letters from Σ in the order they appear in π'. By construction, τ'_i is of the form $\sigma_{s_{i-1},s_i} \xrightarrow{a_i} s_i$ for some states $s_{i-1}, s_i \in Q_A$, $i = 1, 2, \ldots, d$, with s_0 being initial and s_k being accepting. Moreover, for $i < d$, the transition τ'_i is immediately followed in π' by $s_i \xrightarrow{y_{s_{i+1}}} \sigma_{s_i,s_{i+1}}$. Let τ_i be $s_{i-1} \xrightarrow{a_i} s_i$. It is straightforward to verify that $\tau_1, \tau_2, \ldots, \tau_d$ is an accepting path of $P(w')$ in $\mathcal{A}$. Analogously for $\mathcal{B}'$ and $\mathcal{B}$. The fact that the existence of towers of arbitrary height is equivalent to the existence of an infinite tower then concludes the proof. □

A similar construction yields the following variant of the previous theorem.

Theorem 9. *For every two NFAs $\mathcal{A}$ and $\mathcal{B}$ with at most n states and k input letters, there exist two DFAs $\mathcal{A}'$ and $\mathcal{B}'$ with $O(kn)$ states and $O(kn)$ input letters such that there is a tower of height r between $\mathcal{A}$ and $\mathcal{B}$ if and only if there is a tower of height r between $\mathcal{A}'$ and $\mathcal{B}'$. In particular, there is an infinite tower between $\mathcal{A}$ and $\mathcal{B}$ if and only if there is an infinite tower between $\mathcal{A}'$ and $\mathcal{B}'$.*

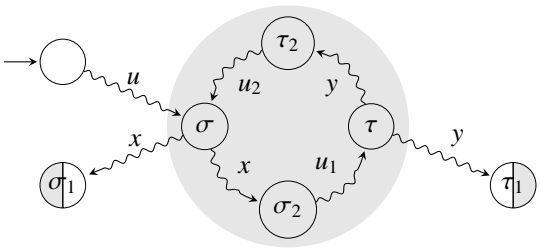

Figure 10: The pattern $(\sigma, \sigma_1, \sigma_2, \tau, \tau_1, \tau_2)$

Proof. Let $Q_{A'} = Q_A \cup \{\sigma_{a,t} \mid a \in \Sigma,\, t \in Q_A\}$ and $Q_{B'} = Q_B \cup \{\sigma_{a,t} \mid a \in \Sigma,\, t \in Q_B\}$, where $\sigma_{a,t}$ are new states. The alphabet of $\mathcal{A}'$ and $\mathcal{B}'$ is $\Sigma \cup \{a_t \mid a \in \Sigma, t \in Q_A \cup Q_B\}$. We have $O(kn)$ states and letters. Each transition $s \xrightarrow{a} t$, in both automata, is replaced with two transitions $s \xrightarrow{a_t} \sigma_{a,t}$ and $\sigma_{a,t} \xrightarrow{a} t$. Self-loops in all new states are added over all new letters. The rest of the proof is analogous to the proof of Theorem 8. □

5. Towers of prefixes

It is remarkable that lower bounds on the height of finite towers for NFAs in this paper were obtained by examples where w_i is not just a subsequence of w_{i+1} but even its prefix (sometimes this rule is violated by the last element of the tower). In this section we therefore investigate what can be said about alternating towers of prefixes. A simple example of languages $L_1 = a(ba)^*$ and $L_2 = b(ab)^*$ shows that the towers of prefixes and towers (of subsequences) may behave differently. Indeed, there is no infinite tower of prefixes between L_1 and L_2, since every word of L_1 begins with a and thus cannot be a prefix of a word of L_2, which begins with b. But there is an infinite tower, namely, $a, bab, ababa, \ldots$. We first describe a pattern on two automata $\mathcal{A}$ and $\mathcal{B}$ that characterizes the existence of an infinite tower of prefixes between them.

