

# The Big-O Problem for Labelled Markov Chains and Weighted Automata

Dmitry Chistikov 

Centre for Discrete Mathematics and its Applications (DIMAP) & Department of Computer Science, University of Warwick, Coventry, UK

Stefan Kiefer

Department of Computer Science, University of Oxford, UK

Andrzej S. Murawski

Department of Computer Science, University of Oxford, UK

David Purser 

Centre for Discrete Mathematics and its Applications (DIMAP) & Department of Computer Science, University of Warwick, Coventry, UK

Max Planck Institute for Software Systems, Saarland Informatics Campus, Germany

---

## Abstract

Given two weighted automata, we consider the problem of whether one is big-O of the other, i.e., if the weight of every finite word in the first is not greater than some constant multiple of the weight in the second.

We show that the problem is undecidable, even for the instantiation of weighted automata as labelled Markov chains. Moreover, even when it is known that one weighted automaton is big-O of another, the problem of finding or approximating the associated constant is also undecidable.

Our positive results show that the big-O problem is polynomial-time solvable for unambiguous automata, **coNP**-complete for unlabelled weighted automata (i.e., when the alphabet is a single character) and decidable, subject to Schanuel's conjecture, when the language is bounded (i.e., a subset of  $w_1^* \dots w_m^*$  for some finite words  $w_1, \dots, w_m$ ).

On labelled Markov chains, the problem can be restated as a ratio total variation distance, which, instead of finding the maximum difference between the probabilities of any two events, finds the maximum ratio between the probabilities of any two events. The problem is related to  $\epsilon$ -differential privacy, for which the optimal constant of the big-O notation is exactly  $\exp(\epsilon)$ .

**2012 ACM Subject Classification** Theory of computation  $\rightarrow$  Probabilistic computation

**Keywords and phrases** weighted automata, labelled Markov chains, probabilistic systems

**Funding** *Dmitry Chistikov*: Supported in part by the Royal Society International Exchanges scheme (IEC\R2\170123).

*Stefan Kiefer*: Supported by a Royal Society Research Fellowship.

*Andrzej S. Murawski*: Supported by a Royal Society Leverhulme Trust Senior Research Fellowship and the International Exchanges Scheme (IE161701).

*David Purser*: Supported by the UK EPSRC Centre for Doctoral Training in Urban Science (EP/L016400/1) and in part by the Royal Society International Exchanges scheme (IEC\R2\170123).

**Acknowledgements** The authors would like to thank to Engel Lefauchaux, Joël Ouaknine, and James Worrell for discussions during the development of this work.

## 1 Introduction

Weighted automata over finite words are a well-known and powerful model of computation, a quantitative analogue of finite-state automata. Special cases of weighted automata include nondeterministic finite automata and labelled Markov chains, two standard formalisms for modelling systems and processes. Algorithms for analysis of weighted automata have been

studied both in the early theory of computing and more recently by the infinite-state systems and algorithmic verification communities.

Given two weighted automata  $\mathcal{A}, \mathcal{B}$  over an algebraic structure  $(\mathcal{S}, +, \times)$ , the equivalence problem asks whether the two associated functions  $f_{\mathcal{A}}, f_{\mathcal{B}}: \Sigma^* \rightarrow \mathcal{S}$  are equal:  $f_{\mathcal{A}}(w) = f_{\mathcal{B}}(w)$  for all finite words  $w$  over the alphabet  $\Sigma$ . Over the ring  $(\mathbb{Q}, +, \times)$ , equivalence is decidable in polynomial time by the results of Schützenberger [41] and Tzeng [46]; subsequently, fast parallel (**NC** and **RNC**) algorithms have been found for this problem [47, 26]. In contrast, for semirings the equivalence problem is hard: undecidable [27, 1] for the semiring  $(\mathbb{Q}, \max, +)$  and **PSPACE-hard** [35] for the Boolean semiring (for which weighted automata are usual nondeterministic finite automata and equivalence is equality of recognized languages). Replacing  $=$  with  $\leq$  makes the problem harder: even for the ring  $(\mathbb{Q}, +, \times)$  the question of whether  $f_{\mathcal{A}}(w) \leq f_{\mathcal{B}}(w)$  for all  $w \in \Sigma^*$  is undecidable—even if  $f_{\mathcal{A}}$  is constant [38]. This problem subsumes the universality problem for (Rabin) probabilistic automata, yet another subclass of weighted automata (see, e.g., [16]).

In this paper, we introduce and study another natural problem, in which the ordering is relaxed from exact (in)equality to (in)equality to within a constant factor. Given  $\mathcal{A}$  and  $\mathcal{B}$  as above, is it true that there exists a constant  $c > 0$  such that

$$f_{\mathcal{A}}(w) \leq c \cdot f_{\mathcal{B}}(w) \quad \text{for all } w \in \Sigma^* ?$$

Using standard mathematical notation, this condition asserts that  $f_{\mathcal{A}}(w) = O(f_{\mathcal{B}}(w))$  as  $|w| \rightarrow \infty$ , and we refer to this problem as the *big-O* problem accordingly.<sup>1</sup> The *big-Θ* problem (which turns out to be computationally equivalent to the big-O problem), in line with the  $\Theta(\cdot)$  notation in analysis of algorithms, asks whether  $f_{\mathcal{A}} = O(f_{\mathcal{B}})$  and  $f_{\mathcal{B}} = O(f_{\mathcal{A}})$ .

We restrict our attention to the ring  $(\mathbb{Q}, +, \times)$  and only consider *non-negative weighted automata*, i.e., those in which all transitions have non-negative weights. We remark that, even under this restriction, weighted automata still form a superclass of (Rabin) probabilistic automata, a non-trivial and rich model of computation. Our initial motivation to study the big-O problem came from yet another formalism, labelled Markov chains (LMCs). One can think of the semantics of LMCs as giving a probability distribution or subdistribution on the set of all finite words. LMCs, often under the name Hidden Markov Models, are widely employed in a diverse range of applications; in computer-aided verification, they are perhaps the most fundamental model for probabilistic systems, with model-checking tools such as Prism [28] or Storm [13] based on analyzing LMCs efficiently. All the results in our paper (including hardness results) hold for LMCs too. Our main findings are as follows.

- The big-O problem for non-negative WA and LMCs turns out to be undecidable in general, by a reduction from nonemptiness for probabilistic automata.
- For unambiguous automata, i.e., where every word has at most one accepting path, the big-O problem becomes decidable and can be solved in polynomial time.
- In the unary case, i.e., if the input alphabet  $\Sigma$  is a singleton, the big-O problem is also decidable and, in fact, complete for the complexity class **coNP**. Unary LMCs are a simple and pure probabilistic model of computation: they run in discrete time and can terminate at any step; the big-O problem refers to this termination probability in two LMCs (or two WA). Our upper bound argument refines an analysis of growth of entries in powers of non-negative matrices by Friedland and Schneider [40], and the lower bound is obtained by a reduction from unary NFA universality [44].

<sup>1</sup> There also exists a related but slightly different definition of big-O; see Remark 12 for details on the corresponding version of our big-O problem.

What about polynomially ambiguous automata?  
This would generalize all these decidability results...

- In a more general **bounded case**, i.e., if the languages of all words  $w$  associated with non-zero weight are included in  $w_1^* w_2^* \dots w_m^*$  for some finite words  $w_1, \dots, w_m \in \Sigma^*$  (that is, are *bounded in the sense of Ginsburg and Spanier*; see [21, Chapter 5] and [22]), the big-O problem is decidable subject to Schanuel's conjecture. This is a well-known conjecture in transcendental number theory [29], which implies that the first-order theory of the real numbers with the exponential function is decidable [30]. Intuitively, our reliance on this conjecture is linked to the expressions for the growth rate in powers of non-negative matrices. These expressions are sums of terms of the form  $\rho^n \cdot n^k$ , where  $n$  is the length of a word,  $k \in \mathbb{N}$ , and  $\rho$  is an algebraic number. Our algorithms (however implicitly) need to compare for equality pairs of real numbers of the form  $\log \rho_1 / \log \rho_2$ , where  $\rho_i$  are algebraic, and it is an open problem in number theory whether there is an effective procedure for this task (the four exponentials conjecture asks whether two such ratios can ever be equal; see, e.g., Waldschmidt [48, Sections 1.3 and 1.4]).

Bounded languages form a well-known subclass of regular languages. In fact, a regular (or even context-free) language  $L$  is bounded if and only if the number of words of length  $n$  in  $L$  is at most polynomial in  $n$ . All other regular languages have, in contrast, exponential growth rate (a fact rediscovered multiple times; see, e.g., references in Gawrychowski et al. [19]). Bounded languages have been studied from combinatorial and algorithmic points of view since the 1960s [22, 19], and have recently been used, e.g., in the analysis of quantitative information flow problems in computer security [34, 33]. In the context of labelled Markov chains, languages that are subsets of  $a_1^* a_2^* \dots a_m^*$  (for individual letters  $a_1, \dots, a_m \in \Sigma$ ) model consecutive arrival of  $m$  events in a discrete-time system. It is curious that natural decision problems for such simple systems can lead to intricate algorithmic questions in number theory at the border of decidability.

### Further motivation and related work.

In the labelled Markov chain setting, the big-O problem can be reformulated as a boundedness problem for the following function. For two LMCs  $\mathcal{A}$  and  $\mathcal{B}$ , define the (asymmetric) *ratio variation function* by

$$r(\mathcal{A}, \mathcal{B}) = \sup_{E \subseteq \Sigma^*} (f_{\mathcal{A}}(E) / f_{\mathcal{B}}(E)),$$

where  $f_{\mathcal{A}}(E)$  and  $f_{\mathcal{B}}(E)$  denote the total probability mass associated with an arbitrary set of finite words  $E \subseteq \Sigma^*$  in  $\mathcal{A}$  and  $\mathcal{B}$ , respectively. Here we assume  $\frac{0}{0} = 0$  and  $\frac{x}{0} = \infty$  for  $x > 0$ . Observe that, because  $\max(\frac{a}{b}, \frac{c}{d}) \geq \frac{a+c}{b+d}$  for  $a, b, c, d \geq 0$ , the supremum over  $E \subseteq \Sigma^*$  can be replaced with supremum over  $w \in \Sigma^*$ . Consequently, the big-O problem for LMCs is equivalent to deciding whether  $r(\mathcal{A}, \mathcal{B}) < \infty$ .

Finding the value of  $r$  amounts to asking for the optimal (minimal) constant in the big-O notation. Further, one can consider a symmetric variant, the *ratio distance*:  $rd(\mathcal{A}, \mathcal{B}) = \max\{r(\mathcal{A}, \mathcal{B}), r(\mathcal{B}, \mathcal{A})\}$ , in an analogy with big- $\Theta$ . Now,  $rd$  is a ratio-oriented variant of the classic *total variation distance*  $tv$ , defined by  $tv(\mathcal{A}, \mathcal{B}) = \sup_{E \subseteq \Sigma^*} (f_{\mathcal{A}}(E) - f_{\mathcal{B}}(E))$ , which is a well-established way of comparing two labelled Markov chains [6, 25]. We also consider the problem of approximating  $r$  (as well as  $rd$ ) to a given precision and the problem of comparing it with a given constant (threshold problem), showing that both are undecidable.

The ratio distance  $rd$  is also equivalent to the exponential of the *multiplicative total variation distance* defined in [5, 43] in the context of differential privacy. Consider a system  $\mathcal{M}$ , modelled by a single labelled Markov chain, where output words are observable to the environment but we want to protect the privacy of the starting configuration. Let

$R \subseteq Q \times Q$  be a symmetric relation, which relates the starting configurations intended to remain indistinguishable. Given  $\epsilon \geq 0$ , we say that  $\mathcal{M}$  is  $\epsilon$ -differentially private (with respect to  $R$ ) if, for all  $(s, s') \in R$ , we have  $f_s(E) \leq e^\epsilon \cdot f_{s'}(E)$  for every observable set of traces  $E \subseteq \Sigma^*$  [14, 7]. **Here in the subscript of  $f$  and elsewhere, references to states  $s$  and  $s'$  replace references to LMCs/automata:  $\mathcal{M}$  stays implicit, and we specify which state it is executed from.** Note that there exists such an  $\epsilon$  if and only if  $r(s, s') < \infty$  for all  $(s, s') \in R$  or, equivalently, (the LMC  $\mathcal{M}$  executed from)  $s$  is big-O of (the LMC  $\mathcal{M}$  executed from)  $s'$  for all  $(s, s') \in R$ . In fact, the minimal such  $\epsilon$  satisfies  $e^\epsilon = \max_{(s, s') \in R} r(s, s')$ , thus  $r$  captures the level of differential privacy between  $s$  and  $s'$ .

Our results show that even deciding whether the multiplicative total variation distance is finite or  $+\infty$  is, in general, impossible. Likewise, it is undecidable whether a system modelled by a labelled Markov chain provides any degree of differential privacy, however low.

## 2 Preliminaries

► **Definition 1.** A weighted automaton  $\mathcal{W}$  over the  $(\mathbb{Q}, +, \times)$  semi-ring is a 4-tuple  $\langle Q, \Sigma, M, F \rangle$ , where  $Q$  is a finite set of states,  $\Sigma$  is a finite alphabet,  $M : \Sigma \rightarrow \mathbb{Q}^{Q \times Q}$  is a transition weighting function, and  $F \subseteq Q$  is a set of final states. We consider only non-negative weighted automata, i.e.  $M(a)(q, q') \geq 0$  for all  $a \in \Sigma$  and  $q, q' \in Q$ .

In complexity-theoretic arguments, we assume that each weight is given as a pair of integers (numerator and denominator) in binary. The description size is then the number of bits required to represent  $\langle Q, \Sigma, M, F \rangle$ , including the bit size of the weights.

Each weighted automaton defines functions  $f_s : \Sigma^* \rightarrow \mathbb{R}$ , where for all  $s \in Q$

$$f_s(w) = \sum_{t \in F} (M(a_1) \times M(a_2) \times \cdots \times M(a_n))_{s,t} \quad \text{for } w = a_1 a_2 \dots a_n \in \Sigma^*$$

and  $A \times B$  is standard matrix multiplication. We refer to  $f_s(w)$  as *the weight of  $w$  from state  $s$* . Without loss of generality, a weighted automaton can have a single final state. If not, introduce a new unique final state  $t$  s.t.  $M(a)(q, t) = \sum_{q' \in F} M(a)(q, q')$  for all  $q \in Q, a \in \Sigma$ .

► **Definition 2.** We denote by  $\mathcal{L}_s(\mathcal{W})$  the set of  $w \in \Sigma^*$  with  $f_s(w) > 0$ , that is, with positive weight from  $s$ . Equivalently, this is the language of  $\mathcal{N}_s(\mathcal{W})$ , the non-deterministic finite automaton (NFA) formed from the same set of states (and final states) as  $\mathcal{W}$ , start state  $s$ , and transitions  $q \xrightarrow{a} q'$  whenever  $M(a)(q, q') > 0$ .

Given  $s, s' \in Q$ , we say that  $s$  **is big-O of  $s'$**  if there exists  $C > 0$  such that  $f_s(w) \leq C \cdot f_{s'}(w)$  for all  $w \in \Sigma^*$ . The paper studies the following problem.

► **Definition 3 (BIG-O PROBLEM).**

INPUT      Weighted automaton  $\langle Q, \Sigma, M, F \rangle$  and  $s, s' \in Q$   
 OUTPUT    Is  $s$  big-O of  $s'$ ?

► **Remark 4.** One could consider whether  $s$  is big- $\Theta$  of  $s'$ , defined as  $s$  is big-O of  $s'$  and  $s'$  is big-O of  $s$ ; equivalently, whether  $rd(s, s') < \infty$  for LMCs. We note that these two notions reduce to each other, justifying our consideration of only the big-O problem (see Appendix C). There is an obvious reduction from big- $\Theta$  to big-O making two oracle calls (a Cook reduction), but this can be strengthened to a single call preserving the answer (a Karp reduction). This, however, requires at least two characters. In the other direction, one can ask if  $s$  big-O of  $s'$  using big- $\Theta$  by asking if a linear combination of  $s$  and  $s'$  is big- $\Theta$  of  $s'$ .

In the paper we also work with labelled Markov chains. In particular, they will appear in examples and hardness (including undecidability) arguments. As they are a special class of weighted automata, this will imply hardness (resp. undecidability) for weighted automata in general. On the other hand, our decidability results will be phrased using weighted automata, which makes them applicable to labelled Markov chains.

► **Definition 5.** A labelled Markov chain (LMC) is a (non-negative) weighted automaton  $\langle Q, \Sigma, M, F \rangle$  such that, for all  $q \in Q \setminus F$ , we have  $\sum_{q' \in Q} \sum_{a \in \Sigma} M(a)(q, q') = 1$  and  $M(a)(q, q') = 0$  for all  $a \in \Sigma, q \in F$  and  $q' \in Q$ .

Since final states have no outgoing transitions, w.l.o.g., one can assume a unique final state. For LMCs, the function  $f_s$  can be extended to a measure on the powerset of  $\Sigma^*$  by  $f_s(E) = \sum_{w \in E} f_s(w)$ , where  $E \subseteq \Sigma^*$ . The measure is a subdistribution:  $\sum_{w \in \Sigma^*} f_s(w) \leq 1$ .

We will also consider *unary* weighted automata, and similarly LMCs, where  $|\Sigma| = 1$ . Then we will often omit  $\Sigma$  on the understanding that  $\Sigma = \{a\}$ , and describe transitions with a single matrix  $A = M(a)$  so that  $f_s(a^n) = A_{s,t}^n$ , where  $t$  is the unique final state. Note that  $A_{s,t}^n$  stands for  $(A^n)(s, t)$ , and not  $(A(s, t))^n$ . Using the notation of regular expressions, we can write  $\mathcal{L}_s(\mathcal{W}) \subseteq a^*$ . It will turn out fruitful to consider several larger classes of languages:

► **Definition 6.** Let  $L \subseteq \Sigma^*$ .  $L$  is bounded [22] if  $L \subseteq w_1^* w_2^* \dots w_m^*$  for some  $w_1, \dots, w_m \in \Sigma^*$ .  $L$  is letter-bounded if  $L \subseteq a_1^* a_2^* \dots a_m^*$  for some  $a_1, \dots, a_m \in \Sigma$ .  $L$  is plus-letter-bounded if  $L \subseteq a_1^+ a_2^+ \dots a_m^+$  for some  $a_1, \dots, a_m \in \Sigma$ .

In each case, if the language of an NFA is suitably bounded, one can extract a corresponding bounding regular expression [19].

### 3 Big-O, Threshold and Approximation problems are undecidable

We show that the big-O problem is undecidable. We also establish undecidability for several other problems related to computing and approximating the ratio variation distance. Recall that this corresponds to identifying the optimal constant for positive instances of the big-O problem or the level of differential privacy between two states in a labelled Markov chain.

► **Definition 7.** The asymmetric threshold problem takes an LMC along with two states  $s, s'$  and a constant  $\theta$ , and asks if  $r(s, s') \leq \theta$ . The variant under the promise of boundedness promises that  $r(s, s') < \infty$ . The strict variant of each problem replaces  $\leq$  with  $<$ .