Let $\mathcal{A} = (Q_A, \Sigma, \delta_A, I_A, F_A)$ and $\mathcal{B} = (Q_B, \Sigma, \delta_B, I_B, F_B)$ be two NFAs. We say that $(\sigma, \sigma_1, \sigma_2, \tau, \tau_1, \tau_2)$ is a *pattern* of the automata $\mathcal{A}$ and $\mathcal{B}$ if σ, σ_1, σ_2, τ, τ_1, τ_2 are states of the product automaton such that

- $\sigma_1 \in F_A \times Q_B$ and $\tau_1 \in Q_A \times F_B$,
- σ is reachable from an initial state,
- states σ_1 and σ_2 are reachable from state σ under a common word,
- states τ_1 and τ_2 are reachable from state τ under a common word, and
- τ is reachable from σ_2 and σ is reachable from τ_2.

The definition is illustrated in Figure 10. We allow any of the words in the definition to be empty, with the convention that any state is reachable from itself under the empty word. The following theorem provides a characterization for the existence of an infinite tower of prefixes.

Theorem 10. *Let $\mathcal{A}$ and $\mathcal{B}$ be two NFAs. Then there is an infinite tower of prefixes between $\mathcal{A}$ and $\mathcal{B}$ if and only if there is a pattern of automata $\mathcal{A}$ and $\mathcal{B}$.*

Proof. Let $(\sigma, \sigma_1, \sigma_2, \tau, \tau_1, \tau_2)$ be a pattern of the automata $\mathcal{A}$ and $\mathcal{B}$. Let u be a word under which state σ is reachable from an initial state (q_A, q_B), x (y resp.) be a word under which both σ_1 and σ_2 (τ_1 and τ_2 resp.) are reachable from σ (τ resp.), u_1 be a word under which τ is reachable from σ_2, and u_2 a word under which σ is reachable from τ_2, see Figure 10. We then have an infinite tower of prefixes ux, $ux(u_1y)$, $ux(u_1y)(u_2x)$, $ux(u_1y)(u_2x)(u_1y)$, ...

Assume now that there exists an infinite tower of prefixes $(w_i)_{i=1}^{\infty}$ between the languages $L(\mathcal{A})$ and $L(\mathcal{B})$. Consider the automaton $\det(\mathcal{A} \times \mathcal{B})$, the determinization of $\mathcal{A} \times \mathcal{B}$ by the standard subset construction, and let $q_{\mathcal{A}\times\mathcal{B}}$ be its initial state. A sufficiently long element of the tower defines a path

$$q_{\mathcal{A}\times\mathcal{B}} \xrightarrow{u} X \xrightarrow{z_X} Y \xrightarrow{z_Y} X$$

in the automaton $\det(\mathcal{A}\times\mathcal{B})$, such that X contains a state $(f_1, q_1) \in F_A \times Q_B$ and Y contains a state $(q_2, f_2) \in Q_A \times F_B$. For every state of X, there exists an incoming path from an element of Y labeled by z_Y since $X = \delta_{\mathcal{A}\times\mathcal{B}}(Y, z_Y)$. Similarly, for every state of Y, there exists an incoming path from an element of X labeled by z_X since $Y = \delta_{\mathcal{A}\times\mathcal{B}}(X, z_X)$. Thus, there are infinitely many paths from X to X labeled with words from $(z_Xz_Y)^+$ ending in state (f_1, q_1). Therefore, there exists a state $(s_1, t_1) \in X$ and integers k_1 and ℓ_1 such that

$$(s_1, t_1) \xrightarrow{(z_Xz_Y)^{k_1}} (s_1, t_1) \xrightarrow{(z_Xz_Y)^{\ell_1}} (f_1, q_1)\,.$$

Similarly, there exists a state $(s_2, t_2) \in X$ and integers k_2 and ℓ_2 such that

$$(s_2, t_2) \xrightarrow{(z_Xz_Y)^{k_2}} (s_2, t_2) \xrightarrow{(z_Xz_Y)^{\ell_2}z_X} (q_2, f_2)\,.$$