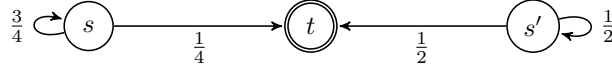
The asymmetric additive approximation task takes an LMC, two states  $s, s'$  and a constant  $\gamma$ , and asks for  $x$  such that  $|r(s, s') - x| \leq \gamma$ . The asymmetric multiplicative approximation task takes an LMC, two states  $s, s'$  and a constant  $\gamma$ , and asks for  $x$  such that  $1 - \gamma \leq \frac{x}{r(s, s')} \leq 1 + \gamma$ .

In each case, the symmetric variant is obtained by replacing  $r$  with  $rd$ .

► **Theorem 8.**

- The big-O problem is undecidable, even for LMCs.
- Each variant of the threshold problem (asymmetric/symmetric, non-strict/strict) is undecidable, even under the promise of boundedness.
- All variants of the approximation tasks (asymmetric/symmetric, additive/multiplicative) are unsolvable, even under the promise of boundedness.

Probabilistic automata are similar to LMCs, except that  $M(a)$  is stochastic for every  $a$ , rather than  $\sum_{a \in \Sigma} M(a)$  being stochastic. Formally, a *probabilistic automaton* is a non-negative weighted automaton with a distinguished start state  $q_s$  such that  $\sum_{q' \in Q} M(a)(q, q') =$



■ **Figure 1** Unbounded ratio but language equivalent.

1 for all  $q \in Q$  and  $a \in \Sigma$ . The problem **EMPTY** asks if  $f_{q_s}(w) \leq \frac{1}{2}$  for all words  $w$ . It is known to be undecidable [38, 16].

**Proof sketch of Theorem 8 (see Appendix D).** We reduce from **EMPTY**. The construction creates two branches of a labelled Markov chain. The first simulates the probabilistic automaton using the original weights multiplied by a scalar ( $\frac{1}{4}$  in the case  $|\Sigma| = 2$ ). The other branch will process each letter from  $\Sigma$  with equal weight (also  $\frac{1}{4}$  in an infinite loop). Consequently, if there is a word accepted with probability greater than  $\frac{1}{2}$ , the ratio between the two branches will be greater than 1. The construction will enable words to be processed repeatedly, so that the ratio can then be pumped unboundedly. Certain linear combinations of the branches enable a gap promise, entailing undecidability of the threshold and approximation tasks. ◀

► **Remark.** The classic *non-strict* threshold problem for the total variation distance (i.e. whether  $tv(s, s') \leq \theta$ ) is known to be undecidable [25], like our distances. However, it is not known if its strict variant (i.e. whether  $tv(s, s') < \theta$ ) is also undecidable. In contrast, in our case, both variants are undecidable. Further note that (additive) approximation of  $tv$  is possible [25, 6], but this is not the case for our distances  $r$  and  $rd$ .

► **Remark.** We have shown the undecidability of the big-O problem using the undecidability of the emptiness problem for probabilistic automata. Another proof of undecidability can be obtained using the **VALUE-1** problem (shown to be undecidable in [20]): indeed the big-O problem and the **VALUE-1** problem are interreducible. However, the reduction from big-O to **VALUE-1** does not entail decidability for subclasses of weighted automata (such as those with bounded languages), as the image of these subclasses does not fall into the known decidable fragments of the **VALUE-1** problem. Further details are available in Appendix D.1.

#### 4 The LC condition

Towards decidability results, we identify a simple necessary (but insufficient) condition for  $s$  being big-O of  $s'$ .

► **Definition 9 (LC condition).** A weighted automaton  $\mathcal{W} = \langle Q, \Sigma, M, F \rangle$  and  $s, s' \in Q$  satisfy the language containment condition (LC) if for all words  $w$  with  $f_s(w) > 0$  we also have  $f_{s'}(w) > 0$ . Equivalently,  $\mathcal{L}_s(\mathcal{W}) \subseteq \mathcal{L}_{s'}(\mathcal{W})$ .

The condition can be verified by constructing NFA  $\mathcal{N}_s(\mathcal{W}), \mathcal{N}_{s'}(\mathcal{W})$  that accept  $\mathcal{L}_s(\mathcal{W})$  and  $\mathcal{L}_{s'}(\mathcal{W})$  respectively and verifying  $\mathcal{L}(\mathcal{N}_s(\mathcal{W})) \subseteq \mathcal{L}(\mathcal{N}_{s'}(\mathcal{W}))$ .

► **Remark 10.** Recall that NFA language containment is **NL**-complete if the automata are in fact deterministic, in **P** if they are unambiguous [10, Theorem 3], **coNP**-complete if they are unary [44] and **PSPACE**-complete in general [35]. In all cases this complexity level will match, or be lower than that for our respective algorithm for the big-O problem.

We observe that, if  $s$  is big-O of  $s'$ , the LC condition must hold and so the LC condition is the first step in each of our verification routines. Example 11 shows that the condition alone is not sufficient to solve the big-O problem, because two states can admit the same set of words with non-zero weight, yet the weight ratios become unbounded.



► **Example 11.** Consider the unary automaton  $\mathcal{W}$  in Figure 1. We have  $\mathcal{L}_s(\mathcal{W}) = \mathcal{L}_{s'}(\mathcal{W}) = \{a^n \mid n \geq 1\}$ , but  $\frac{f_s(a^n)}{f_{s'}(a^n)} = \frac{(0.75)^{n-1} \cdot 0.25}{(0.5)^{n-1} \cdot 0.5} = 0.5 \cdot 1.5^{n-1} \xrightarrow{n \rightarrow \infty} \infty$ .

► **Remark 12.** The original big-O notation on  $f, g : \mathbb{N} \rightarrow \mathbb{N}$ , states that  $f$  is  $O(g)$  if  $\exists C, k > 0 \forall n > k f(n) \leq C g(n)$ . Despite excluding finitely many points, when  $g(n) \geq 1$ , it is equivalent to  $\exists C > 0 \forall n > 0 f(n) \leq C g(n)$  by taking  $C$  large enough to deal with the finite prefix.

In the paper, though, we formally consider  $s$  to not be big-O of  $s'$  if there exists even a single word  $w$  such that  $f_s(w) > 0$  and  $f_{s'}(w) = 0$ . However, for weighted automata, we could amend our definition to “eventually big-O” as follows:  $\exists C > 0, k > 0 : \forall w \in \Sigma^{\geq k} f_s(w) \leq C \cdot f_{s'}(w)$ .

The big-O problem reduces to its eventual variant by checking both the LC condition and the eventually big-O condition. Thus our undecidability (and hardness) results transfer to the eventually big-O problem. The eventually big-O problem can be solved via the big-O problem by “fixing” the LC condition through the addition of a branch from  $s'$  that accepts all appropriate words with very low probability (see Appendix E for more details).

## 4.1 Application: unambiguous weighted automata

In this section, we prove the first decidability result, that is, polynomial-time solvability in the unambiguous case. We say a weighted automaton  $\mathcal{W}$  is *unambiguous from a state  $s$*  if every word has at most one accepting path in  $\mathcal{N}_s(\mathcal{W})$ .

► **Lemma 13.** *If a weighted automaton  $\mathcal{W}$  is unambiguous from states  $s$  and  $s'$ , the big-O problem is decidable in polynomial time.*

**Proof sketch (see Appendix E.1).** We construct a product weighted automaton, with edge weights of the form  $M'(a)((q_1, q'_1), (q_2, q'_2)) = \frac{M(a)(q_1, q_2)}{M(a)(q'_1, q'_2)}$  and ask if there is a cycle on a path from  $(s, s')$  to  $(t, t)$  with weight  $> 1$ , which can be detected in polynomial time using a variation on the Bellman-Ford algorithm. ◀

Note the relevant behaviours are those on cycles—transitions which are taken at most once are of little significance to the big-O problem. Such transitions have at most a constant multiplicative effect on the ratio. This is the case whether or not the system is unambiguous.

## 5 The big-O problem for unary weighted automata is coNP-complete

In this section we show coNP-completeness in the unary case.

► **Theorem 14.** *The big-O problem for unary weighted automata is coNP-complete. It is coNP-hard even for unary labelled Markov chains.*

For the upper bound, our analysis will refine the analysis of the growth of powers of non-negative matrices of Friedland and Schneider [18, 40] which gives the asymptotic order of growth of  $A_{s,t}^n + A_{s,t}^{n+1} + \dots + A_{s,t}^{n+q} \approx \rho^n n^k$  for some  $\rho, k$  and  $q$ , which smooths over the periodic behaviour (see Theorem 18). Our results require a non-smoothed analysis, valid for each  $n$ . This isn’t provided in [18, 40], where the smoothing forces the existence of a single limit—which we don’t require. Our big- $\Theta$  lemma (Lemma 21) will accurately characterise the asymptotic behaviour of  $A_{s,t}^n$  by exhibiting the correct value of  $\rho$  and  $k$  for every word.

## 5.1 Preliminaries

Let  $\mathcal{W}$  be a unary non-negative weighted automaton with states  $Q$ , transition matrix  $A$  and a unique final state  $t$ . When we refer to a *path* in  $\mathcal{W}$ , we mean a path in the NFA of  $\mathcal{W}$ , i.e. paths only use transitions with non-zero weights and states on a path may repeat.

► **Definition 15.**

- A state  $q$  can reach  $q'$  if there is a path from  $q$  to  $q'$ . In particular, any state  $q$  can always reach itself.
- A strongly connected component (SCC)  $\varphi \subseteq Q$  is a maximal set of states such that for each  $q, q' \in \varphi$ ,  $q$  can reach  $q'$ . We denote by  $\text{SCC}(q)$  the SCC of state  $q$  and by  $A^\varphi$ , the  $|\varphi| \times |\varphi|$  transition matrix of  $\varphi$ . Note every state is in a SCC, even if it is a singleton.
- The DAG of  $\mathcal{W}$  is the directed acyclic graph of strongly connected components. Components  $\varphi, \varphi'$  are connected by an edge if there exist  $q \in \varphi$  and  $q' \in \varphi'$  with  $A(q, q') > 0$ .
- The spectral radius of an  $m \times m$  matrix  $A$  is the largest absolute value of its eigenvalues. Recall the eigenvalues of  $A$  are  $\{\lambda \in \mathbb{C} \mid \text{exists vector } \vec{x} \in \mathbb{C}^m, \vec{x} \neq 0 \text{ with } A\vec{x} = \lambda\vec{x}\}$ . The spectral radius of  $\varphi$ , denoted by  $\rho_\varphi$ , is the spectral radius of  $A^\varphi$ . By  $\rho(q)$  we denote the spectral radius of the SCC in which  $q$  is a member.
- We denote by  $T^\varphi$  the period of the SCC  $\varphi$ : the greatest common divisor of return times for some state  $s \in \varphi$ , i.e.  $\gcd\{t \in \mathbb{N} \mid A^t(s, s) > 0\}$ . It is known that any choice of state in the SCC gives the same value (see e.g. [42, Theorem 1.20]). If  $A^\varphi = [0]$  then  $T^\varphi = 0$ .
- Let  $\mathcal{P}(s, s')$  be the set of paths from the SCC of  $s$  to the SCC of  $s'$  in the DAG of  $\mathcal{W}$ . Thus a path  $\pi \in \mathcal{P}(s, s')$  is a sequence of SCCs  $\varphi_1, \dots, \varphi_m$ .
- $T(s, s')$ , called the local period between  $s$  and  $s'$ , is defined by  $T(s, s') = \text{lcm}_{\pi \in \mathcal{P}(s, s')} \gcd_{\varphi \in \pi} T^\varphi$ .
- The spectral radius between states  $s$  and  $s'$ , written  $\rho(s, s')$ , is the largest spectral radius of any SCC seen on a path from  $s$  to  $s'$ :  $\rho(s, s') = \max_{\pi \in \mathcal{P}(s, s')} \rho(\pi)$ , where  $\rho(\pi) = \max_{\varphi \in \pi} \rho_\varphi$  for  $\pi \in \mathcal{P}(s, s')$ .
- The following function captures the number of SCCs which attain the largest spectral radius on the path that has the most SCCs of maximal spectral radius. Let  $k(s, s') = \max_{\pi \in \mathcal{P}(s, s')} k(\pi) - 1$ , where, for  $\pi \in \mathcal{P}(s, s')$ ,  $k(\pi) = |\{\varphi \in \pi \mid \rho_\varphi = \rho(s, s')\}|$ .

► **Remark 16.** Since our weighted automata have rational weights, the spectral radius of an SCC is an algebraic number, as the absolute value of a root of a polynomial with rational coefficients. In general, an algebraic number  $z \in \mathbb{A}$  can be represented by a tuple  $(p_z, a, b, r) \in \mathbb{Q}[x] \times \mathbb{Q}^3$ , where  $p_z$  is a polynomial over  $x$  and  $a, b, r$  specify an approximation to distinguish  $z$  from all other roots:  $z$  is the only root of  $p_z(x)$  with  $|z - (a + bi)| \leq r$ . This representation, which admits standard operations (addition, multiplication, absolute value, (in)equality testing, etc.), can be found in polynomial time (see, e.g. [36]). Henceforth, when we refer to the spectral radius we will implicitly mean representation in this form.

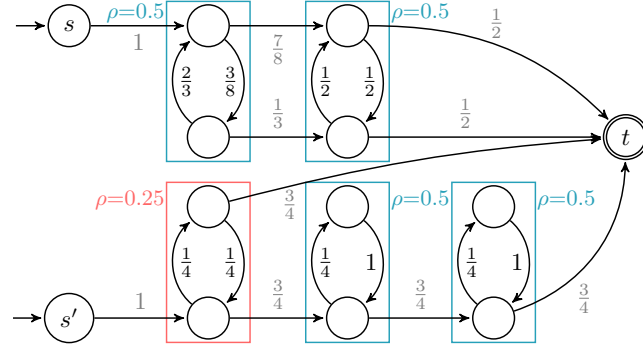
The asymptotic behaviours of weighted automata will be characterised using  $(\rho, k)$ -pairs:

► **Definition 17.** A  $(\rho, k)$ -pair is an element of  $\mathbb{R} \times \mathbb{N}$ . The ordering on  $\mathbb{R} \times \mathbb{N}$  is lexicographic, i.e.  $(\rho_1, k_1) \leq (\rho_2, k_2) \iff \rho_1 < \rho_2 \vee (\rho_1 = \rho_2 \wedge k_1 \leq k_2)$ .

Friedland and Schneider [18, 40] essentially use  $(\rho, k)$ -pairs to show the asymptotic behaviour of the powers of non-negative matrices. In particular they find the asymptotic behaviour of the sum of several  $A_{s, s'}^n$ , smoothing the periodic behaviour of the matrix.

► **Theorem 18** (Friedland and Schneider [18, 40]). Let  $A$  be an  $m \times m$  non-negative matrix, inducing a unary weighted automaton  $\mathcal{W}$  with states  $Q = \{1, \dots, m\}$ . Given  $s, t \in Q$ , let  $B_{s, t}^n = A_{s, t}^n + A_{s, t}^{n+1} + \dots + A_{s, t}^{n+T(s, t)-1}$ . Then  $\lim_{n \rightarrow \infty} \frac{B_{s, t}^n}{\rho(s, t)^n n^{k(s, t)}} = c$ ,  $0 < c < \infty$ .





■ **Figure 2** Different rates for different phases.

In the case where the local period is 1 ( $T(s, t) = T(s', t) = 1$ ), Theorem 18 can already be used to solve the big-O problem (in particular if the matrix  $A$  is aperiodic). In this case  $A_{s,t}^n = B_{s,t}^n = \Theta(\rho(s, t)^n n^{k(s,t)})$ . Then to establish that  $s$  is big-O of  $s'$  we check that the language containment condition holds and that  $(\rho(s, t), k(s, t)) \leq (\rho(s', t), k(s', t))$ . However, this is not sufficient if the local period is not 1.

► **Example 19.** Consider the chains shown in Figure 2 with local period 2. The behaviour for  $n \geq 3$  is  $A_{s,t}^n = \Theta(0.5^n n)$  and  $A_{s',t}^n = \Theta(0.25^n)$  when  $n$  is odd and  $A_{s,t}^n = \Theta(0.5^n n)$  when  $n$  is even. However, Theorem 18 tells us  $B_{s,t}^n = \Theta(0.5^n n)$  and  $B_{s',t}^n = \Theta(0.5^n n)$  suggesting the ratio is bounded, but in fact  $s$  is not big-O  $s'$  (although  $s'$  is big-O of  $s$ ) because  $\frac{A_{s,t}^{2n+1}}{A_{s',t}^{2n+1}} \xrightarrow{n \rightarrow \infty} \infty$ .

## 5.2 Upper bound: The unary big-O problem is in coNP

Let  $\mathcal{W}$  be a unary weighted automaton and suppose we are asked whether  $s$  is big-O of  $s'$ . We assume w.l.o.g. (a) that there is a unique final state  $t$  with no outgoing transitions, and (b) that  $s, s'$  do not appear on any cycle<sup>2</sup>.

Next we define a ‘degree function’, which captures the asymptotic behaviour of each word  $a^n$  by a  $(\rho, k)$ -pair, capturing the exponential and polynomial behaviours respectively.

► **Definition 20.** Given a unary weighted automaton  $\mathcal{W}$ , let  $d_{s,t} : \mathbb{N} \rightarrow \mathbb{R} \times \mathbb{N}$  be defined by  $d_{s,t}(n) = (\rho, k)$ , where:

- $\rho$  is the largest spectral radius of any vertex visited on any path of length  $n$  from  $s$  to  $t$
- the path from  $s$  to  $t$  that visits the most SCCs of spectral radius  $\rho$  visits  $k + 1$  such SCCs;
- if there is no length- $n$  path from  $s$  to  $t$ , then  $(\rho, k) = (0, 0)$ .

Let  $s, t \in Q$  be fixed. We are now ready to state the key technical lemma of this subsection (cf. Theorem 18, Friedland and Schneider [18, 40]), where we assume the functions  $\rho(n), k(n)$ , defined by  $d_{s,t}(n) = (\rho(n), k(n))$ .

► **Lemma 21** (The big- $\Theta$  lemma). *There exist  $c, C > 0$  such that, for every  $n > |Q|$ ,*

$$c \cdot \rho(n)^n n^{k(n)} \leq A_{s,t}^n \leq C \cdot \rho(n)^n n^{k(n)}.$$

<sup>2</sup> If this is not the case, copies of  $s, s'$  and their transitions can be taken.

The set of *admissible*  $(\rho, k)$ -pairs is the image of  $d_{s,t}$ . Observe that this set is finite and of size at most  $|Q|^2$ : there can be no more than  $|Q|$  values of  $\rho$  (if at worst each state were its own SCC) and the value of  $k$  is also bounded by the number of SCCs and thus  $|Q|$ .

We next define the  $(\rho, k)$ -annotated version of  $\mathcal{W}$ , i.e. in each state we record the relevant value of  $(\rho, k)$  corresponding to the current run to the state.

► **Definition 22** (The weighted automaton  $\mathcal{W}^\dagger$ ). *Given  $\mathcal{W} = \langle Q, \Sigma, A, \{t\} \rangle$  and  $s \in Q$ , the weighted automaton  $\mathcal{W}^\dagger$  has states of the form  $(q, \rho, k)$  for all  $q \in Q$  and all admissible  $(\rho, k)$ -pairs, the same  $\Sigma$  and no final states. For every transition  $q \xrightarrow{p} q'$  from  $\mathcal{W}$  denoting  $A(q, q') = p$ , include the following transition in  $\mathcal{W}^\dagger$  for each admissible  $(\rho, k)$ :*

- $(q, \rho, k) \xrightarrow{p} (q', \rho, k)$  if  $\text{SCC}(q) = \text{SCC}(q')$ ,
- $(q, \rho, k) \xrightarrow{p} (q', \rho, k + 1)$  if  $\text{SCC}(q) \neq \text{SCC}(q')$  and  $\rho = \rho(q')$ ,
- $(q, \rho, k) \xrightarrow{p} (q', \rho, k)$  if  $\text{SCC}(q) \neq \text{SCC}(q')$  and  $\rho > \rho(q')$ ,
- $(q, \rho, k) \xrightarrow{p} (q', \rho(q'), 0)$  if  $\text{SCC}(q) \neq \text{SCC}(q')$  and  $\rho(q') > \rho$ .

$\mathcal{W}^\dagger$  is constructable in polynomial time given  $\mathcal{W}$ . Indeed, the spectral radii of all SCCs can be computed and compared to each other in time polynomial in the size of  $\mathcal{W}$  (see Remark 16).

For the following lemma, recall the language containment (LC) condition from Definition 9 and the ordering on  $(\rho, k)$ -pairs from Definition 17.

► **Lemma 23.** *A state  $s$  is big-O of  $s'$  if and only if the LC condition holds and, for all but finitely many  $n \in \mathbb{N}$ , we have  $d_{s,t}(n) \leq d_{s',t}(n)$ .*

**Proof sketch.** Whenever  $d_{s,t}(n) \leq d_{s',t}(n)$ , by Lemma 21, we have  $f_s(a^n) \leq (\frac{C}{c}(\frac{\rho}{\rho'})^n n^{k-k'}) \cdot f_{s'}(a^n)$ , in which case either  $d_{s,t}(n) = d_{s',t}(n)$  and  $(\frac{\rho}{\rho'})^n n^{k-k'} = 1$  or  $\lim_{n \rightarrow \infty} (\frac{\rho}{\rho'})^n n^{k-k'} = 0$  and so  $(\frac{\rho}{\rho'})^n n^{k-k'} \leq 1$  for all but finitely many  $n$ .

However, whenever  $d_{s,t}(n) > d_{s',t}(n)$ , Lemma 21 yields  $f_s(a^n) \geq (\frac{c}{C}(\frac{\rho}{\rho'})^n n^{k-k'}) \cdot f_{s'}(a^n)$  but then  $\lim_{n \rightarrow \infty} (\frac{\rho}{\rho'})^n n^{k-k'} = \infty$ . ◀

We are going to use the characterisation from Lemma 23 to prove Theorem 14. As already discussed, the LC condition can be checked via NFA inclusion testing. To tackle the “for all but finitely many ...” condition, we introduce the concept of eventual inclusion.

► **Definition 24.** *Given sets  $A, B$ , we say  $A$  is eventually included in  $B$ , written  $A \sqsubset B$ , if and only if  $A \setminus B$  is finite.*

The next three lemmas relate deciding the big-O problem using the characterisation of Lemma 23 to eventual inclusion. The missing proofs are available in the Appendix.

► **Lemma 25.** *Given unary NFAs  $\mathcal{N}_1, \mathcal{N}_2$ , the problem  $\mathcal{L}(\mathcal{N}_1) \sqsubset \mathcal{L}(\mathcal{N}_2)$  is in **coNP**.*

► **Lemma 26.** *Suppose  $d_1, d_2 : \mathbb{N} \rightarrow X$ , with  $(X, \leq)$  a finite total order. Then  $d_1(n) \leq d_2(n)$  for all but finitely many  $n$  if and only if  $\{n \mid d_1(n) \geq x\} \sqsubset \{n \mid d_2(n) \geq x\}$  for all  $x \in X$ .*

► **Lemma 27.** *Given a unary weighted automaton  $\mathcal{W}$ , the associated problem whether  $d_{s,t}(n) \leq d_{s',t}(n)$  for all but finitely many  $n \in \mathbb{N}$  is in **coNP**.*

**Proof.** Given an admissible pair  $x = (\rho, k)$ , we construct an NFA  $\mathcal{N}_{s,x}$  accepting  $\{a^n \mid d_{s,t}(n) \geq x\}$  (similarly  $\mathcal{N}_{s',x}$  for  $s'$ ), by taking the NFA  $\mathcal{N}_s(\mathcal{W}^\dagger)$  (Definitions 2, 22) with a suitable choice of accepting states. Recall that states in  $\mathcal{W}^\dagger$  are of the form  $(q, \rho', k')$ , where  $q$  is a

state from  $\mathcal{W}$  and  $(\rho', k')$  is admissible. If we designate states  $(t, \rho', k')$  with  $(\rho', k') \geq x$  as accepting, it will accept  $\{a^n \mid d_{s,t}(n) \geq x\}$ . This is a polynomial-time construction.

Then, by Lemma 26, the problem whether  $d_{s,t}(n) \leq d_{s',t}(n)$  for all but finitely many  $n \in \mathbb{N}$  is equivalent to  $\mathcal{L}(\mathcal{N}_{s,x}) \subsetneq \mathcal{L}(\mathcal{N}_{s',x})$  for all admissible  $x$ . As there are at most  $|Q|^2$  values of  $x$  and each can be verified non-deterministically in **coNP**, it suffices to show that  $\mathcal{L}(\mathcal{N}_{s,x}) \subsetneq \mathcal{L}(\mathcal{N}_{s',x})$  is in **coNP** for each  $x$ . This is the case by Lemma 25.  $\blacktriangleleft$

Remark 10 and Lemma 27 together complete the upper bound result for Theorem 14.

► **Remark.** Lemma 26 may appear simpler using  $\{n \mid f_1(n) = x\} \subsetneq \{n \mid f_2(n) \geq x\}$ . However, it does not seem possible to construct an NFA for  $\{a^n \mid d_{s,t}(n) = x\}$  in polynomial time. Taking just  $(t, \rho, k)$  as accepting would not be correct, as there could be paths of the same length ending in  $(t, \rho', k')$  with  $(\rho', k') > (\rho, k)$ . Using  $\geq$  instead of  $=$  avoids this problem.

► **Remark.** An alternative approach for obtaining an upper bound could be to compute the Jordan normal form of the transition matrix and consider its powers. Instead of the interplay of strongly connected components in the transition graph, we would need to consider linear combinations of the  $n$ th powers of complex numbers (such as roots of unity). It is not clear this algebraic approach leads to a representation more convenient for our purposes.

### 5.3 coNP-hardness for unary LMC

Given a unary NFA  $\mathcal{N}$ , the *NFA universality problem* asks if  $\mathcal{L}(\mathcal{N}) = \{a^n \mid n \in \mathbb{N}\}$ . This problem is **coNP**-complete [44]. We exhibit a polynomial-time reduction from (a variant of) the unary universality problem to the big-O problem on unary Markov chains.

## 6 Decidability for weighted automata with bounded languages

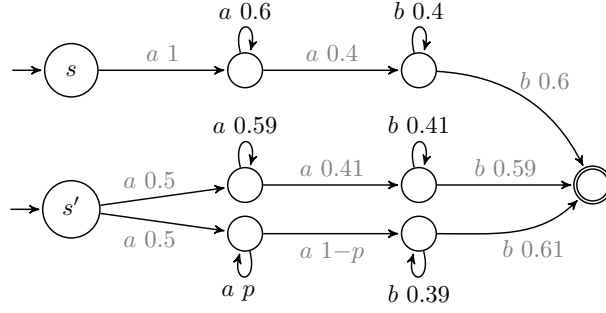
In this section we consider the big-O problem for a weighted automaton  $\mathcal{W}$  and states  $s, s'$  such that  $\mathcal{L}_s(\mathcal{W})$ ,  $\mathcal{L}_{s'}(\mathcal{W})$  are bounded. Throughout the section, we assume that the LC condition has already been checked, i.e.  $\mathcal{L}_s(\mathcal{W}) \subseteq \mathcal{L}_{s'}(\mathcal{W})$ . We will show that the problem is conditionally decidable, subject to Schanuel's conjecture.

**Logical theories of arithmetic and Schanuel's conjecture.** In *first-order logical theories of arithmetic*, variables denote numbers (from  $\mathbb{Z}$  or  $\mathbb{R}$ , as appropriate), and atomic predicates are equalities and inequalities between terms built from variables and function symbols. Nullary function symbols are constants, always from  $\mathbb{Z}$ . If binary addition and multiplication are available, then:

- for  $\mathbb{R}$  we obtain the first-order theory of the reals, where the truth value of sentences is decidable due to the celebrated Tarski–Seidenberg theorem [3, Chapter 11 and Theorem 2.77];
- for  $\mathbb{Z}$ , the first-order theory of the integers is, in contrast, undecidable (see, e.g., [39]).

In the case of  $\mathbb{R}$ , adding the unary symbol for the exponential function  $x \mapsto e^x$ , leads to the *first-order theory of the real numbers with exponential function* ( $\text{Th}(\mathbb{R}_{\text{exp}})$ ). Logarithms base 2, for example, are easily expressible in  $\text{Th}(\mathbb{R}_{\text{exp}})$ . The decidability of  $\text{Th}(\mathbb{R}_{\text{exp}})$  is an open problem and hinges upon Schanuel's conjecture [30].

*Schanuel's conjecture* [29] is a unifying conjecture of transcendental number theory, saying that for all  $z_1, \dots, z_n \in \mathbb{C}$  linearly independent over  $\mathbb{Q}$  the field extension  $\mathbb{Q}(z_1, \dots, z_n, e^{z_1}, \dots, e^{z_n})$  has transcendence degree at least  $n$  over  $\mathbb{Q}$ , meaning that for some  $S \subseteq \{z_1, \dots, z_n, e^{z_1}, \dots, e^{z_n}\}$  of cardinality  $n$ , say  $S = \{s_1, \dots, s_n\}$ , the only polynomial  $p$  over  $\mathbb{Q}$  satisfying  $p(s_1, \dots, s_n) = 0$  is  $p \equiv 0$ . See, e.g., Waldschmidt's book [48, Section 1.4] for further



■ **Figure 3** Relative orderings are the same, but the boundedness question is different.

context. If indeed true, this conjecture would generalise several known results, including the Lindemann–Weierstrass theorem and Baker’s theorem, and would entail the decidability of  $\text{Th}(\mathbb{R}_{\text{exp}})$ . Our work follows an exciting line of research that reduces problems from verification [12, 31], linear dynamical systems [2, 8], and symbolic computation [24] to the decision problem for  $\text{Th}(\mathbb{R}_{\text{exp}})$ .

► **Theorem 28.** *Given a weighted automaton  $\mathcal{W} = \langle Q, \Sigma, M, F \rangle$ ,  $s, s' \in Q$ , with  $\mathcal{L}_s(\mathcal{W})$  and  $\mathcal{L}_{s'}(\mathcal{W})$  bounded, it is decidable whether  $s$  is big-O of  $s'$ , subject to Schanuel’s conjecture.*

In the unary case, it was sufficient to consider the *relative order* between spectral radii, with careful handling of the periodic behaviour. This approach is insufficient in the bounded case. Example 29 highlights that the actual values of the spectral radii have to be examined.

► **Example 29** (Relative orderings are insufficient). Consider the LMC in Figure 3, with  $0.61 \leq p \leq 0.62$ . We have  $f_s(a^m b^n) = \Theta(0.6^m 0.4^n)$  and  $f_{s'}(a^m b^n) = \Theta(p^m 0.39^n + 0.59^m 0.41^n)$ . Note that neither  $0.59^m 0.41^n$  nor  $p^m 0.39^n$  dominate, nor are dominated by,  $0.6^m 0.4^n$  for any value of  $0.61 \leq p \leq 0.62$ . That is, there are values of  $m, n$  where  $0.59^m 0.41^n \gg 0.6^m 0.4^n$  (in particular large  $n$ ) and values of  $m, n$  where  $0.59^m 0.41^n \ll 0.6^m 0.4^n$  (in particular large  $m$ ); similarly for  $p^m 0.39^n$  vs  $0.6^m 0.4^n$  (but the cases in which  $n$  or  $m$  needs to be large are swapped). However, the big-O status can be different for different values of  $p \in [0.61, 0.62]$ , despite the same relative ordering between spectral radii. When  $p = 0.62$ , the ratio turns out to be bounded:  $\frac{f_s(a^m b^n)}{f_{s'}(a^m b^n)} \leq \frac{1600}{1579}$  for all  $m, n$  (in particular, maximal at  $m = n = 0$ ). In contrast, when  $p = 0.61$ , we have  $\frac{f_s(a^m b^n)}{f_{s'}(a^m b^n)} \xrightarrow{m \rightarrow \infty} \infty$ .

We first prove Theorem 28 for the plus-letter-bounded case, which is the most technically involved; the other bounded cases will be reduced to it. In the plus-letter-bounded case, we will characterise the behaviour of such automata, generalising  $(\rho, k)$ -pairs of the unary case. We will need to rely upon the first-order theory of the reals with exponentials to compare these behaviours.

## 6.1 The plus-letter-bounded case

We assume  $\mathcal{L}_{s'}(\mathcal{W}) \subseteq a_1^+ \cdots a_m^+$ , where  $a_1, \dots, a_m \in \Sigma$  and because the LC condition holds, we also have  $\mathcal{L}_s(\mathcal{W}) \subseteq a_1^+ \cdots a_m^+$ . In the plus-letter-bounded cases, without loss of generality, we assume  $a_i \neq a_j$  for  $i \neq j$  (see Appendix G for a justification). Then any word  $w = a_1^{n_1} \cdots a_m^{n_m}$  is uniquely specified by a vector  $(n_1, \dots, n_m) \in \mathbb{N}_{>0}^m$ , where  $n_i$  is the number of  $a_i$ ’s in  $w$ .

Like in Definition 20, we define a degree function  $d$ , which will be used to study the asymptotic behaviour of words. This time we will associate a separate  $(\rho, k)$  pair to each of the  $m$  characters and, consequently, words will induce sequences of the form  $(\rho_1, k_1) \cdots (\rho_m, k_m)$ .

Further, as there may be multiple, incomparable behaviours, words will induce sets of such sequences, i.e.  $d: \mathbb{N}^m \rightarrow \mathcal{P}((\mathbb{R} \times \mathbb{N})^m)$ . For the sake of comparisons, it will be convenient to focus on maximal elements with respect to the pointwise order on  $(\mathbb{R} \times \mathbb{N})^m$ , written  $\leq$ , where the lexicographic order (recall Definition 17) is used to compare elements of  $\mathbb{R} \times \mathbb{N}$ .

Recall Lemma 21 does not capture the asymptotics when  $n \leq |Q|$ . In the unary case this is inconsequential as small words are covered by the *finitely many* exceptions and the LC condition. However, here, a small number of one character may be used to enable access to a particular part of the automaton in another character. For this case, we introduce a new number  $\delta = \frac{1}{2} \min_{\varphi: \rho_\varphi > 0} \rho_\varphi$  which is strictly smaller than the spectral radius of every non-zero SCC (so will not dominate with the partial order), but non-zero.

► **Definition 30.** Let  $\hat{\rho} = (\rho_1, k_1), \dots, (\rho_m, k_m) \in (\mathbb{R} \times \mathbb{N})^m$ . An  $a_1^{n_1} a_2^{n_2} \dots a_m^{n_m}$ -labelled path from  $s$  (to the final state) is compatible with  $\hat{\rho}$  if, for each  $i = 1, \dots, m$ , it visits  $k_i + 1$  SCCs with spectral radius  $\rho_i$  while reading  $a_i$ , unless the path visits only singletons with no loops, in which case  $(\rho_i, k_i) = (\delta, 0)$ . The notation  $(\rho, k) \in \hat{\rho}$  is used for ‘ $(\rho, k)$  is an element of  $\hat{\rho}$ ’.

► **Definition 31.** Let  $d_s: \mathbb{N}^m \rightarrow \mathcal{P}((\mathbb{R} \times \mathbb{N})^m)$  be s.t.:  $\hat{\rho} \in d_s(n_1, \dots, n_m)$  if and only if  
 (1) there exists an  $a_1^{n_1} a_2^{n_2} \dots a_m^{n_m}$ -labelled path from  $s$  to the final state compatible with  $\hat{\rho}$ , and  
 (2) for every  $a_1^{n_1} a_2^{n_2} \dots a_m^{n_m}$ -labelled path from  $s$  compatible with  $\hat{\sigma}$  s.t.  $\hat{\rho} \leq \hat{\sigma}$ , we have  $\hat{\rho} = \hat{\sigma}$ .

Observe that  $\hat{\rho}$  may range over at most  $|Q|^{2m}$  possible values. We write  $\mathcal{D}$  for the set containing them, so that  $d_s: \mathbb{N}^m \rightarrow \mathcal{P}(\mathcal{D})$ . In this extended setting, the big- $\Theta$  lemma (Lemma 21) may be generalised as follows.

► **Lemma 32.** Denote  $z(n_1, \dots, n_m) = \sum_{\hat{\rho} \in d_s(n_1, \dots, n_m)} \prod_{(\rho_i, k_i) \in \hat{\rho}} \rho_i^{n_i} \cdot n_i^{k_i}$ . There exist  $c, C > 0$  such that for all  $n_1, \dots, n_m \in \mathbb{N}$ :

$$c \cdot z(n_1, \dots, n_m) \leq f_s(a_1^{n_1} a_2^{n_2} \dots a_m^{n_m}) \leq C \cdot z(n_1, \dots, n_m).$$

The following lemma provides the key characterisation of negative instances of the big-O problem, in the plus-letter-bounded case and assuming the LC condition. Here and below, we write  $n(t)$  to refer to the  $t$ th vector in a sequence  $n: \mathbb{N} \rightarrow \mathbb{N}^m$ .

► **Lemma 33 (Main lemma).** Assume  $\mathcal{L}_s(\mathcal{W}) \subseteq \mathcal{L}_{s'}(\mathcal{W})$ . Then  $s$  is not big-O of  $s'$  if and only if there exists a sequence  $n: \mathbb{N} \rightarrow \mathbb{N}^m$  and  $X \in \mathcal{D}$ ,  $\mathcal{Y} \subseteq \mathcal{D}$  such that

- (a)  $X \in d_s(n(t))$  and  $\mathcal{Y} = d_{s'}(n(t))$  for all  $t$ , and
- (b) for all  $j \in h_{\mathcal{Y}}$ , the sequence  $n$  satisfies

$$\sum_{i=1}^m \alpha_{j,i} n(t)_i + p_{j,i} \log n(t)_i \xrightarrow{t \rightarrow \infty} -\infty,$$

where  $h_{\mathcal{Y}} \subseteq \{1, \dots, |\mathcal{Y}|\}$ ,  $\alpha_{j,i} \in \mathbb{R}$ ,  $p_{j,i} \in \mathbb{Z}$  ( $1 \leq i \leq m$ ) are uniquely determined by  $X$  and  $\mathcal{Y}$  (in a way detailed below),  $h_{\mathcal{Y}}$  and  $p_{j,i}$ ’s are effectively computable and  $\alpha_{j,i}$ ’s are first-order expressible (with exponential function).