Let $\sigma = \tau = (s_1, t_2)$. Since $(q_{\mathcal{A}\times\mathcal{B}}) \xrightarrow{u} (s_i, t_i)$, $i = 1, 2$, also $(q_{\mathcal{A}\times\mathcal{B}}) \xrightarrow{u} \sigma$. Let $x = (z_Xz_Y)^{\ell_1}$ and $y = (z_Xz_Y)^{\ell_2}z_X$. Then $\sigma \xrightarrow{x} (f_1, t_3)$ where t_3 is a state in the cycle $t_2 \xrightarrow{(z_Xz_Y)^{k_2}} t_2$ in $\mathcal{B}$. Similarly, $\tau \xrightarrow{y} (s_3, f_2)$ where s_3 is a state in the cycle $s_1 \xrightarrow{(z_Xz_Y)^{k_1}} s_1$ in $\mathcal{A}$. We set $\sigma_1 = (f_1, t_3)$ and $\tau_1 = (s_3, f_2)$. The pattern is completed by states σ_2 and τ_2, such that

$$\sigma \xrightarrow{x} \sigma_2 \xrightarrow{u_1} \tau \xrightarrow{y} \tau_2 \xrightarrow{u_2} \sigma$$

where u_1 and u_2 can be chosen as $u_1 = (z_Xz_Y)^{\ell_1k_1k_2-\ell_1}$ and $u_2 = z_Y(z_Xz_Y)^{\ell_2k_1k_2-\ell_2-1}$. □

We point out that the identification is easy. It could even be shown that to decide whether there is a pattern between the automata, that is, whether there is an infinite tower of prefixes, is an NL-complete problem for both NFAs and DFAs (cf. our technical report [7]). This is in contrast to deciding the existence of an infinite tower of subsequences, which is PTime-complete [10]. Notice that if there is a pattern, then there is also a pattern with $\sigma = \tau$ as shown in the proof above. From the point of view of finding the pattern, however, it is more natural to keep the more general definition of the pattern given above.

We have already mentioned that if there are towers of arbitrary height, then there is an infinite tower. This property holds for any relation that is a well quasi order (WQO) [3, Lemma 6] of which the subsequence relation is an instance. The prefix relation is not a WQO. However, Theorem 10 and its proof shows that the pattern and therefore also an infinite tower of prefixes can be found as soon as there exists a sufficiently long tower of prefixes. On the other hand, this argument depends on the fact that the languages are regular. Indeed, the following example shows that the property in general does not hold for non-regular languages.

Example 11. Let $K = \{a, b\}^*a$ and $L = \{a^m(ba^*)^nb \mid m > n \geq 0\}$ be two languages. Note that K is regular and L is non-regular context-free. The languages are disjoint, since the words of K end with a and the words of L with b. For any $r \geq 1$, the words $w_{2i+1} = a^r(ba)^i \in K$ and $w_{2(i+1)} = a^r(ba)^ib \in L$ for $i = 0, 1, \ldots, r-1$ form a tower of prefixes between K and L of height $2r$. On the other hand, let $w_1, w_2, \ldots$ be a tower of prefixes between the languages K and L. Without loss of generality, we may assume that w_1 belongs to L. Then $a^\ell b$ is a prefix of w_1 for some $\ell \geq 1$. It is not hard to see that $|w_i|_b < |w_{i+2}|_b$ holds for any $w_i \leq w_{i+1} \leq w_{i+2}$ with w_i, w_{i+2} in L and w_{i+1} in K. As any word of L with a prefix $a^\ell b$ can have at most ℓ occurrences of letter b, the tower cannot be infinite.

Given that the height of finite towers of prefixes for regular languages is bounded, we now investigate the bound. We need the following auxiliary combinatorial lemma, which is fairly straightforward, but its proof is technical, and therefore we formulate it outside the main proof.