**Proof.** Observe that then  $s$  is not big-O of  $s'$  iff there exists an infinite sequence of words such that, for all  $C > 0$ , the sequence contains a word  $w$  such that  $\frac{f_s(w)}{f_{s'}(w)} > C$ . Thanks to

Lemma 32, this is equivalent to the existence of a sequence  $n : \mathbb{N} \rightarrow \mathbb{N}^m$  such that

$$\frac{\sum_{X \in d_s(n(t)_1, \dots, n(t)_m)} \prod_{(\rho_i, k_i) \in X} \rho_i^{n(t)_i} \cdot n(t)_i^{k_i}}{\sum_{Y \in d_{s'}(n(t)_1, \dots, n(t)_m)} \prod_{(\sigma_i, \ell_i) \in Y} \sigma_i^{n(t)_i} \cdot n(t)_i^{\ell_i}} \xrightarrow{t \rightarrow \infty} \infty,$$

where  $n(t)_i$  denotes the  $i$ th component of  $n(t)$ . Since there are finitely many possible values of  $d_s$  and  $d_{s'}$ , it suffices to look for sequences  $n$  such that  $d_s(n(t))$  and  $d_{s'}(n(t))$  are fixed. Further, because of the sum in the numerator, only one  $X \in \mathcal{X}$  is required such that  $X \in d_s(n_1, \dots, n_m)$ . Thus, we need to determine whether there exist  $X \in \mathcal{D}$ ,  $\mathcal{Y} \subseteq \mathcal{D}$  and  $n : \mathbb{N} \rightarrow \mathbb{N}^m$  such that  $X \in d_s(n(t))$ ,  $d_{s'}(n(t)) = \mathcal{Y}$  (for all  $t$ ) and

$$\frac{\prod_{i=1}^m \rho_i^{n(t)_i} \cdot n(t)_i^{k_i}}{\sum_{j=1}^{h_Y} \prod_{i=1}^m \sigma_{ji}^{n(t)_i} \cdot n(t)_i^{\ell_{ji}}} \xrightarrow{t \rightarrow \infty} \infty.$$

where  $X = (\rho_1, k_1) \cdots (\rho_m, k_m)$ ,  $\mathcal{Y} = \{Y_1, \dots, Y_{|\mathcal{Y}|}\}$ , and  $Y_j = (\sigma_{j1}, \ell_{j1}) \cdots (\sigma_{jm}, \ell_{jm})$  ( $1 \leq j \leq |\mathcal{Y}|$ ). Taking the reciprocal and requiring each of the summands to go to zero, we obtain

$$\frac{\prod_{i=1}^m \sigma_{ji}^{n(t)_i} \cdot n(t)_i^{\ell_{ji}}}{\prod_{i=1}^m \rho_i^{n(t)_i} \cdot n(t)_i^{k_i}} = \prod_{i=1}^m \left( \frac{\sigma_{ji}}{\rho_i} \right)^{n(t)_i} n(t)_i^{\ell_{ji} - k_i} \xrightarrow{t \rightarrow \infty} 0 \quad \text{for all } 1 \leq j \leq |\mathcal{Y}|.$$

If we take logarithms, letting  $\alpha_{j,i} = \log\left(\frac{\sigma_{ji}}{\rho_i}\right)$  and  $p_{j,i} = \ell_{ji} - k_i$ , we get

$$\sum_{i=1}^m \alpha_{j,i} n(t)_i + p_{j,i} \log n(t)_i \xrightarrow{t \rightarrow \infty} -\infty$$

for all  $j$  in  $h_Y = \{1 \leq j \leq |\mathcal{Y}| \mid \sigma_{ji} > 0 \text{ for all } 1 \leq i \leq m\}$ .

The number  $\alpha_{j,i}$  is the logarithm of the ratio of two algebraic numbers, which are not given explicitly. However, they admit an unambiguous, first-order expressible characterisation (see Remark 16). The logarithm is encoded using the exponential function:  $\log(z)$  is  $\exists x \in \mathbb{R} : \exp(x) = z$ .  $\blacktriangleleft$

Lemma 33 identifies violation of the big-O property using two conditions. In the remainder of this subsection we will handle Condition (a) using automata-theoretic tools (the Parikh theorem and semi-linear sets) and Condition (b) using logics. In summary, the characterisation of Lemma 33 will be expressed in the first-order theory of the reals with exponentiation, which is decidable subject to Schanuel's conjecture.

### Condition (a) via automata

It turns out that sequences  $n$  satisfying Condition (a) in Lemma 33 can be captured by a finite automaton. In more detail, for any  $X \in \mathcal{D}$ , there exists an automaton  $\mathcal{N}_X^s$  such that  $\mathcal{L}(\mathcal{N}_X^s) = \{a_1^{n_1} \cdots a_m^{n_m} \mid X \in d_s(n_1, \dots, n_m)\}$ . For any  $\mathcal{Y} \subseteq \mathcal{D}$ , there exists an automaton  $\mathcal{N}_{\mathcal{Y}}^s$  such that  $\mathcal{L}(\mathcal{N}_{\mathcal{Y}}^s) = \{a_1^{n_1} \cdots a_m^{n_m} \mid d_s(n_1, \dots, n_m) = \mathcal{Y}\}$ . The relevant automaton capturing  $X$  and  $\mathcal{Y}$  is then found by taking the intersection of  $\mathcal{L}(\mathcal{N}_X^s)$  and  $\mathcal{L}(\mathcal{N}_{\mathcal{Y}}^s)$ .

► **Lemma 34.** *For any  $X \in \mathcal{D}$  and  $\mathcal{Y} \subseteq \mathcal{D}$ , there exists an automaton  $\mathcal{N}_{X,\mathcal{Y}}$  such that  $\mathcal{L}(\mathcal{N}_{X,\mathcal{Y}}) = \{a_1^{n_1} \cdots a_m^{n_m} \mid X \in d_s(n_1, \dots, n_m), \mathcal{Y} = d_{s'}(n_1, \dots, n_m)\}$ .*



Because of our  $a_i \neq a_j$  assumption, the vector  $(n_1, \dots, n_m)$  indicates the number of occurrences of each character. The set of such vectors derived from the language of an automaton is known as the Parikh image of this language [37]. It is well known that the Parikh image of an NFA is a semi-linear set, i.e. a finite union of linear sets (a linear set has the form  $\{\vec{b} + \lambda_1 \vec{r}^1 + \dots + \lambda_s \vec{r}^s \mid \lambda_1, \dots, \lambda_s \in \mathbb{N}\}$ , where  $\vec{b} \in \mathbb{N}^m$  is the base vector and  $\vec{r}^1, \dots, \vec{r}^s \in \mathbb{N}^m$  are called period vectors). However, since  $\mathcal{L}(\mathcal{N}_{X,Y}) \subseteq a_1^+ a_2^+ \dots a_m^+$ , the linear sets are of a very particular form, where each  $\vec{r}^i$  is a constant multiple of the  $i$ th unit vector.

► **Lemma 35.** *The language of  $\mathcal{N}_{X,Y}$  can be effectively decomposed as  $\mathcal{L}(\mathcal{N}_{X,Y}) = \bigcup_{k=1}^{S_{X,Y}} \mathcal{L}_k$ , where  $\mathcal{L}_k = \left\{ a_1^{b_{k1} + r_{k1}\lambda_1} \dots a_m^{b_{km} + r_{km}\lambda_m} \mid \lambda_1, \dots, \lambda_m \in \mathbb{N} \right\}$ ,  $S_{X,Y} \in \mathbb{N}$  and  $b_{ki}, r_{ki} \in \mathbb{N}$  ( $1 \leq k \leq S_{X,Y}$ ,  $1 \leq i \leq m$ ).*

Lemma 35 captures Condition (a) of Lemma 33 precisely.

### Condition (b) via logic

With Lemma 35 in place, we now move on to add Condition (b) to the existing machinery. In fact, the logical formulae in the following lemmas will express the conjunction of both conditions of Lemma 33.

► **Lemma 36.** *Assume  $\mathcal{L}_s(\mathcal{W}) \subseteq \mathcal{L}_{s'}(\mathcal{W})$ . Then  $s$  is not big-O of  $s'$  if and only if there exists  $X \in \mathcal{D}$ ,  $\mathcal{Y} \subseteq \mathcal{D}$ ,  $1 \leq k \leq S_{X,Y}$  such that*

$$\forall C < 0 \exists \vec{\lambda} \in \mathbb{N}^m \bigwedge_{j \in h_Y} \sum_{i=1}^m \alpha_{j,i} (b_{ki} + r_{ki} \lambda_i) + p_{j,i} \log(b_{ki} + r_{ki} \lambda_i) < C,$$

where  $h_Y, \alpha_{j,i}, p_{j,i}$  (resp.  $b_{ki}, r_{ki}$ ) satisfy the same conditions as in Lemma 33 (resp. 35).

Note that the formula of Lemma 36 uses quantification over natural numbers. Our next step will be to replace integer variables with real variables. In other words, we will obtain an equivalent condition in the first-order theory of the reals with exponentiation, as follows.

► **Lemma 37.** *Assume  $\mathcal{L}_s(\mathcal{W}) \subseteq \mathcal{L}_{s'}(\mathcal{W})$ . Then  $s$  is not big-O of  $s'$  if and only if there exist  $X \in \mathcal{D}$ ,  $\mathcal{Y} \subseteq \mathcal{D}$ ,  $1 \leq k \leq S_{X,Y}$  and  $U \subseteq \{i \in \{1, \dots, m\} \mid r_{ki} > 0\}$  such that*

$$\forall C < 0 \exists \vec{x} \in \mathbb{R}_{\geq B_k}^{|U|} \bigwedge_{j \in h_Y} \sum_{i \in U} \alpha_{j,i} r_{ki} x_i + p_{j,i} \log(x_i) < C,$$

where  $B_k = \max_i b_{ki}$  and  $h_Y, \alpha_{j,i}, p_{j,i}, b_{ki}, r_{ki}$  are as in Lemma 36.

**Proof Sketch.** Compare the logical characterisation in Lemmas 36 and 37. The first difference to note is that the effect of  $b_{ki}$ 's is simply a constant offset, and so the sequence would tend to  $-\infty$  with or without its presence. Similar simplifications can be made inside the logarithm: the multiplicative effect of  $r_{ki}$  inside the logarithm can be extracted as an additive offset and thus similarly be discarded.

The second crucial difference is to relax the variable domains from integers to reals. If each of the  $\lambda_i$  in the satisfying assignment is sufficiently large, we show we can relax the condition to real numbers rather than integers without affecting whether the sequence goes to  $-\infty$ . To do this, we test sets of indices  $U$ , where if  $i \in U$  then  $\lambda_i$  needs to be arbitrarily large over all  $C$  (i.e. unbounded). The positions where  $\lambda_i$  is always bounded are again a constant offset and are omitted. ◀

By testing the LC condition and the condition from Lemma 37 for each possible  $X, \mathcal{Y}, k, U$ , in turn using the relevant (conditionally decidable) first-order theory of the reals, we have:

► **Lemma 38.** *Given a weighted automaton  $\mathcal{W}$  and states  $s, s'$  such that  $\mathcal{L}_s(\mathcal{W})$  and  $\mathcal{L}_{s'}(\mathcal{W})$  are plus-letter-bounded, it is decidable whether  $s$  is big-O  $s'$ , subject to Schanuel's conjecture.*

## 6.2 The letter-bounded case

Here we consider the case where  $\mathcal{L}_s(\mathcal{W})$  and  $\mathcal{L}_{s'}(\mathcal{W})$  are letter-bounded,  $\mathcal{L}_s(\mathcal{W})$  and  $\mathcal{L}_{s'}(\mathcal{W})$  are subsets of  $a_1^* \dots a_m^*$  for some  $a_1, \dots, a_m \in \Sigma$ , which is a relaxation of the preceding case. For the plus-letter-bounded case, we relied on a 1-1 correspondence between numeric vectors and words. This correspondence no longer holds in the letter-bounded case: for example,  $a^n$  matches  $a^*b^*a^*$ , but it could correspond to  $(n, 0, 0)$ ,  $(0, 0, n)$ , as well as any  $(n_1, 0, n_2)$  with  $n_1 + n_2 = n$ . Still, there is a reduction to the plus-letter-bounded case.

► **Lemma 39.** *The big-O problem for  $\mathcal{W}, s, s'$  with  $\mathcal{L}_s(\mathcal{W})$  and  $\mathcal{L}_{s'}(\mathcal{W})$  letter-bounded reduces to the plus-letter-bounded case.*

**Proof.** Suppose the LC condition holds and  $\mathcal{L}_s(\mathcal{W}) \subseteq \mathcal{L}_{s'}(\mathcal{W}) \subseteq a_1^* \dots a_m^*$ . Let  $I$  be the set of strictly increasing sequences  $\vec{i} = i_1 \dots i_k$  of integers between 1 and  $m$ . Given  $\vec{i} \in I$ , let  $\mathcal{W}_{\vec{i}}$  be the weighted automaton obtained by intersecting  $\mathcal{W}$  with a DFA for  $a_{i_1}^+ \dots a_{i_k}^+$  whose initial state is  $q$ . Note that  $s$  is big-O of  $s'$  (in  $\mathcal{W}$ ) iff  $(s, q)$  is big-O of  $(s', q)$  in  $\mathcal{W}_{\vec{i}}$  for all  $\vec{i} \in I$ , because  $a_1^* \dots a_m^* = \bigcup_{\vec{i} \in I} a_{i_1}^+ \dots a_{i_k}^+$ . Because the big-O problem for each  $\mathcal{W}_{\vec{i}}, (s, q)$ ,  $(s', q)$  falls into the plus-letter-bounded case, the results follows from Lemma 38. ◀

## 6.3 The bounded case

Here we consider the case where  $\mathcal{L}_s(\mathcal{W})$  and  $\mathcal{L}_{s'}(\mathcal{W})$  are bounded, which is a relaxation of letter-boundedness (see Definition 6):  $\mathcal{L}_s(\mathcal{W})$  and  $\mathcal{L}_{s'}(\mathcal{W})$  are subsets of  $w_1^* \dots w_m^*$  for some  $w_1, \dots, w_m \in \Sigma^*$ . We show a reduction to the letter-bounded case from Section 6.2.

To showcase the difference to the letter-bounded case, consider the language  $(abab)^*a^*b^*(ab)^*$ . Observe that, for example the word  $(ab)^4$  can be decomposed in a number of ways:  $(abab)^2a^0b^0(ab)^0$ ,  $(abab)^1a^1b^1(ab)^1$ ,  $(abab)^1a^0b^0(ab)^2$ ,  $(abab)^0a^1b^1(ab)^3$  or  $(abab)^0a^0b^0(ab)^4$ . One must be careful to consider all such decompositions.

► **Lemma 40.** *The big-O problem for  $\mathcal{W}, s, s'$  with  $\mathcal{L}_s(\mathcal{W})$  and  $\mathcal{L}_{s'}(\mathcal{W})$  bounded reduces to the letter-bounded case.*

**Proof sketch (see Appendix G.3).** Suppose  $\mathcal{W}$  is bounded over  $w_1^* \dots w_m^*$ , we will construct a new weighted automaton  $\mathcal{W}'$  letter-bounded over a new alphabet  $a_1^* \dots a_m^*$  with the following property. For *every* decomposition of a word  $w$ , as  $w_1^{n_1} \dots w_m^{n_m}$ , the weight of  $a_1^{n_1} \dots a_m^{n_m}$  in  $\mathcal{W}'$  is equal to the weight of  $w$  in  $\mathcal{W}$ . ◀

## 7 Conclusion

Despite undecidability results, we have identified several decidable cases of the big-O problem. However, for bounded languages, the result depends on a conjecture from number theory, leaving open the exact borderline between decidability and undecidability.

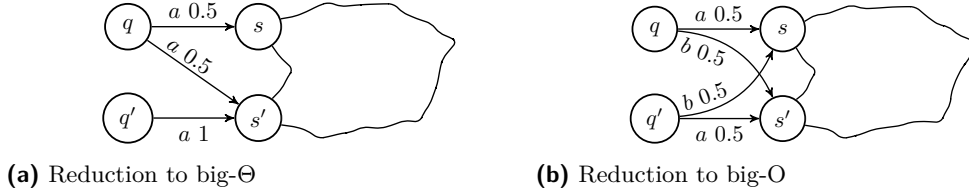
Natural directions for future work include the analogous problem for infinite words, further analysis on ambiguity (e.g., is the big-O problem decidable for  $k$ -ambiguous weighted automata?), and the extension to negative edge weights.

## References

- 1 Shaull Almagor, Udi Boker, and Orna Kupferman. What’s decidable about weighted automata? In *ATVA*, volume 6996 of *Lecture Notes in Computer Science*, pages 482–491. Springer, 2011.
- 2 Shaull Almagor, Dmitry Chistikov, Joël Ouaknine, and James Worrell. O-minimal invariants for linear loops. In Ioannis Chatzigiannakis, Christos Kaklamanis, Dániel Marx, and Donald Sannella, editors, *45th International Colloquium on Automata, Languages, and Programming, ICALP 2018, July 9-13, 2018, Prague, Czech Republic*, volume 107 of *LIPIcs*, pages 114:1–114:14. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2018. doi:10.4230/LIPIcs.ICALP.2018.114.
- 3 Saugata Basu, Richard Pollack, and Marie-Françoise Roy. *Algorithms in Real Algebraic Geometry*, volume 10 of *Algorithms and computation in mathematics*. Springer, 2nd edition, 2006.
- 4 Rohit Chadha, Dileep Kini, and Mahesh Viswanathan. Decidable problems for unary PFAs. In Gethin Norman and William H. Sanders, editors, *Quantitative Evaluation of Systems - 11th International Conference, QEST 2014*, volume 8657 of *Lecture Notes in Computer Science*, pages 329–344. Springer, 2014. doi:10.1007/978-3-319-10696-0\_26.
- 5 Konstantinos Chatzikokolakis, Daniel Gebler, Catuscia Palamidessi, and Lili Xu. Generalized Bisimulation Metrics. In Paolo Baldan and Daniele Gorla, editors, *CONCUR 2014 - Concurrency Theory - 25th International Conference, CONCUR 2014*, volume 8704 of *Lecture Notes in Computer Science*, pages 32–46. Springer, 2014. doi:10.1007/978-3-662-44584-6\_4.
- 6 Taolue Chen and Stefan Kiefer. On the total variation distance of labelled Markov chains. In Thomas A. Henzinger and Dale Miller, editors, *Joint Meeting of the Twenty-Third EACSL Annual Conference on Computer Science Logic (CSL) and the Twenty-Ninth Annual ACM/IEEE Symposium on Logic in Computer Science (LICS), CSL-LICS 2014*, pages 33:1–33:10. ACM, 2014. URL: <http://dl.acm.org/citation.cfm?id=2603088>, doi:10.1145/2603088.2603099.
- 7 Dmitry Chistikov, Andrzej S. Murawski, and David Purser. Asymmetric distances for approximate differential privacy. In Wan Fokkink and Rob van Glabbeek, editors, *30th International Conference on Concurrency Theory, CONCUR 2019*, volume 140 of *LIPIcs*, pages 10:1–10:17. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2019. doi:10.4230/LIPIcs.CONCUR.2019.10.
- 8 Ventsislav Chonev, Joël Ouaknine, and James Worrell. On the Skolem problem for continuous linear dynamical systems. In Ioannis Chatzigiannakis, Michael Mitzenmacher, Yuval Rabani, and Davide Sangiorgi, editors, *43rd International Colloquium on Automata, Languages, and Programming, ICALP 2016, July 11-15, 2016, Rome, Italy*, volume 55 of *LIPIcs*, pages 100:1–100:13. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2016. doi:10.4230/LIPIcs.ICALP.2016.100.
- 9 Marek Chrobak. Finite automata and unary languages. *Theor. Comput. Sci.*, 47(3):149–158, 1986. doi:10.1016/0304-3975(86)90142-8.
- 10 Thomas Colcombet. Unambiguity in automata theory. In Jeffrey O. Shallit and Alexander Okhotin, editors, *Descriptive Complexity of Formal Systems - 17th International Workshop, DCFS 2015*, volume 9118 of *Lecture Notes in Computer Science*, pages 3–18. Springer, 2015. doi:10.1007/978-3-319-19225-3\_1.
- 11 T. H. Cormen, C. E. Leiserson, and R. L. Rivest. *Introduction to Algorithms*. MIT Press, 1990.
- 12 Laure Daviaud, Marcin Jurdzinski, Ranko Lazic, Filip Mazowiecki, Guillermo A. Pérez, and James Worrell. When is containment decidable for probabilistic automata? In Ioannis Chatzigiannakis, Christos Kaklamanis, Dániel Marx, and Donald Sannella, editors, *45th International Colloquium on Automata, Languages, and Programming, ICALP 2018, July 9-13, 2018, Prague, Czech Republic*, volume 107 of *LIPIcs*, pages 121:1–121:14. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2018. doi:10.4230/LIPIcs.ICALP.2018.121.