Lemma 12. *Let $k_1, \ell_1, k_2, \ell_2 \geq 0$ be integers such that $k_1+k_2 > 0$ and $\ell_1+\ell_2 > 0$. Then $2\cdot\min(k_1k_2, \ell_1\ell_2) \leq \frac{(k_1+\ell_1)(k_2+\ell_2)}{2}$. Moreover, if $k_1k_2 \neq \ell_1\ell_2$, then $2 \cdot \min(k_1k_2, \ell_1\ell_2) + 1 \leq \frac{(k_1+\ell_1)(k_2+\ell_2)}{2}$.*

Proof. Suppose that $k_1 = 0$. Then the first claim is obvious. If $k_1k_2 \neq \ell_1\ell_2$, then $\ell_1, \ell_2 > 0$. Since also $k_2 > 0$, we get the second claim. By symmetry, we shall further suppose that $k_1, \ell_1, k_2, \ell_2 \geq 1$.

Let us now assume that $k_1 \leq \ell_1$ and $k_2 < \ell_2$. Then

$$2\min(k_1k_2, \ell_1\ell_2) + 1 = 2k_1k_2 + 1 \leq 2k_1k_2 + k_1 = \frac{2k_1(2k_2+1)}{2} \leq \frac{(k_1+\ell_1)(k_2+\ell_2)}{2}\,.$$

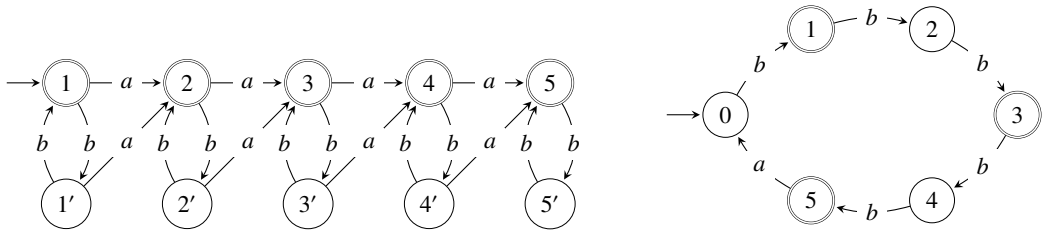

Figure 11: DFAs $\mathcal{A}_d$ and $\mathcal{B}_e$ of Theorem 14 for $d = e = 5$

By symmetry, it remains to consider cases $k_i \le \ell_i$, $\ell_j \le k_j$, $\{i, j\} = \{1, 2\}$. Then

$$2\min(k_1k_2, \ell_1\ell_2) + |k_1k_2 - \ell_1\ell_2| = k_1k_2 + \ell_1\ell_2 \le k_1k_2 + \ell_1\ell_2 + \frac{(k_1 - \ell_1)(\ell_2 - k_2)}{2} = \frac{(k_1 + \ell_1)(k_2 + \ell_2)}{2},$$

which concludes the proof. □

For DFAs we now have the following bound.

Theorem 13. *Let $\mathcal{A}$ and $\mathcal{B}$ be two DFAs with n and m states that have no infinite tower of prefixes. Then the height of a tower of prefixes between $\mathcal{A}$ and $\mathcal{B}$ is at most $\frac{nm}{2} + 1$.*

Proof. Let $\mathcal{A} = (Q_\mathcal{A}, \Sigma, \delta_\mathcal{A}, q_\mathcal{A}, F_\mathcal{A})$ and $\mathcal{B} = (Q_\mathcal{B}, \Sigma, \delta_\mathcal{B}, q_\mathcal{B}, F_\mathcal{B})$, and let $X = F_\mathcal{A} \times (Q_\mathcal{B} \setminus F_\mathcal{B})$ and $Y = (Q_\mathcal{A} \setminus F_\mathcal{A}) \times F_\mathcal{B}$. Final states $(p_i, q_i) = \delta((q_\mathcal{A}, q_\mathcal{B}), w_i)$ of any tower of prefixes $(w_i)_{i=1}^r$ between $\mathcal{A}$ and $\mathcal{B}$ in the product automaton $\mathcal{A} \times \mathcal{B}$ have to alternate between the states of X and Y, with the exception of w_r: there may be no path labeled by w_r in the non-accepting automaton, and therefore also no path in the product automaton $\mathcal{A} \times \mathcal{B}$ (recall our convention not to consider states that do not appear on an accepting path).