- 13 C. Dehnert, S. Junges, J.-P. Katoen, and M. Volk. A Storm is coming: A modern probabilistic model checker. In *Proceedings of Computer Aided Verification (CAV)*, pages 592–600. Springer, 2017.
- 14 Cynthia Dwork, Frank McSherry, Kobbi Nissim, and Adam D. Smith. Calibrating Noise to Sensitivity in Private Data Analysis. In Shai Halevi and Tal Rabin, editors, *Theory of Cryptography, Third Theory of Cryptography Conference, TCC 2006*, volume 3876 of *Lecture Notes in Computer Science*, pages 265–284. Springer, 2006. doi:10.1007/11681878\_14.
- 15 Shimon Even, Alan L. Selman, and Yacov Yacobi. The complexity of promise problems with applications to public-key cryptography. *Information and Control*, 61(2):159–173, 1984.
- 16 Nathanaël Fijalkow. Undecidability results for probabilistic automata. *SIGLOG News*, 4(4):10–17, 2017. URL: <https://dl.acm.org/citation.cfm?id=3157833>.
- 17 Nathanaël Fijalkow, Hugo Gimbert, and Youssef Oualhadj. Deciding the value 1 problem for probabilistic leaktight automata. In *Proceedings of the 27th Annual IEEE Symposium on Logic in Computer Science, LICS 2012*, pages 295–304. IEEE Computer Society, 2012. doi:10.1109/LICS.2012.40.
- 18 Shmuel Friedland and Hans Schneider. The growth of powers of a nonnegative matrix. *SIAM J. Matrix Analysis Applications*, 1(2):185–200, 1980. doi:10.1137/0601022.
- 19 Pawel Gawrychowski, Dalia Krieger, Narad Rampersad, and Jeffrey Shallit. Finding the growth rate of a regular or context-free language in polynomial time. *Int. J. Found. Comput. Sci.*, 21(4):597–618, 2010. doi:10.1142/S0129054110007441.
- 20 Hugo Gimbert and Youssef Oualhadj. Probabilistic automata on finite words: Decidable and undecidable problems. In Samson Abramsky, Cyril Gavaille, Claude Kirchner, Friedhelm Meyer auf der Heide, and Paul G. Spirakis, editors, *Automata, Languages and Programming, 37th International Colloquium, ICALP 2010, Bordeaux, France, July 6-10, 2010, Proceedings, Part II*, volume 6199 of *Lecture Notes in Computer Science*, pages 527–538. Springer, 2010. doi:10.1007/978-3-642-14162-1\_44.
- 21 Seymour Ginsburg. *The Mathematical Theory of Context-Free Languages*. McGraw-Hill, 1966.
- 22 Seymour Ginsburg and Edwin H Spanier. Bounded algol-like languages. *Transactions of the American Mathematical Society*, 113(2):333–368, 1964.
- 23 Thanh Minh Hoang and Thomas Thierauf. The complexity of the characteristic and the minimal polynomial. *Theor. Comput. Sci.*, 295:205–222, 2003. doi:10.1016/S0304-3975(02)00404-8.
- 24 Cheng-Chao Huang, Jing-Cao Li, Ming Xu, and Zhi-Bin Li. Positive root isolation for poly-powers by exclusion and differentiation. *Journal of Symbolic Computation*, 85:148–169, 2018. 41th International Symposium on Symbolic and Algebraic Computation (ISSAC’16). doi:<https://doi.org/10.1016/j.jsc.2017.07.007>.
- 25 Stefan Kiefer. On computing the total variation distance of hidden Markov models. In Ioannis Chatzigiannakis, Christos Kaklamanis, Dániel Marx, and Donald Sannella, editors, *45th International Colloquium on Automata, Languages, and Programming, ICALP 2018*, volume 107 of *LIPIcs*, pages 130:1–130:13. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2018. doi:10.4230/LIPIcs.ICALP.2018.130.
- 26 Stefan Kiefer, Andrzej S. Murawski, Joël Ouaknine, Björn Wachter, and James Worrell. On the Complexity of Equivalence and Minimisation for Q-weighted Automata. *Logical Methods in Computer Science*, 9(1), 2013. doi:10.2168/LMCS-9(1:8)2013.
- 27 Daniel Kroh. The equality problem for rational series with multiplicities in the tropical semiring is undecidable. *International Journal of Algebra and Computation*, 4:405–425, 1994.
- 28 M. Kwiatkowska, G. Norman, and D. Parker. PRISM 4.0: Verification of probabilistic real-time systems. In *Proceedings of Computer Aided Verification (CAV)*, volume 6806 of *LNCS*, pages 585–591. Springer, 2011.
- 29 Serge Lang. *Introduction to transcendental numbers*. Addison-Wesley Pub. Co., 1966.
- 30 Angus Macintyre and Alex J Wilkie. On the decidability of the real exponential field, 1996.
- 31 Rupak Majumdar, Mahmoud Salamati, and Sadegh Soudjani. On decidability of time-bounded reachability in CTMDPs. In Artur Czumaj, Anuj Dawar, and Emanuela Merelli,

- editors, *47th International Colloquium on Automata, Languages, and Programming (ICALP 2020)*, volume 168 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 133:1–133:19, Dagstuhl, Germany, 2020. Schloss Dagstuhl–Leibniz-Zentrum für Informatik. doi: 10.4230/LIPIcs.ICALP.2020.133.
- 32 Andrew Martinez. Efficient computation of regular expressions from unary NFAs. In Jürgen Dassow, Maia Hoeberechts, Helmut Jürgensen, and Detlef Wotschke, editors, *Fourth International Workshop on Descriptive Complexity of Formal Systems - DCFS 2002*, volume Report No. 586, pages 174–187. Department of Computer Science, The University of Western Ontario, Canada, 2002.
  - 33 David Mestel. Quantifying information flow in interactive systems. In *32nd IEEE Computer Security Foundations Symposium, CSF 2019, Hoboken, NJ, USA, June 25–28, 2019*, pages 414–427. IEEE, 2019. doi:10.1109/CSF.2019.00035.
  - 34 David Mestel. Widths of Regular and Context-Free Languages. In *39th IARCS Annual Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS 2019)*, volume 150 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 49:1–49:14, Dagstuhl, Germany, 2019. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik. URL: <https://drops.dagstuhl.de/opus/volltexte/2019/11611>, doi:10.4230/LIPIcs.FSTTCS.2019.49.
  - 35 Albert R. Meyer and Larry J. Stockmeyer. The equivalence problem for regular expressions with squaring requires exponential space. In *Proceedings of the 13th Annual Symposium on Switching and Automata Theory, College Park, Maryland, USA, October 25–27, 1972*, pages 125–129. IEEE Computer Society, 1972.
  - 36 Joël Ouaknine and James Worrell. Positivity problems for low-order linear recurrence sequences. In Chandra Chekuri, editor, *Proceedings of the Twenty-Fifth Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2014*, pages 366–379. SIAM, 2014. doi:10.1137/1.9781611973402.27.
  - 37 Rohit J Parikh. On context-free languages. *Journal of the ACM (JACM)*, 13(4):570–581, 1966.
  - 38 Azaria Paz. *Introduction to probabilistic automata*. Academic Press, 2014.
  - 39 Bjorn Poonen. Hilbert’s tenth problem over rings of number-theoretic interest. *Note from the lecture at the Arizona Winter School on “Number Theory and Logic”*, 2003. URL: <https://math.mit.edu/~poonen/papers/aws2003.pdf>.
  - 40 Hans Schneider. The influence of the marked reduced graph of a nonnegative matrix on the Jordan form and on related properties: A survey. *Linear Algebra and its Applications*, 84:161–189, 1986.
  - 41 Marcel Paul Schützenberger. On the definition of a family of automata. *Information and Control*, 4(2-3):245–270, 1961. doi:10.1016/S0019-9958(61)80020-X.
  - 42 Bruno Sericola. *Markov chains: theory and applications*. John Wiley & Sons, 2013.
  - 43 Adam D. Smith. Efficient, Differentially Private Point Estimators. *CoRR*, abs/0809.4794, 2008. URL: <http://arxiv.org/abs/0809.4794>.
  - 44 Larry J. Stockmeyer and Albert R. Meyer. Word problems requiring exponential time: Preliminary report. In Alfred V. Aho, Allan Borodin, Robert L. Constable, Robert W. Floyd, Michael A. Harrison, Richard M. Karp, and H. Raymond Strong, editors, *Proceedings of the 5th Annual ACM Symposium on Theory of Computing, 1973*, pages 1–9. ACM, 1973. doi:10.1145/800125.804029.
  - 45 Anthony Widjaja To. Unary finite automata vs. arithmetic progressions. *Inf. Process. Lett.*, 109(17):1010–1014, 2009. doi:10.1016/j.ipl.2009.06.005.
  - 46 Wen-Guey Tzeng. A polynomial-time algorithm for the equivalence of probabilistic automata. *SIAM J. Comput.*, 21(2):216–227, 1992. doi:10.1137/0221017.
  - 47 Wen-Guey Tzeng. On path equivalence of nondeterministic finite automata. *Inf. Process. Lett.*, 58(1):43–46, 1996. doi:10.1016/0020-0190(96)00039-7.
  - 48 Michel Waldschmidt. *Diophantine Approximation on Linear Algebraic Groups*, volume 326 of *Grundlehren der mathematischen Wissenschaften (A Series of Comprehensive Studies in Mathematics)*. Springer, Berlin, Heidelberg, 2000.



■ **Figure 4** Reductions between big-O and big- $\Theta$

## A Additional notation for the appendix

We will typically define weighted automata by listing transitions as  $q \xrightarrow{a} q'$  (to mean  $M(a)(q, q') = p$ ) with the assumption that any unspecified transition has weight 0.

## B Additional material for Section 1

► **Proposition 41.** *For  $r$ , and  $rd$ , on labelled Markov chains, it is sufficient to consider the supremum over  $w \in \Sigma^*$  rather than  $E \subseteq \Sigma^*$ .*

**Proof of Proposition 41.** We will show we can approximate any event by a finite subset, then we can always simplify an event with more than one word, and not decrease.

Suppose  $\frac{a+b}{c+d} > \frac{a}{c}$  and  $\frac{a+b}{c+d} > \frac{b}{d}$ . By the first we have  $ac + bc > ac + dc = bc > ad \implies \frac{b}{d} > \frac{a}{c}$ . By the second we have  $ad + bd > bc + bd = ad > bc \implies \frac{a}{c} > \frac{b}{d}$ . Contradiction.

Hence, for the purposes of maximisation, given  $f, g$  and a *finite* set  $E$ , such a set can always be simplified, by repeated application. That is, there exists  $e'$  such that,

$$\frac{\sum_{e \in E} f(e)}{\sum_{e \in E} g(e)} \leq \frac{f(e')}{g(e')}. \quad (1)$$

Consider an event  $E \subseteq \Sigma^*$ , then for every  $\lambda > 0$  there is a  $k$  such that  $f_s(E \cap \Sigma^{>k}) \leq \lambda$ . Then  $f_s(E \cap \Sigma^{\leq k}) \leq f_s(E) \leq f_s(E \cap \Sigma^{\leq k}) + \lambda$  [25, Lemma 12]. For any  $\epsilon$ , by choice of sufficiently small  $\lambda$  there is a finite set  $E'$  such that  $\frac{f_s(E')}{f_{s'}(E')} - \epsilon \leq \frac{f_s(E)}{f_{s'}(E)} \leq \frac{f_s(E')}{f_{s'}(E')} + \epsilon$ .

Consider  $\sup_{E \subseteq \Sigma^*} \frac{f_s(E)}{f_{s'}(E)}$ , this is equivalent to  $\lim_{k \rightarrow \infty} \sup_{E \subseteq \Sigma^* \cap \Sigma^{\leq k}} \frac{f_s(E)}{f_{s'}(E)}$  and by Equation (1) this is equivalent to  $\lim_{k \rightarrow \infty} \sup_{w \in \Sigma^* \cap \Sigma^{\leq k}} \frac{f_s(w)}{f_{s'}(w)} = \sup_{w \in \Sigma^*} \frac{f_s(w)}{f_{s'}(w)}$ . ◀

## C Additional material for Section 2

► **Lemma 42.** *The big-O problem is interreducible with the big- $\Theta$  problem.*

**Proof. big-O problem reduces to the big- $\Theta$  problem:** To ask if  $s$  is big-O of  $s'$ , add states  $q, q'$  using the construction of Figure 4a, then ask if  $q$  is big- $\Theta$  of  $q'$ .

$$\frac{f_q(aw)}{f_{q'}(aw)} = \frac{0.5f_s(w) + 0.5f_{s'}(w)}{f_{s'}(w)} < C \iff \frac{f_s(w)}{f_{s'}(w)} < 2C - 1$$

$$\frac{f_{q'}(aw)}{f_q(aw)} = \frac{f_{s'}(w)}{0.5f_s(w) + 0.5f_{s'}(w)} \leq 2$$

**big- $\Theta$  problem reduces to the big-O problem:** To ask if  $s$  is big- $\Theta$  of  $s'$ , add states  $q, q'$  using the construction of Figure 4b, then ask if  $q$  is big-O of  $q'$ .



$$\frac{f_q(aw)}{f_{q'}(aw)} = \frac{0.5f_s(w)}{0.5f_{s'}(w)} < C \iff \frac{f_s(w)}{f_{s'}(w)} < C$$

$$\frac{f_q(bw)}{f_{q'}(bw)} = \frac{0.5f_{s'}(w)}{0.5f_s(w)} < C \iff \frac{f_{s'}(w)}{f_s(w)} < C$$

Each of the reductions adds a constant number of bits, as such they operate in logarithmic space.  $\blacktriangleleft$

## D Additional material for Section 3

In this section we use the notation that  $\mathbb{P}_{\mathcal{A}}(w) = f_{q_s}(w)$ , where  $q_s$  is the start state of the probabilistic automaton  $\mathcal{A}$ . This is to avoid confusion when there is both the probabilistic automaton being reduced from and the labelled Markov chain being reduced to. Henceforth in this section, the notation  $f_s(w)$  refers to the labelled Markov chain.

### Undecidability by Emptiness of Probabilistic automata (Theorem 8)

The following lemma plays a key role in proving the result. In its statement, “undecidable to distinguish” means that the corresponding *promise problem* (see e.g. [15]) is undecidable. In other words, if the input is not in one of the two cases which should be distinguished between, the answer is not specified and can be arbitrary (including non-termination).

Results in this section are presented on ratio total variation distances on *labelled Markov chains*, and thus apply to the big-O problem in the more general weighted automata.

► **Lemma 43.** 1. *Given an LMC along with two states  $s, s'$  and constant  $c$ , it is undecidable to distinguish between  $r(s, s') \leq c$  and  $r(s, s') = \infty$ .*

2. *Given an LMC along with two states  $s, s''$  and two numbers  $c$  and  $C$  such that  $c < C$ , it is undecidable to distinguish between  $r(s, s'') \leq c$  and  $C \leq r(s, s'') < \infty$ .*

*Both statements remain true if  $r$  is replaced with  $rd$ .*

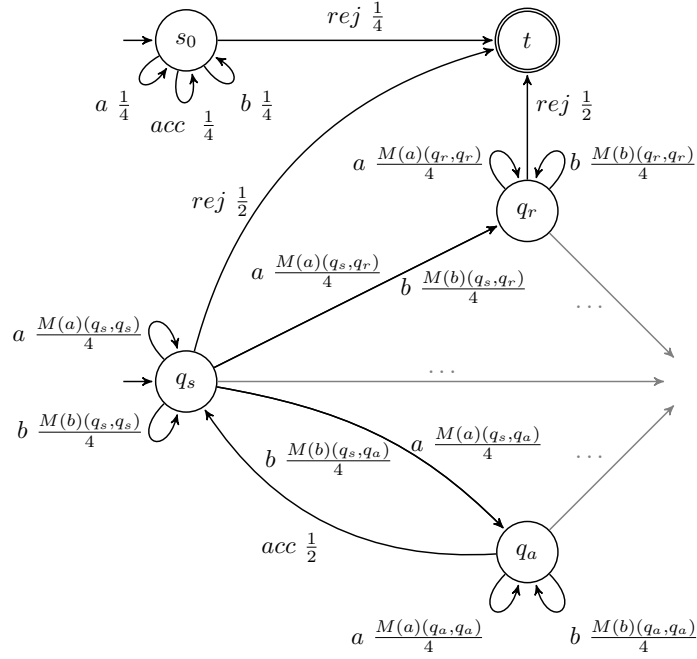
**Proof.** For both cases, we reduce from EMPTY. We show our construction for  $\Sigma = \{a, b\}$ , but the procedure can be generalised to arbitrary alphabets.

The construction will create two branches of a labelled Markov chain. The first, from state  $q_s$ , will simulate the given probabilistic automaton using the original weights multiplied by the same scalar (in this case  $\frac{1}{4}$ ). The other branch, from state  $s_0$ , will process each letter from  $\Sigma$  with equal weight (also  $\frac{1}{4}$  in an infinite loop). Consequently, if there is a word accepted with probability greater than  $\frac{1}{2}$ , the ratio between the two branches will be greater than 1. The construction will make it possible to process words repeatedly, so that the ratio can then be pumped unboundedly.

Formally, given a probabilistic automaton  $\mathcal{A} = \langle Q, \Sigma, M, F \rangle$  with start state  $q_s$ . First observe that w.l.o.g.  $q_s$  is not accepting, since in this case the empty word is accepted with probability 1, and thus there is a word with probability greater than  $\frac{1}{2}$  and a trivial positive instance of the big-O problem can be returned.

We construct the LMC  $\langle Q', \Sigma', \delta, F' \rangle$  taking  $Q' = Q \uplus \{s, s', s'', s_0, t\}$  where  $\uplus$  denotes disjoint union,  $\Sigma' = \{a, b, acc, rej, \vdash\}$ ,  $F' = \{t\}$  and  $\delta$  as specified below. First we simulate the probabilistic automaton with a scaling factor of  $\frac{1}{4}$ : for all  $q, q' \in Q$ ,

$$q \xrightarrow[\frac{1}{4}]{M(a)(q, q')} q' \quad q \xrightarrow[\frac{1}{4}]{M(b)(q, q')} q'.$$



■ **Figure 5** Reduction; where  $q_a$  represents accepting states of the probabilistic automaton,  $q_r$  represents rejecting states and  $q_s$  represents the start state (assumed to be rejecting).

Originally accepting runs trigger a restart, while rejecting ones are redirected to  $t$ :

$$\text{if } q \in F : q \xrightarrow[\text{acc}]{\frac{1}{2}} q_s \quad \text{and} \quad \text{if } q \notin F : q \xrightarrow[\text{rej}]{\frac{1}{2}} t.$$

We then add a part of the chain which behaves equally, rather than according to the probabilistic automaton:

$$s_0 \xrightarrow[a]{\frac{1}{4}} s_0 \quad s_0 \xrightarrow[b]{\frac{1}{4}} s_0 \quad s_0 \xrightarrow[\text{acc}]{\frac{1}{4}} s_0 \quad s_0 \xrightarrow[\text{rej}]{\frac{1}{4}} t.$$

The construction is illustrated in Figure 5. To complete the reduction, we add the following transitions from  $s, s', s''$ .

$$s \xrightarrow[\vdash]{\frac{1}{2}} s_0 \quad s \xrightarrow[\vdash]{\frac{1}{2}} q_s \quad s' \xrightarrow[\vdash]{\frac{1}{2}} s_0 \quad s'' \xrightarrow[\vdash]{\frac{99}{100}} s_0 \quad s'' \xrightarrow[\vdash]{\frac{1}{100}} q_s$$

We make the following claims:

▷ **Claim 44.** If  $\mathcal{A} \notin \text{EMPTY}$  then  $r(s, s') = \infty$ . If  $\mathcal{A} \in \text{EMPTY}$  then  $r(s, s') \leq 2$ .

▷ **Claim 45.** If  $\mathcal{A} \notin \text{EMPTY}$  then  $49 < r(s, s'') \leq 51$ . If  $\mathcal{A} \in \text{EMPTY}$  then  $r(s, s'') \leq 2$ .

Correctness of the reduction (for  $r$ ) follows from the undecidability of **EMPTY**. Note that  $s, s''$  are taken to be certain “linear combinations” of  $s_0$  and  $q_s$ . This ensures that  $r(s', s) \leq 2$  and  $r(s'', s) \leq 2$ , consequently the claims for  $rd$  will follow.

**Proof of Claim 44.** First observe that

$$\frac{f_s(\vdash w')}{f_{s'}(\vdash w')} = \frac{\frac{1}{2}f_{s_0}(w') + \frac{1}{2}f_{q_s}(w')}{f_{s_0}(w')} = \frac{1}{2} + \frac{1}{2} \frac{f_{q_s}(w')}{f_{s_0}(w')} \quad (2)$$

If there is a word  $w$  that is accepted by the automaton with probability  $> \frac{1}{2}$ , then let  $w' = (w \text{ acc})^i \text{ rej}$  and we have

$$\frac{f_{q_s}(w')}{f_{s_0}(w')} = \frac{((\frac{1}{4})^{|w|} \mathbb{P}(w) \frac{1}{2})^i}{((\frac{1}{4})^{|w|} \frac{1}{4})^i} = (2\mathbb{P}(w))^i \quad (3)$$

Since  $\mathbb{P}(w) > \frac{1}{2}$  then  $2\mathbb{P}(w) > 1$  and we have:

$$\lim_{i \rightarrow \infty} \frac{f_s(\vdash (w \text{ acc})^i \text{ rej})}{f_{s'}(\vdash (w \text{ acc})^i \text{ rej})} = \infty \quad \text{and} \quad r(s, s') = rd(s, s') = \infty.$$

If there is no such word then  $\forall w \in \Sigma^* : \mathbb{P}(w) \leq \frac{1}{2}$ , then probability ratio of all words is bounded. All words start with  $\vdash$  and are terminated by  $\text{rej}$ , so in general all words take the form  $w = \vdash ((w_1 \text{ acc}) \dots (w_n \text{ acc})(w_{n+1} \text{ rej}))$ . Let us consider the probability of  $w' = ((w_1 \text{ acc}) \dots (w_n \text{ acc})(w_{n+1} \text{ rej}))$  words from  $s_0$  and  $q_s$ . Then:

$$\frac{f_{q_s}(w')}{f_{s_0}(w')} \quad (4)$$

$$= \frac{(\prod_{i=1}^n \frac{1}{2} (\frac{1}{4})^{|w_i|} \mathbb{P}[w_i]) ((\frac{1}{4})^{|w_{n+1}|} (1 - \mathbb{P}[w_{n+1}]) \frac{1}{2})}{(\frac{1}{4})^{|w_1| + \dots + |w_n|} (\frac{1}{4})^n (\frac{1}{4})^{|w_{n+1}|} \frac{1}{4}} \quad (5)$$

$$\leq \frac{((\frac{1}{4})^{|w_1| + \dots + |w_n|} (\frac{1}{2})^n (\frac{1}{2})^n ((\frac{1}{4})^{|w_{n+1}|} \frac{1}{2}))}{(\frac{1}{4})^{|w_1| + \dots + |w_n| + n} (\frac{1}{4})^{|w_{n+1}|} \frac{1}{4}} \quad (\forall i : \mathbb{P}[w_i] \leq \frac{1}{2})$$

$$= 2 \quad (6)$$

Then using Equation (2) we have for every word  $w$  we have  $\frac{1}{2} \leq \frac{f_s(w)}{f_{s'}(w)} \leq \frac{3}{2}$  and  $r(s, s') \leq \frac{3}{2}$  and  $rd(s, s') \leq 2$ .  $\triangleleft$

Proof of Claim 45. First observe that the direction of  $\frac{f_{s''}(\vdash w)}{f_s(\vdash w)}$  is always  $\leq 2$ , resulting in the only interesting direction being  $\frac{f_s(\vdash w)}{f_{s''}(\vdash w)}$ :

$$\begin{aligned} \frac{f_{s''}(\vdash w)}{f_s(\vdash w)} &= \frac{\frac{99}{100} f_{s_0}(w) + \frac{1}{100} f_{q_s}(w)}{\frac{1}{2} f_{s_0}(w) + \frac{1}{2} f_{q_s}(w)} \\ &= \frac{\frac{99}{100} f_{s_0}(w)}{\frac{1}{2} f_{s_0}(w) + \frac{1}{2} f_{q_s}(w)} + \frac{\frac{1}{100} f_{q_s}(w)}{\frac{1}{2} f_{s_0}(w) + \frac{1}{2} f_{q_s}(w)} \\ &\leq \frac{\frac{99}{100} f_{s_0}(w)}{\frac{1}{2} f_{s_0}(w)} + \frac{\frac{1}{100} f_{q_s}(w)}{\frac{1}{2} f_{q_s}(w)} \\ &= \frac{2 \cdot 99}{100} + \frac{2}{100} = 2 \end{aligned}$$

We observe that for all words  $\vdash w$ ,  $r$  and  $rd$  is bounded:

$$\begin{aligned} \frac{f_s(\vdash w)}{f_{s''}(\vdash w)} &= \frac{\frac{1}{2} f_{s_0}(w) + \frac{1}{2} f_{q_s}(w)}{\frac{99}{100} f_{s_0}(w) + \frac{1}{100} f_{q_s}(w)} \\ &= \frac{\frac{1}{2} f_{s_0}(w)}{\frac{99}{100} f_{s_0}(w) + \frac{1}{100} f_{q_s}(w)} + \frac{\frac{1}{2} f_{q_s}(w)}{\frac{99}{100} f_{s_0}(w) + \frac{1}{100} f_{q_s}(w)} \\ &\leq \frac{\frac{1}{2} f_{s_0}(w)}{\frac{99}{100} f_{s_0}(w)} + \frac{\frac{1}{2} f_{q_s}(w)}{\frac{1}{100} f_{q_s}(w)} \\ &\leq \frac{100}{2 \cdot 99} + \frac{100}{2} \leq 51 \end{aligned}$$

If there is a word  $w$  that is accepted by the automaton with probability  $> \frac{1}{2}$ , then we consider the word  $\vdash (w \text{ acc})^i \text{ rej}$ , let  $w' = (w \text{ acc})^i \text{ rej}$ .

$$\begin{aligned} \frac{f_s(\vdash (w \text{ acc})^i \text{ rej})}{f_{s''}(\vdash (w \text{ acc})^i \text{ rej})} &= \frac{\frac{1}{2}f_{s_0}(w') + \frac{1}{2}f_{q_s}(w')}{\frac{99}{100}f_{s_0}(w') + \frac{1}{100}f_{q_s}(w')} \\ &\geq \frac{\frac{1}{2}f_{q_s}(w')}{\frac{99}{100}f_{s_0}(w') + \frac{1}{100}f_{q_s}(w')} \end{aligned}$$

By the previous proof (Equation (3)) we know  $\frac{f_{q_s}(w')}{f_{s_0}(w')} \xrightarrow{i \rightarrow \infty} \infty$ , thus  $\frac{f_{s_0}(w')}{f_{q_s}(w')} \xrightarrow{i \rightarrow \infty} 0$ . Consider

$$\frac{\frac{99}{100}f_{s_0}(w') + \frac{1}{100}f_{q_s}(w')}{\frac{1}{2}f_{q_s}(w')} = \frac{2}{100} + \frac{2 \cdot 99}{100} \left[ \frac{f_{s_0}(w')}{f_{q_s}(w')} \right] \xrightarrow{i \rightarrow \infty} \frac{2}{100}$$

Then  $\frac{\frac{1}{2}f_{q_s}(w')}{\frac{99}{100}f_{s_0}(w') + \frac{1}{100}f_{q_s}(w')} \xrightarrow{i \rightarrow \infty} \frac{100}{2} = 50$ . So for all  $\epsilon$  there exists an  $i$  such that  $\frac{f_s(\vdash (w \text{ acc})^i \text{ rej})}{f_{s''}(\vdash (w \text{ acc})^i \text{ rej})} \geq 50 - \epsilon$ . In particular for example  $r(s, s'') \geq 49$ .

If there is no such word then  $\forall w \in \Sigma^* : \mathbb{P}(w) \leq \frac{1}{2}$ , then we show the total variation distance will be small. All words start with  $\vdash$  and are terminated by  $\text{rej}$ , so in general all words take the form  $w = \vdash ((w_1 \text{ acc}) \dots (w_n \text{ acc})(w_{n+1} \text{ rej}))$ . Let us consider the probability of such words from  $s, s''$ .

$$\begin{aligned} \frac{f_s(w)}{f_{s''}(w)} &= \frac{\frac{1}{2}f_{s_0}(w') + \frac{1}{2}f_{q_s}(w')}{\frac{99}{100}f_{s_0}(w') + \frac{1}{100}f_{q_s}(w')} \leq \frac{\frac{1}{2}f_{s_0}(w') + \frac{1}{2}f_{q_s}(w')}{\frac{99}{100}f_{s_0}(w')} \\ &\leq \frac{100}{99} \cdot \left[ \frac{1}{2} + \frac{1}{2} \frac{f_{q_s}(w')}{f_{s_0}(w')} \right] \\ &\leq \frac{100}{99} \cdot \frac{3}{2} \quad (\text{by Equation (6)}) \\ &\leq 2 \end{aligned}$$

This creates a significant gap between the case where there is a word with probability greater than one half and not; in particular if  $\exists w : \mathbb{P}(w) > \frac{1}{2}$  then  $49 < r(s, s'') \leq 51$  and  $49 < rd(s, s'') \leq 51$  and if not then  $r(s, s'') \leq 2$  and  $rd(s, s'') \leq 2$ .  $\triangleleft$

## Theorem 8

Lemma 43 implies Theorem 8.

**Proof of Theorem 8.** We reason by contradiction using Lemma 43. For the big-O problem, it suffices to observe that, if it were decidable, one could use it to solve the first promise problem from the Lemma (recall that in a promise problem the input is guaranteed to fall into one of the two cases). This would contradict Lemma 43.

Similarly, the decidability of the (asymmetric) threshold problem would allow us to distinguish between  $r(s, s') \leq c$  and  $C \leq r(s, s') < \infty$  (second promise problem from the Lemma) by considering the instance  $r(s, s') \leq \frac{c+C}{2}$  (non-strict variant) or  $r(s, s') < \frac{c+C}{2}$  (strict variant). A positive answer (regardless of the variant) implies  $r(s, s') < C$ , while a negative one yields  $r(s, s') > c$ , which suffices to distinguish the cases. Note that in both

cases  $r(s, s')$  is bounded, so the reasoning remains valid if it is known in advance that  $r(s, s')$  is bounded.

For additive (asymmetric) approximation, we observe that finding  $x$  such that  $|r(s, s') - x| \leq \frac{C-c}{4}$  and comparing it with  $\frac{c+C}{2}$  makes it possible to distinguish between  $r(s, s') \leq c$  and  $C \leq r(s, s') < \infty$ . This is because  $r(s, s') \leq c$  then implies  $x < \frac{c+C}{2}$  and  $C \leq r(s, s')$  implies  $\frac{c+C}{2} < x$ .

In the multiplicative case, finding  $x$  such that  $1 - \frac{C-c}{4C} \leq \frac{x}{r(s, s')} \leq 1 + \frac{C-c}{4C}$  and comparing  $x$  with  $\frac{c+C}{2}$  yields an analogous argument.

Since Lemma 43 also applies to  $rd$ , all of our results hold when  $r$  is replaced by  $rd$ . ◀

## D.1 The relation to the Value-1 Problem

The previous section showed undecidability of the big-O problem via the emptiness problem for probabilistic automata. Another undecidable problem for probabilistic automata is the VALUE-1 problem [20]. The VALUE-1 problem asks whether some word of a probabilistic automaton is one, or at least arbitrarily close to 1. This section shows that there is a close, but not complete, connection between the VALUE-1 problem and big-O problem by reducing in both directions between the two, the results are shown in Lemmas 47 and 48.

► **Definition 46.** *The VALUE-1 problem, given a Probabilistic Automaton  $\mathcal{A}$ , asks if for all  $\delta > 0$  there exists a word  $w$  such that  $\mathbb{P}_{\mathcal{A}}(w) > 1 - \delta$ .*

► **Lemma 47.** *VALUE-1 problem reduces to the big-O problem*

► **Lemma 48.** *The big-O problem reduces to VALUE-1 problem.*

### Proof of Lemma 47 (Value-1 reduces to big-O).

Given a probabilistic automaton  $\mathcal{A} = \langle Q, \Sigma, M, F \rangle$  and a dedicated starting state  $q_0 \in Q$ , which accepts words with probability  $\mathbb{P}_{\mathcal{A}}(w)$ , first construct  $\mathcal{A}'$  in which words are accepted with probability  $\mathbb{P}_{\mathcal{A}'}(w) = 1 - \mathbb{P}_{\mathcal{A}}(w)$ , by inverting accepting states.

The proof uses a two letter alphabet,  $\Sigma = \{a, b\}$ , but the procedure can be generalised to arbitrary alphabets. Construct a Markov chain  $\mathcal{M}_{\mathcal{A}} = \langle Q', \Sigma', M', F' \rangle$ , where  $Q' = Q \cup \{s, s', s_0, rej, acc\}$ ,  $\Sigma' = \{a, b, c\}$  and  $F' = \{acc\}$ . The probabilistic automaton will be simulated by  $\mathcal{M}_{\mathcal{A}}$ . The relation  $M'$  is described by the notation  $\xrightarrow[p]{a}$ :

For all  $q \in Q$ :

$$\forall q' \in Q : q \xrightarrow[\frac{1}{a}]{\frac{1}{3}M(a)(q, q')} q' \quad q \xrightarrow[\frac{1}{b}]{\frac{1}{3}M(b)(q, q')} q'$$

$$\text{if } q \in F : q \xrightarrow[\frac{1}{c}]{\frac{1}{3}} acc \quad \text{and} \quad \text{if } q \notin F : q \xrightarrow[\frac{1}{c}]{\frac{1}{3}} rej$$

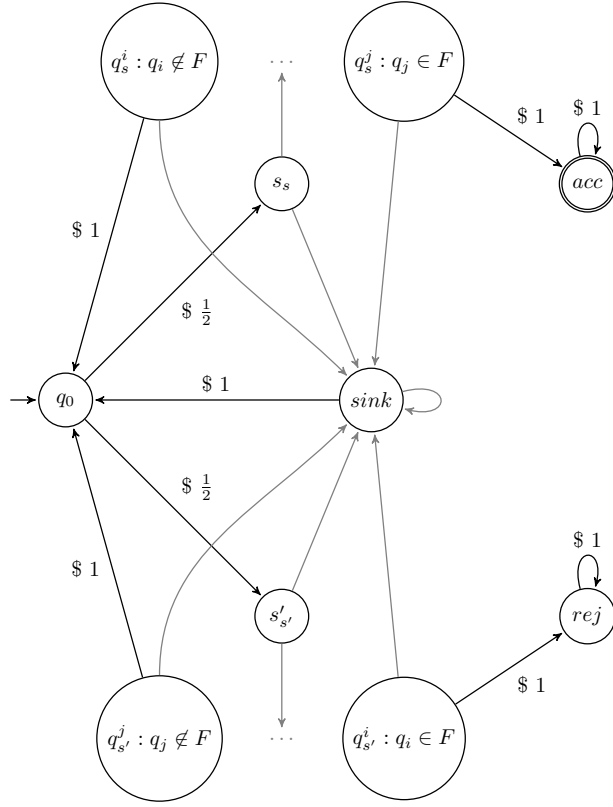
$$s' \xrightarrow[\frac{1}{c}]{\frac{1}{3}} q_0 \quad s \xrightarrow[\frac{1}{c}]{\frac{1}{3}} s_0 \quad s_0 \xrightarrow[\frac{1}{a}]{\frac{1}{3}} s_0 \quad s_0 \xrightarrow[\frac{1}{b}]{\frac{1}{3}} s_0 \quad s_0 \xrightarrow[\frac{1}{c}]{\frac{1}{3}} acc$$

Note the only words with positive probability are words of the form  $c\Sigma^*c \subseteq \Sigma'^*$ . Then given a word  $w \in \Sigma^*$ ,  $f_s(cwc) = (\frac{1}{|\Sigma|+1})^{|wc|}$  and  $f_{s'}(cwc) = (\frac{1}{|\Sigma|+1})^{|wc|}(1 - \mathbb{P}_{\mathcal{A}}(w))$ .

Then if there is a sequence of words for which  $\mathbb{P}_{\mathcal{A}}(w)$  tends to 1 then  $\frac{f_s(cwc)}{f_{s'}(cwc)}$  is unbounded.