If $(p_i, q_i) = (p_j, q_j)$ for some $1 \le i < j < r$, then there is a path

$$(q_\mathcal{A}, q_\mathcal{B}) \xrightarrow{w_i} (p_i, q_i) \xrightarrow{u} (p_{i+1}, q_{i+1}) \xrightarrow{v} (p_i, q_i)$$

with $w_{i+1} = w_iu$ and $w_j = w_iuv$. Then there is an infinite tower of prefixes $w_i, w_iu, w_iuv, w_iuvu, \ldots$, a contradiction. Therefore, it remains to show that there may be at most $\frac{nm}{2}$ alternations without repeated states between X and Y.

If $|X| = |Y|$, then there are at most $2 \cdot \min(|X|, |Y|)$ such alternations, and if $|X| \ne |Y|$, then there are at most $2 \cdot \min(|X|, |Y|) + 1$ such alternations. In both cases, the proof is completed by Lemma 12 with $k_1 = |F_\mathcal{A}|$, $\ell_2 = |F_\mathcal{B}|$, $k_1 + \ell_1 = n$ and $k_2 + \ell_2 = m$, noting that for $k_1 = 0$ or $\ell_2 = 0$ the claim holds since then $L(\mathcal{A})$ or $L(\mathcal{B})$ is empty. □

The following theorem allows to conclude that the above bound is tight.

Theorem 14. *For every positive integer d and every odd positive integer e, there exists a binary DFA with $2d$ states and a binary DFA with $e + 1$ states having a tower of prefixes of height $d(e + 1) + 1$ and no infinite tower.*

Proof. We consider the proof of Theorem 2, but instead of taking the NFA $\mathcal{A}_d$, we take its DFA equivalent, which has $2d$ states and, for simplicity, we denote it $\mathcal{A}_d$ as well, cf. Figure 11. From Theorem 2, there is no infinite tower between the languages, and hence there is also no infinite tower of prefixes between the DFAs.

Consider the word $w = (b^e a)^{d-1} b^{e+1}$. By the proof of Theorem 2, $\mathcal{A}_d$ accepts all prefixes of w ending with an even number of b's, including those ending with a, and $\mathcal{B}_e$ accepts all prefixes of w ending with an odd number of b's. The sequence $(w_i)_{i=1}^{|w|+1}$, where w_i is the prefix of w of length $i - 1$ for $i = 1, 2, \ldots, |w| + 1$, is therefore a tower of prefixes between $\mathcal{A}_d$ and $\mathcal{B}_e$ of height $|w| + 1 = (e + 1)(d - 1) + e + 1 + 1 = d(e + 1) + 1$. (The last word of the tower in Theorem 2 does not fit to a prefix tower.) □

The following corollary now states that the bound of Theorem 13 is tight.

Corollary 15. *For all even positive integers n and m, there exist binary DFAs with n and m states having a tower of prefixes of height $\frac{nm}{2} + 1$ and no infinite tower.*

Proof. The claim follows from Theorem 14 by setting $d = \frac{n}{2}$ and $e = m - 1$. □

Comparing towers of subsequences and prefixes with respect to the number of states of DFAs, Theorem 7 shows that there are towers of subsequences of exponential height, while Theorem 13 gives a quadratic bound on the height of towers of prefixes. It shows an exponential gap between the height of towers of subsequences and prefixes for DFAs. What is the situation for NFAs? An immediate consequence of the NFA-to-DFA transformation and Theorem 13 give the following asymptotically tight bound.