However, if there exists some  $\gamma > 0$  so that for all  $w \in \Sigma^*$  we have  $\mathbb{P}_{\mathcal{A}}(w) \leq (1 - \gamma)$  then  $(1 - \mathbb{P}_{\mathcal{A}}(w)) \geq \gamma$ , and so  $\frac{f_s(cwc)}{f_{s'}(cwc)} \leq \frac{1}{\gamma}$ . ◀

**Proof of Lemma 48 (big-O reduces to Value-1).** Given  $\mathcal{M} = \langle Q, \Sigma, M, F \rangle$  and  $s, s' \in Q$ , construct a probabilistic automaton  $\mathcal{A} = \langle Q', \Sigma', M', F' \rangle$ . Each state of  $Q$  will be duplicated, once for  $s$  and once for  $s'$ ;  $Q_s = \{q_s \mid q \in Q\}$ ,  $Q_{s'} = \{q_{s'} \mid q \in Q\}$ . Let  $Q' = Q_s \cup Q_{s'} \cup \{q_0, acc, rej, sink\}$ ,  $\Sigma' = \Sigma \cup \{\$ \}$  and  $F' = \{acc\}$ . The reduction can be seen in Figure 6.



■ **Figure 6** Reduction to VALUE-1. Only the effect of transitions on the \$ symbol are shown in black, with the possibility to transition to the sink state depicted in grey (on symbols in  $\Sigma$ ). All remaining transitions are omitted.

Each transition of  $\mathcal{M}$  will be simulated in each of the copies according to the probability in  $\mathcal{M}$ . For every  $q, q' \in Q, a \in \Sigma$ , let  $M'(a)(q_s, q'_s) = M(a)(q, q')$  and  $M'(a)(q_{s'}, q'_{s'}) = M(a)(q, q')$ . A probabilistic automaton should be stochastic for every  $a \in \Sigma$ , so there is unused probability for each character, which will divert to a sink. For every  $q \in Q$  and  $a \in \Sigma$ , let

$$M'(a)(q_s, sink) = 1 - \sum_{q' \in Q} M(a)(q, q')$$

and

$$M'(a)(q_{s'}, sink) = 1 - \sum_{q' \in Q} M(a)(q, q').$$

There will be an additional character \$.

From  $q_0$  the machine will pick either of the two machines with equal probability;  $M(\$)(q_0, s_s) = M(\$)(q_0, s'_{s'}) = \frac{1}{2}$ . If in the accepting or rejecting state the system will stay there forever  $M'(\$)(acc, acc) = 1$  and  $M'(\$)(rej, rej) = 1$ .

The behaviour on \$ will differ in the two copies of  $\mathcal{M}$ . If in an  $s$  state the system will preference the accepting state when accepting and otherwise restart. If in an  $s'$  state the system will preference the rejecting state when accepting and otherwise restart. Formally,

$$M'(\$)(q_s, acc) \text{ when } q_s \in F \text{ and } M'(\$)(q_s, q_0) \text{ when } q_s \notin F$$



and

$$M'(\$)(q_{s'}, rej) \text{ when } q_{s'} \in F \text{ and } M'(\$)(q_{s'}, q_0) \text{ when } q_{s'} \notin F.$$

When in the sink state, the system restarts on \$,  $M'(\$)(sink, q_0) = 1$ , or for all  $a \in \Sigma$  stays there  $M'(a)(sink, sink) = 1$ .

The idea is that if  $f_s(w) \gg f_{s'}(w)$  then, by repeated reading of the word  $w$ , all of the probability mass will eventually move to 'acc'; otherwise a sufficiently large amount of mass will be lost to 'rej'.

Denote by  $\mathbb{P}_{\mathcal{A}}(w)$  the probability of a word  $w$  in the probabilistic automaton, from state  $q_0$ , i.e.  $f_{q_0}(w)$ . However,  $f$  will be used to refer to the probability in the labelled Markov chain  $\mathcal{M}$ . Further the notation  $\mathbb{P}[q \xrightarrow{w} q']$  is used to denote  $(M'(w_1) \times \dots \times M'(w_{|w|}))_{q, q'}$ , i.e. the probability of transitioning from state  $q$  to  $q'$  after reading  $w$  in  $\mathcal{A}$ .

Consider each direction:

► **Case 1** (Not big-O implies VALUE-1). *The proof shows that  $\forall \delta \exists C, i \in \mathbb{N}, w \in \Sigma^*$  such that  $f_s(w) > C f_{s'}(w)$  and  $\mathbb{P}_{\mathcal{A}}((w\$)^i) > 1 - \delta$ .*

*Hence given  $\delta$ , choose  $C$  such that  $(1 - \frac{\delta}{2}) \frac{C}{C+1} > 1 - \delta$ . Then by the big-O property, choose a word such that  $f_s(w) = C' f_{s'}(w)$ , with  $C' > C$ . Then  $(1 - \frac{\delta}{2}) \frac{C'}{C'+1} > (1 - \frac{\delta}{2}) \frac{C}{C+1} > 1 - \delta$ .*

*Given the fixed sequence  $(\$w\$)^i$ , this induces a (unary) Markov chain, represented by the Matrix  $A$ , representing states  $q_0, acc$  and  $rej$  in the three positions respectively:*

$$A = \begin{bmatrix} 0.5(1 - f_s(w)) + 0.5(1 - f_{s'}(w)) & 0.5f_s(w) & 0.5f_{s'}(w) \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

*Then in the long run, starting from state 0, observe:*

$$\begin{bmatrix} 1 & 0 & 0 \end{bmatrix} A^i \xrightarrow{i \rightarrow \infty} \begin{bmatrix} 0 & Cx & x \end{bmatrix} \text{ with } C'x + x = 1$$

*Clearly,  $A^i(0, 1) + A^i(0, 2) + A^i(0, 0) = 1$ , and choose  $i$  such that  $A^i(0, 0) \leq \frac{\delta}{2}$ . Then  $A^i(0, 1) + A^i(0, 2) \geq 1 - \frac{\delta}{2}$ , using the fact that  $A^i(0, 1) = C' A^i(0, 2)$ , obtaining  $A^i(0, 1) + \frac{A^i(0, 1)}{C'} \geq 1 - \frac{\delta}{2}$*

*Hence  $A^i(0, 1) \geq (1 - \frac{\delta}{2}) \frac{C'}{C'+1} > 1 - \delta$ , as required.*

► **Case 2** (big-O implies Not Value-1). *We have there exists  $C$  such that  $\forall w f_s(w) \leq C f_{s'}(w)$  and should show there exists  $\delta > 0$  such that  $\forall w \in (\Sigma \cup \{\$\})^*$  we have  $\mathbb{P}_{\mathcal{A}}(w) \leq 1 - \delta$*

*To move probability from  $q_0$  to acc it is necessary to use words of the form  $\Sigma^* \$$  where  $\Sigma$  is the alphabet of  $\mathcal{M}$ . Hence any word can be decomposed into  $\$w_1 \$w_2 \$ \dots \$w_m \$$ .*

*After reading  $w_1$  the probability is such that*

$$x_1 = \mathbb{P}[q_0 \xrightarrow{\$w_1 \$} acc] = f_s(w_1)$$

$$y_1 = \mathbb{P}[q_0 \xrightarrow{\$w_1 \$} rej] = f_{s'}(w_1)$$

$$\mathbb{P}[q_0 \xrightarrow{\$w_1 \$} q_0] = 1 - x_1 - y_1$$

*Since  $\exists C \forall w_i : f_s(w_i) \leq C f_{s'}(w_i)$ , we have  $x_1 \leq C y_1$ . By induction, repeating this process*

we have for all  $i$ :  $x_i \leq Cy_i$ .

$$x_i = \mathbb{P}[q_0 \xrightarrow{\$w_1\$ \dots \$w_i\$} acc] = (1 - f_s(w_i) - f_{s'}(w_i))x_{i-1} + f_s(w_i)$$

$$y_i = \mathbb{P}[q_0 \xrightarrow{\$w_1\$ \dots \$w_i\$} acc] = (1 - f_s(w_i) - f_{s'}(w_i))y_{i-1} + f_{s'}(w_i)$$

$$\mathbb{P}[q_0 \xrightarrow{\$w_1\$ \dots \$w_i\$} q_0] = \prod_{j=1}^i (1 - x_j + y_j).$$

Hence

$$\begin{aligned} x_i &= (1 - f_s(w_i) - f_{s'}(w_i))x_{i-1} + f_s(w_i) \\ &\leq (1 - f_s(w_i) - f_{s'}(w_i))Cy_{i-1} + Cf_{s'}(w_i) \\ &= C[(1 - f_s(w_i) - f_{s'}(w_i))y_{i-1} + f_{s'}(w_i)] \\ &\leq Cy_i. \end{aligned}$$

In the extreme  $x_m + y_m = 1$ , then  $x_m \leq \frac{C}{C+1} < 1$ , so the probability of reaching *acc* is bounded away from 1 for every word. ◀

The VALUE-1 problem is undecidable in general, however it is decidable in the unary case in **coNP** [4] and for *leaktight automata* [17]. Note, however, that the construction combined with these decidability results *does not* entail any decidability results for the big-O problem. Firstly note that the construction adds an additional character, and such a unary instance of the big-O problem always has at least two characters when translated to the VALUE-1 problem. Further the construction does not result in a leaktight automaton, to see this the definition of leaktight automata are recalled from [17]. The following, does not, of course, preclude the existence of a construction which does maintain these properties.

► **Definition 49.** A finite word  $u$  is *idempotent* if reading once or twice the word  $u$  does not change qualitatively the transition probabilities. That is  $\mathbb{P}_A[q \xrightarrow{u} q'] > 0 \iff \mathbb{P}_A[q \xrightarrow{uu} q'] > 0$ .

Let  $u_n$  be a sequence of idempotent words. Assume that the sequence of matrices  $\mathbb{P}_A(u_n)$  converges to a limit  $M$ , that this limit is idempotent and denote  $M$  the associated Markov chain. The sequence  $u_n$  is a *leak* if there exist  $r, q \in Q$  such that the following three conditions hold:

1.  $r$  and  $q$  are recurrent in  $M$ ,
2.  $\lim \mathbb{P}_A[r \xrightarrow{u_n} q] = 0$ ,
3. for all  $n$ ,  $\mathbb{P}_A[r \xrightarrow{u_n} q] > 0$ .

An automaton is *leaktight* if there is no leak.

If there were no leak in the probabilistic automaton then decidability would follow. However, this is not the case, and the reduction does not solve any cases by reduction to known decidable fragment of the VALUE-1 problem.

▷ **Claim 50.** The resulting automaton from the reduction of the big-O problem to the VALUE-1 problem has a leak.

**Proof.** Consider some infinite sequence of words  $w_i$  growing in length, such that  $f_s(w_i) > 0$  for every  $i$ . Let  $u_i = \$w_i\$$ .

Observe that this word is idempotent. For each starting state, consider the possible states with non-zero probability and from each of these the set of reachable states. Observe that in all cases the set reachable after one application is equal to the set reachable after two.

- $acc \xrightarrow{\$w_i\$} acc \xrightarrow{\$w_i\$} acc$
- $rej \xrightarrow{\$w_i\$} rej \xrightarrow{\$w_i\$} rej$
- $q_0 \xrightarrow{\$w_i\$} q_0, acc, rej \xrightarrow{\$w_i\$} q_0, acc, rej$
- $q_0 \xrightarrow{\$w_i\$} q_0, acc, rej \xrightarrow{\$w_i\$} q_0, acc, rej$
- For  $q$  accepting in  $Q_s$ :  $q \xrightarrow{\$w_i\$} acc \xrightarrow{\$w_i\$} acc$
- For  $q$  rejecting in  $Q_s$ :  $q \xrightarrow{\$w_i\$} \emptyset \xrightarrow{\$w_i\$} \emptyset$
- For  $q$  accepting in  $Q_{s'}$ :  $q \xrightarrow{\$w_i\$} rej \xrightarrow{\$w_i\$} rej$
- For  $q$  rejecting in  $Q_{s'}$ :  $q \xrightarrow{\$w_i\$} \emptyset \xrightarrow{\$w_i\$} \emptyset$

Assume that the labelled Markov chain  $\mathcal{M}$  has a sink, that is the decision to terminate the word must be made by probability. Then  $\forall \lambda > 0$  there exists  $n$  such that  $f_s(\Sigma^{>n}) < \lambda$  and  $f_{s'}(\Sigma^{>n}) < \lambda$  [25, Lemma 12.].

Suppose limit  $\mathbb{P}_{\mathcal{A}}(u_n)$  converges to a limit  $M$  and let  $r = q_0$  and  $q = acc$ .

Hence for longer and longer words the probability of reaching  $acc$  is diminishing. Thus  $\lim \mathbb{P}_{\mathcal{A}}[r \xrightarrow{u_n} q] = 0$ , and in  $M$  we have  $r$  and  $q$  in different SCCs.  $acc$  is clearly recurrent as it is deterministically looping on every character. Since the probability of reaching  $acc$  is diminishing for longer and longer words, whenever  $\$$  is read the state returns to  $r$ , hence all words return to  $r$  with probability 1 in the limit. By the choice of words in the sequence, for every word  $f_s(u_n) > 0$ , we have  $\mathbb{P}_{\mathcal{A}}[r \xrightarrow{u_n} q] > 0$  for all  $n$ .

Hence a leak has been defined, even in the case where  $\mathcal{M}$  is unary. ◀

## E Additional material for Section 4

Here we discuss the relationship between the big-O problem and the eventually big-O problem. Let  $\mathcal{W} = \langle Q, \Sigma, M, \{t\} \rangle$  be a weighted automaton,  $s, s' \in Q$ , and  $s \neq s'$ . Below, whenever we write  $f_s$  (resp.  $f_{s'}$ ), this will refer to word weights from  $s$  (resp.  $s'$ ) in  $\mathcal{W}$ .

Choose  $\delta$  to be a real number such that  $0 < \delta < 1$  and  $\delta$  is smaller than any positive weight in  $\mathcal{W}$ . Construct  $\mathcal{W}'$  by adding the following transitions for all  $x \in \Sigma$ :

$$s' \xrightarrow{x} t \quad s' \xrightarrow{x} \bullet \quad \bullet \xrightarrow{x} \bullet \quad \bullet \xrightarrow{x} t,$$

where  $\bullet$  is a new state. Consequently, for any  $w \in \Sigma^+$ , we get:

- the weight of  $w$  in  $\mathcal{W}'$  from  $s'$  is  $f_{s'}(w) + \delta^{|w|}$ ,
- if  $f_{s'}(w) > 0$  then  $f_{s'}(w) > \delta^{|w|}$ .

► **Lemma 51.**  *$s$  is eventually big-O of  $s'$  in  $\mathcal{W}$  if and only if  $\mathcal{L}_s(\mathcal{W}) \setminus \mathcal{L}_{s'}(\mathcal{W})$  is finite and  $s$  is big-O of  $s'$  in  $\mathcal{W}'$ .*

**Proof.**

( $\Rightarrow$ ) Suppose  $s$  is eventually big-O of  $s'$  in  $\mathcal{W}$ , i.e. there exist  $C, k$  such that, for all  $w \in \Sigma^{\geq k}$ ,  $f_s(w) \leq C f_{s'}(w)$ . Note that, for  $w \in \Sigma^{\geq k}$ , this implies that, whenever  $f_s(w) > 0$ , we must also have  $f_{s'}(w) > 0$ . Consequently,  $\mathcal{L}_s(\mathcal{W}) \setminus \mathcal{L}_{s'}(\mathcal{W}) \subseteq \Sigma^{<k}$ , i.e.  $\mathcal{L}_s(\mathcal{W}) \setminus \mathcal{L}_{s'}(\mathcal{W})$  must be finite.

Let  $w \in \Sigma^*$ ,  $m = \max_{w \in \Sigma^{<k}} f_s(w)$  and  $C' = \frac{m}{\delta^k}$ .

- If  $w \in \Sigma^{\geq k}$ , we have  $f_s(w) \leq C f_{s'}(w) \leq C(f_{s'}(w) + \delta^{|w|})$ .
- If  $w \in \Sigma^{<k}$ , then  $f_s(w) \leq m = \frac{m}{\delta^k} \delta^k = C' \delta^k \leq C' \delta^{|w|} \leq C'(f_{s'}(w) + \delta^{|w|})$ . Note that  $\delta^k \leq \delta^{|w|}$  follows from  $w \in \Sigma^{<k}$  and  $0 < \delta < 1$ .

Taking  $\max(C, C')$  as the relevant constant, we can conclude that  $s$  is big-O of  $s'$  in  $\mathcal{W}'$ .

( $\Leftarrow$ ) Suppose  $\mathcal{L}_s(\mathcal{W}) \setminus \mathcal{L}_{s'}(\mathcal{W})$  is finite and  $s$  is big-O of  $s'$  in  $\mathcal{W}'$ . Because  $\mathcal{L}_s(\mathcal{W}) \setminus \mathcal{L}_{s'}(\mathcal{W})$  is finite, there exists  $k$ , such that, for all  $w \in \Sigma^{\geq k}$ ,  $f_s(w) > 0$  implies  $f_{s'}(w) > 0$ . Because  $s$  is big-O of  $s'$  in  $\mathcal{W}'$ , there exists  $C$ , such that  $f_s(w) \leq C(f_{s'}(w) + \delta^{|w|})$  for any  $w \in \Sigma^*$ . Let  $w \in \Sigma^{\geq k}$ . From  $s$  being big-O of  $s'$ , we get  $f_s(w) \leq C(f_{s'}(w) + \delta^{|w|})$ .

- If  $f_s(w) > 0$  then  $f_{s'}(w) > 0$ . By construction of  $\mathcal{W}'$ , we get  $f_{s'}(w) > \delta^{|w|}$ , so

$$f_s(w) \leq C(f_{s'}(w) + \delta^{|w|}) < C(f_{s'}(w) + f_{s'}(w)) = 2Cf_{s'}(w).$$

- If  $f_s(w) = 0$  then we also have  $f_s(w) = 0 \leq 2Cf_{s'}(w)$ .

Consequently, for any  $w \in \Sigma^{\geq k}$ ,  $f_s(w) \leq 2Cf_{s'}(w)$ , i.e.  $s$  is eventually big-O of  $s'$  in  $\mathcal{W}$ .  $\blacktriangleleft$

The above argument relied on completing the automaton so that any word is accepted with some weight. To transfer our decidability results for bounded languages, it will be necessary to complete the automaton with respect to a bound, i.e. the extra weights are added only for words from  $a_1^+ \cdots a_m^+$ ,  $a_1^* \cdots a_m^*$ ,  $w_1^* \cdots w_k^*$  respectively. This can be done easily by introducing the extra transitions according to DFA for the bounding language.

## E.1 Unambiguous Automata

**Proof of Lemma 13.** Let  $\mathcal{W} = \langle Q, \Sigma, M, F \rangle$  be a weighted automaton. Suppose  $s, s' \in Q$ ,  $t$  is a unique final state, and  $\mathcal{W}$  is unambiguous from  $s, s'$ .

If  $\mathcal{W}$  fails the LC condition (recall that it can be checked in polynomial time), we return no. Otherwise, let us construct a weighted automaton  $\mathcal{W}'$  through a restricted product construction involving two copies of  $\mathcal{W}$ : for all  $q_1, q_2, q'_1, q'_2 \in Q$ , we add edges  $(q_1, q'_1) \xrightarrow{p} (q_2, q'_2)$  provided  $M(a)(q_1, q_2) > 0$ ,  $M(a)(q'_1, q'_2) > 0$  and  $p = \frac{M(a)(q_1, q_2)}{M(a)(q'_1, q'_2)}$ . Note that there exists a positively-weighted  $w$ -labelled path from  $(s, s')$  to  $(t, t)$  in  $\mathcal{W}'$  iff  $w \in \mathcal{L}_s(\mathcal{W}) \cap \mathcal{L}_{s'}(\mathcal{W})$ . By the LC condition, this is equivalent to  $w \in \mathcal{L}_s(\mathcal{W})$ , and, to examine the big-O problem, it suffices to consider only such words.