Corollary 16. *Given two NFAs with at most n and m states and with no infinite tower of prefixes, the height of a tower of prefixes between them is at most* $2^{n+m-1} - 2^{n-1} - 2^{m-1} + 1$. *Moreover, the lower bound is* $2^{n+m-2} - 2^{m-2} + 1$ *for any* $n, m \geq 2$.

Proof. Let two NFAs with n and m states be given. Their corresponding minimal DFAs have at most $2^n - 1$ and $2^m - 1$ nonempty states. By Theorem 13, the upper bound on the height of towers of prefixes is $\frac{1}{2}(2^n - 1)(2^m - 1) + 1$. Taking the integer part, the height is at most $\frac{(2^n-1)(2^m-1)+1}{2} = 2^{n+m-1} - 2^{n-1} - 2^{m-1} + 1$.

The lower bound is obtained from Theorem 4 and Remark 1. □

A natural question is whether there are any requirements on the size of the alphabet in case of automata with exponentially high towers of prefixes. The following corollary shows that the alphabet can be binary and the tower is still more than polynomial in the number of states.

Corollary 17. *For any n there are binary NFAs with at most n states with no infinite tower of prefixes and with a tower of prefixes of a superpolynomial height with respect to n.*

Proof. An automaton over the alphabet of cardinality k can be transformed into a binary automaton in the obvious way: replace each letter with its binary code of length $\log k$, and replace every transition by a path with $\log k - 1$ new states. Note that the property of being a tower of prefixes between two automata is preserved by the transformation.

Consider automata $\mathcal{A}_{j,j}$ and $\mathcal{B}_{j,j}$ of Theorem 4. It can be calculated that each of them has less than $2j^2$ transitions. Therefore, by the transformation, we obtain binary automata $\mathcal{A}'_{j,j}$ and $\mathcal{B}'_{j,j}$, each with at most $2j^2 \log 2j$ states. By Remark 1, the transformed automata have no infinite tower of prefixes and a finite tower of prefixes of height at least 2^{2j-3}. Choosing

$$j = \left\lfloor \sqrt{\frac{n}{2 \log 2n}} \right\rfloor,$$

the binary automata $\mathcal{A}'_{j,j}$ and $\mathcal{B}'_{j,j}$ have at most n states, and they have a tower of prefixes of height

$$\Omega\left(2^{\sqrt{\frac{2n}{\log 2n}}}\right).$$

□

The following question is open.

Open Problem 2. Given two NFAs with n and m states over a fixed alphabet with m letters. Assume that there is no infinite tower of prefixes between the automata. What is the tight bound on the height of towers of prefixes?

6. Conclusion

We investigated the height of finite towers between two regular languages as a function of the number of states of the automata representing the languages. We also paid attention to three additional parameters: (non)determinism, the structure of the tower (formed by subsequences or by prefixes), and the size of the alphabet. The connection between the parameters is summarized as follows.

The NFA vs. DFA representation does not play a crucial role since any tower between two NFAs can be "determinized" to a tower between two DFAs with only a moderate increase of the number of states.

A difference between towers of subsequences and towers of prefixes is less clear. It is conspicuous that our best, exponentially high towers are essentially towers of prefixes. We want to stress that this was not an intention but rather a surprising observation. Although this holds only for NFAs, it is worth noting that the proper subsequence relation is used exclusively in the determinization constructions. It leaves an intriguing open question whether, in the nondeterministic case, there is any substantial difference between towers of subsequences and towers of prefixes. In other words, the question is whether the subsequence relation can be simulated by the prefix relation using nondeterminism.

The real influence of the alphabet size is also unclear. We have seen that the height of towers grows exponentially with the alphabet size up to the point when the alphabet size is roughly the same as the number of states. The second intriguing question is thus whether the towers can grow beyond this point using a larger alphabet. The unconditional upper bound we have obtained is $O\left(n^{|\Sigma|}\right)$, where the only limit on the size of Σ is the trivial bound 2^{n^2} on the number of inequivalent letters in an n-state NFA (a letter a can be identified with the mapping $\delta(\cdot, a) : Q \to 2^Q$).

The lack of understanding of the impact of the alphabet size seems to be related to the fact that the estimate of the number κ in Place et al. [12] is doubly exponential in the alphabet size. On a positive side, the difficulty to find examples of very high towers means that the construction suggested in Section 2.1 is going to be rather fast on typical instances. This should be contrasted with the construction by Place et al. [12], where the huge number κ is prohibitive, even if suspected to be overestimated.

The two open questions formulated in the paper are related. If, for NFAs, towers of prefixes are as high as towers of subsequences, then $\Theta(2^{n+m})$ is the optimal bound (cf. Open Problem 1).

To conclude, we inform the reader that slightly better bounds can be obtained in specific constellations by more technical constructions that can be found in the technical report of this paper [8]. We present simplified constructions in this paper since they do not have any impact on the asymptotic results.

Acknowledgements. We are grateful to anonymous referees for their suggestions that allowed to improve and simplify the exposition.

References

[1] Almeida, J., 1990. Implicit operations on finite J-trivial semigroups and a conjecture of I. Simon. Journal of Pure and Applied Algebra 69, 205–218.
[2] Almeida, J., 1995. Finite semigroups and universal algebra. Vol. 3 of Series in Algebra. World Scientific.
[3] Czerwiński, W., Martens, W., Masopust, T., 2013. Efficient separability of regular languages by subsequences and suffixes. In: Fomin, F. V., Freivalds, R., Kwiatkowska, M. Z., Peleg, D. (Eds.), International Colloquium on Automata, Languages and Programming (ICALP). Vol. 7966 of LNCS. Springer, pp. 150–161, full version available at http://arxiv.org/abs/1303.0966.
[4] Czerwiński, W., Martens, W., van Rooijen, L., Zeitoun, M., Zetzsche, G., 2017. A characterization for decidable separability by piecewise testable languages. Discrete Mathematics & Theoretical Computer Science 19 (4).
[5] Higman, G., 1952. Ordering by divisibility in abstract algebras. Proceedings of the London Mathematical Society s3-2 (1), 326–336.
[6] Holub, Š., Jirásková, G., Masopust, T., 2014. On upper and lower bounds on the length of alternating towers. In: Csuhaj-Varjú, E., Dietzfelbinger, M., Ésik, Z. (Eds.), Mathematical Foundations of Computer Science (MFCS). Vol. 8634 of LNCS. Springer, pp. 315–326.
[7] Holub, Š., Masopust, T., Thomazo, M., 2014. Alternating towers and piecewise testable separators. CoRR abs/1409.3943.
[8] Holub, Š., Masopust, T., Thomazo, M., 2017. On the height of towers of subsequences and prefixes. CoRR abs/1705.02813.
[9] Karandikar, P., Kufleitner, M., Schnoebelen, P., 2015. On the index of Simon's congruence for piecewise testability. Information Processing Letters 115 (4), 515–519.
[10] Masopust, T., 2018. Separability by piecewise testable languages is PTime-complete. Theoretical Computer Science 711, 109–114.
[11] Masopust, T., Krötzsch, M., 2018. Deciding universality of ptNFAs is PSpace-complete. In: Tjoa, A. M., Bellatreche, L., Biffl, S., van Leeuwen, J., Wiedermann, J. (Eds.), International Conference on Current Trends in Theory and Practice of Computer Science (SOFSEM). Vol. 10706 of LNCS. Springer, pp. 413–427.
[12] Place, T., van Rooijen, L., Zeitoun, M., 2013. Separating regular languages by piecewise testable and unambiguous languages. In: Chatterjee, K., Sgall, J. (Eds.), Mathematical Foundations of Computer Science (MFCS). Vol. 8087 of LNCS. Springer, pp. 729–740.
[13] Stern, J., 1985. Characterizations of some classes of regular events. Theoretical Computer Science 35, 17–42.