By unambiguity of  $\mathcal{W}$  from  $s$  and  $s'$ , for any  $w \in \mathcal{L}_s(\mathcal{W})$ , there can be exactly one positively-weighted path from  $(s, s')$  to  $(t, t)$  in  $\mathcal{W}'$ . Consequently, the product of weights along this path is equal to  $f_s(w)/f_{s'}(w)$ . Hence,  $s$  is not big-O of  $s'$  (for  $\mathcal{W}$ ) if and only there exists a positively-weighted path from  $(s, s')$  to  $(t, t)$  in  $\mathcal{W}'$  that contains a cycle such that the product of the weights in that cycle is greater than 1.

Thus, to decide the big-O problem for  $s, s'$ , it suffices to be able to detect such cycles. This can be done, for instance, by a modified version of the Bellman-Ford algorithm [11] applied to the weighted directed graph consisting of positively-weighted edges of  $\mathcal{W}'$ . The algorithm is normally used to find negative cycles in the sense that the sum of weights is negative. To adapt it to our setting, we can apply the logarithm function to the weights. However, to preserve rationality of weights and polynomial-time complexity, we cannot afford to do that explicitly. Instead, whenever  $\log(x) < \log(y)$  would be tested, we test  $x < y$  and, whenever  $\log(x) + \log(y)$  would be performed, we compute  $xy$  instead.  $\blacktriangleleft$

## F Additional material for Section 5

► **Lemma 52.** *Given  $A^\varphi$ , a representation of the value  $\rho_\varphi$  can be found in polynomial time. This representation will admit polynomial time testing of  $\rho_\varphi > \rho_{\varphi'}$  and  $\rho_\varphi = \rho_{\varphi'}$  and can be embedded into the first order theory of the reals.*

**Proof.** An algebraic number  $z$  can be represented as a tuple  $(p_z, a, b, r) \in \mathbb{Q}[x] \times \mathbb{Q}^3$ . Here  $p_z$  is a polynomial over  $x$  and  $a, b, r$  form an approximation such that  $z$  is the only root of  $p_z(x)$  with  $|z - (a + bi)| \leq r$ .

Then operations such as addition and multiplication of two algebraic numbers, finding  $|x|$ , testing if  $x > 0$  can be done in polynomial time in the size of the representation  $(p, a, b, r)$ , yielding the same representation. Additionally given a polynomial, one can find the representation of each of its roots in polynomial time (see e.g. [36]).

Any coefficient of the characteristic polynomial of an *integer* matrix can be found in **GapL** [23]. **GapL** is the difference of two **#L** calls, each of which can be found in  $\text{NC}^2 \subseteq \text{P}$ . Here the matrix will be rational; but it can be normalised to an integer matrix by a scaler, the least common multiple of the denominator of each rational. This number could be exponential, but representable in polynomial space. The final eigenvalues can be renormalised by this constant.

The characteristic polynomial of an  $n \times n$  matrix has degree at most  $n$ , since each coefficient can be found in polynomial time, the whole characteristic polynomial can be found in this time. Thus by enumerating its roots (at most  $n$ ), taking the modulus of each, and sorting them ( $a > b \iff a + -1 \times b > 0$ ) we can find the spectral radius in this form  $(p_z, a, b, r)$ .

Note that the spectral radius is a real number, so that given the spectral radius in the form  $(p_z, a, b, r)$  we actually have  $b = 0$ . Then the number can be encoded exactly in the first order theory of the reals using  $\exists z : p_z(z) = 0 \wedge z - a \leq r \wedge a - z \leq r$ .  $\blacktriangleleft$

**Proof of Lemma 21. (lower bound)** Let  $n \in \mathbb{N}$  and suppose  $d_{s,t}(n) = (\rho', k')$ . Consider the witnessing path in  $\mathcal{W}$ , i.e. the length- $n$  path from  $s$  to  $t$  that visits  $k' + 1$  SCCs of spectral radius  $\rho'$  and no SCC with a larger spectral radius. Let  $\pi = \varphi_1 \dots \varphi_k \in \mathcal{P}(s, t)$  be the corresponding sequence of SCCs visited by that path and let  $s_i, e_i$  ( $1 \leq i \leq k$ ) be the entry and exit points (respectively into and out of  $\varphi_i$ ) on that path. i.e.  $s = s_1$ ,  $\text{SCC}(s_i) = \text{SCC}(e_i) = \varphi_i$  ( $1 \leq i \leq k$ ), there is a transition (of positive weight) from  $e_i$  to  $s_{i+1}$  and  $e_k = t$ . We write  $s_i, \vec{e}_i$  to represent the particular sequence of entry/exit points.

Let us define a new unary weighted automaton  $\mathcal{W}^{s_i, \vec{e}_i}$  to be a restriction of  $\mathcal{W}$  so that the only entry points to its SCCs are  $s_i$ 's and the only exit point are  $e_i$ 's, i.e. the weight is reduced to zero for any violating transition. Let  $D$  be the transition matrix of  $\mathcal{W}^{s_i, \vec{e}_i}$ .

Clearly  $A_{s,t}^n \geq D_{s,t}^n$ , since  $\mathcal{W}^{s_i, \vec{e}_i}$  is a restriction of  $\mathcal{W}$ . Note that, in  $\mathcal{W}^{s_i, \vec{e}_i}$ ,  $\rho(s, t) = \rho'$  and  $k(s, t) = k'$ , because all paths from  $s$  to  $t$  must visit  $k' + 1$  SCC's with spectral radius  $\rho'$ . Hence, by Theorem 18,  $D_{s,t}^n + D_{s,t}^{n+1} + \dots + D_{s,t}^{n+T-1} \geq c_{s_i, \vec{e}_i} (\rho')^n n^{k'}$ , for some  $c_{s_i, \vec{e}_i} > 0$ , where  $T$  is the local period from  $s$  to  $t$  in  $\mathcal{W}^{s_i, \vec{e}_i}$ . Next we shall show that  $D_{s,t}^{n+1} + \dots + D_{s,t}^{n+T-1} = 0$ , which will imply  $D_{s,t}^n \geq c_{s_i, \vec{e}_i} (\rho')^n n^{k'}$  and, hence,  $A_{s,t}^n \geq c_{s_i, \vec{e}_i} (\rho')^n n^{k'}$ .

Let  $L$  be the length of the shortest path from  $s$  to  $t$  in  $\mathcal{W}^{s_i, \vec{e}_i}$ . Observe that paths from  $s$  to  $t$  in  $\mathcal{W}^{s_i, \vec{e}_i}$  can only have lengths from  $\{L + n_1 \cdot T^{\text{SCC}(s_1)} + \dots + n_k \cdot T^{\text{SCC}(s_k)} \mid n_1, \dots, n_k \in \mathbb{N}\}$  and, thus,  $\{L + n \cdot \gcd\{T^{\text{SCC}(s_1)}, \dots, T^{\text{SCC}(s_k)}\} \mid n \in \mathbb{N}\}$ . As  $\mathcal{P}(s, t) = \{\pi\}$  in  $\mathcal{W}^{s_i, \vec{e}_i}$ ,  $T = \gcd\{T^{\text{SCC}(s_1)}, \dots, T^{\text{SCC}(s_k)}\}$ . Consequently, all paths from  $s$  to  $t$  in  $\mathcal{W}^{s_i, \vec{e}_i}$  have lengths of the form  $L + nT$ . Hence, since  $D_{s,t}^n$  is positive, there are no paths which can contribute positive value to  $D_{s,t}^{n+1} + \dots + D_{s,t}^{n+T-1}$ .

As  $c_{s_i, \vec{e}_i}$  depends only on  $s_i, \vec{e}_i$ , to finish the proof it suffices to take  $c$  to be the smallest among the finitely many  $c_{s_i, \vec{e}_i}$ .

**(upper bound)** Let  $N_{(\rho', k')} = \{n \mid d_{s,t}(n) = (\rho', k')\}$ . This gives a finite partition of  $\mathbb{N}$  as  $\bigcup_{(\rho', k')} N_{(\rho', k')}$ . For each  $(\rho', k')$ , we shall find a value  $C_{(\rho', k')}$  so that, for  $n \in N_{(\rho', k')}$ , we have

$A_{s,t}^n \leq C_{(\rho',k')}(\rho')^n n^{k'}$ . Then, to have  $A_{s,t}^n \leq C\rho(n)^n n^{k(n)}$  for all  $n \in \mathbb{N}$ , it will suffice to take  $C$  to be the maximum over all  $C_{(\rho',k')}$ .

Let us fix  $(\rho', k')$ . Consider  $\mathcal{W}^\bullet$  to be  $\mathcal{W}^\dagger$  in which, for every  $(\rho, k) \leq (\rho', k')$ , we merge the states  $(t, \rho, k)$  into a single final state  $t'$  (recall there are no outgoing edges from  $t$ ). Let us rename the state  $(s, 0, 0)$  to  $s'$ . Let  $E$  be the corresponding transition matrix of  $\mathcal{W}^\bullet$ . Note that all paths from  $s'$  to  $t'$  in  $\mathcal{W}^\bullet$  go through at most  $k' + 1$  SCCs with spectral radius  $\rho'$ .

▷ **Claim 53.** For all  $n \in N_{(\rho',k')}$ , we have  $A_{s,t}^n = E_{s',t'}^n$ .

Consider any path  $s \rightarrow q_1 \rightarrow \dots \rightarrow q_m \rightarrow t$  in  $\mathcal{W}$ . There is a corresponding path in  $\mathcal{W}^\bullet$ , however the states  $q_i$  are annotated as  $(q_i, \rho, k)$ , where  $\rho$  is the largest spectral radius seen so far, and  $k + 1$  is the number of SCC's of that radius number seen so far. The only paths removed are those terminating at  $(t, \rho, k)$  with  $(\rho, k) > (\rho', k')$ . Since  $d_{s,t}(n) = (\rho', k')$ , we know that no path visits more than  $k' + 1$  SCCs of spectral radius  $\rho'$ , or an SCC of spectral radius greater than  $\rho'$ . Consequently, no such path is disallowed in  $\mathcal{W}^\bullet$ . No paths were added either. Because every SCC in  $\mathcal{W}$  remains a strongly connected component in  $\mathcal{W}^\bullet$  (duplicated with various  $(\rho, k)$ ) and its transition probability matrix (and hence the spectral radius) remains the same, we can conclude that  $A_{s,t}^n = E_{s',t'}^n$ .

▷ **Claim 54.** There exists  $C_{(\rho',k')}$  such that  $A_{s,t}^n \leq C_{(\rho',k')}(\rho')^n n^{k'}$ .

We have  $A_{s,t}^n = E_{s',t'}^n \leq E_{s',t'}^n + E_{s',t'}^{n+1} + \dots + E_{s',t'}^{n+T(s',t')-1}$ , where  $T(s', t')$  is the local period between states  $s'$  and  $t'$  in  $\mathcal{W}^\bullet$ . By Theorem 18, there exists  $C_{(\rho',k')}$  such that this quantity is bounded by  $C_{(\rho',k')}(\rho')^n n^{k'}$ . Thus, for  $n \in N_{(\rho',k')}$ , we have  $A_{s,t}^n \leq C_{(\rho',k')}(\rho')^n n^{k'}$ . ◀

**Proof of Lemma 23.** First we note some consequences of  $d_{s,t}(n) \leq d_{s',t}(n)$ . Suppose  $d_{s,t}(n) = (\rho, k)$  and  $d_{s',t}(n) = (\rho', k')$ . Thanks to Lemma 21, we have  $f_s(a^n) \leq (\frac{C}{c})(\frac{\rho}{\rho'})^n n^{k-k'}$ . If  $d_{s,t}(n) \leq d_{s',t}(n)$  we can distinguish two cases: either  $(\rho, k) = (\rho', k')$  or  $(\rho, k) < (\rho', k')$ .

- In the former case,  $(\frac{\rho}{\rho'})^n n^{k-k'} = 1$  and, thus,  $f_s(a^n) \leq (\frac{C}{c}) \cdot f_{s'}(a^n)$ .
- In the latter case, we have  $\lim_{m \rightarrow \infty} (\frac{\rho}{\rho'})^m m^{k-k'} = 0$  and, thus,  $(\frac{\rho}{\rho'})^m m^{k-k'} < 1$  for all but finitely many  $m$ . Consequently, for all but finitely many  $n$ , we can conclude  $f_s(a^n) \leq (\frac{C}{c}) \cdot f_{s'}(a^n)$ .

Thanks to the above analysis, if  $d_{s,t}(n) \leq d_{s',t}(n)$  holds for all but finitely many  $n$ , it follows that  $f_s(a^n) \leq (\frac{C}{c}) \cdot f_{s'}(a^n)$  for all but finitely many  $n$ . Moreover, the language containment condition implies that  $f_s(a^n) \leq C' \cdot f_{s'}(a^n)$  for some  $C'$  in the remaining (finitely many) cases. Hence,  $s$  is big-O of  $s'$ , which shows the right-to-left implication.

For the converse, recall that we have already established that “ $s$  is big-O of  $s'$ ” implies the language containment condition. For the remaining part, we reason by contraposition and suppose that there are infinitely many  $n$  with  $d_{s,t}(n) > d_{s',t}(n)$ . As there are finitely many values in the range of  $d_{s,t}$  and  $d_{s',t}$ , there exist  $(\rho, k)$  and  $(\rho', k')$  such that  $(\rho, k) > (\rho', k')$  and, for infinitely many  $n$ ,  $d_{s,t} = (\rho, k)$  and  $d_{s',t} = (\rho', k')$ . For such  $n$ , Lemma 21 yields  $f_s(a^n) \geq (\frac{c}{C})(\frac{\rho}{\rho'})^n n^{k-k'}$ . But  $(\rho, k) > (\rho', k')$  implies

$$\lim_{m \rightarrow \infty} \left( \frac{\rho}{\rho'} \right)^m m^{k-k'} = \infty,$$

i.e.  $(\frac{\rho}{\rho'})^n n^{k-k'}$  is unbounded. Thus,  $s$  cannot be big-O of  $s'$ . ◀



**Proof of Lemma 25.** Let  $M$  be a DFA accepting  $\mathcal{L}(\mathcal{N}_1) \cap \overline{\mathcal{L}(\mathcal{N}_2)}$  obtained through standard automata constructions, i.e.  $|M| \leq 2^{|\mathcal{N}_1|+|\mathcal{N}_2|}$ . Note that  $\mathcal{L}(\mathcal{N}_1) \subsetneq \mathcal{L}(\mathcal{N}_2)$  if and only if  $\mathcal{L}(M)$  is finite. Observe that  $\mathcal{L}(M)$  is infinite if and only if there exists  $w \in \mathcal{L}(M)$  with  $|M| \leq w \leq 2|M|$ .

Consequently, violation of eventual inclusion can be detected by guessing  $n \in \mathbb{N}$  such that  $|M| \leq n \leq 2|M|$  and verifying  $a^n \in \mathcal{L}(M)$ .

Even though  $M$  is of exponential size, it is possible to verify  $a^n \in \mathcal{L}(M)$  in polynomial time. To this end, we use  $\mathcal{N}_1, \mathcal{N}_2$  instead of  $M$  and view their transition functions as matrices. Then one can verify the condition using fast matrix exponentiation (by squaring). Because the binary size of  $n$  must be polynomial in  $|\mathcal{N}_1| + |\mathcal{N}_2|$ , the lemma follows.  $\blacktriangleleft$

**Proof of Lemma 26.** The left-to-right implication is clear. For the opposite direction, observe that, because the order on  $X$  is total,  $d_1(n) > d_2(n)$  implies the existence of  $x \in X$  such that  $d_1(n) \geq x$  and  $d_2(n) < x$  (it suffices to take  $x = d_1(n)$ ). Because  $X$  is finite,  $d_1(n) > d_2(n)$  for infinitely many  $n$  implies failure of  $\{n \mid d_1(n) \geq x\} \subsetneq \{n \mid d_1(n) \geq x\}$  for some  $x$ .  $\blacktriangleleft$

## F.1 Hardness

► **Theorem 55.** *The big-O problem is coNP-hard on unary Markov chains.*

Let us first consider a particular form of unary NFAs.

► **Definition 56.** *A unary NFA  $\mathcal{N} = \langle Q, \rightarrow, q_s, F \rangle$  is in Chrobak normal form [9] if*

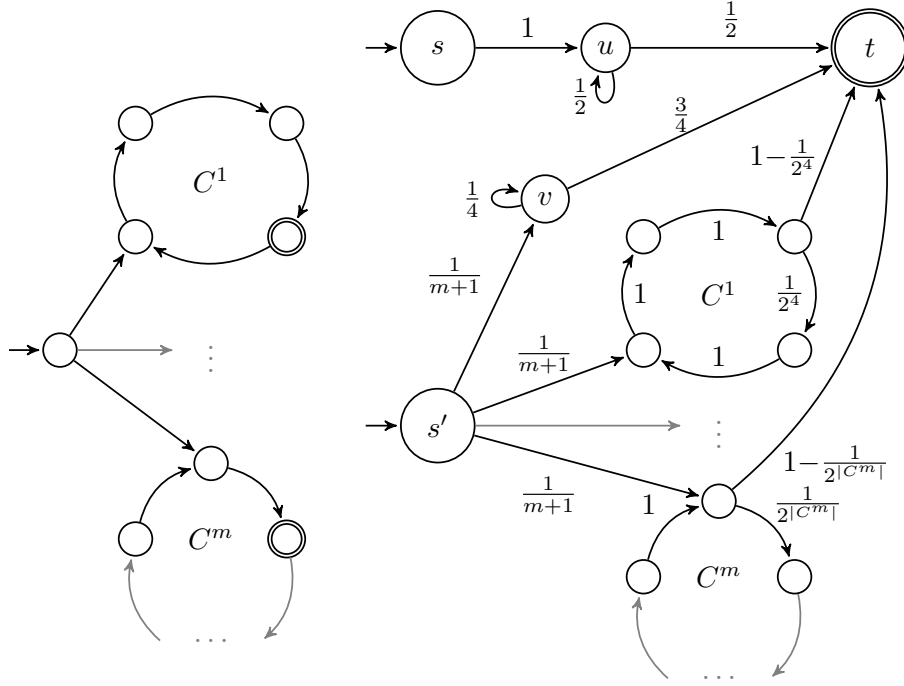
- $Q = S \uplus C^1 \uplus \dots \uplus C^m$  and  $q_s \in S$ ;
- $S = \{s_1, \dots, s_k\}$ ,  $q_s = s_1 \in S$  and transitions between states from  $S$  form a path  $s_1 \xrightarrow{a} s_2 \xrightarrow{a} \dots \xrightarrow{a} s_k$ ;
- $C^i = \{c_0^i, \dots, c_{|C^i|-1}^i\}$  ( $1 \leq i \leq m$ ) and transitions between states from  $C^i$  form a cycle  $c_0^i \xrightarrow{a} c_1^i \xrightarrow{a} \dots \xrightarrow{a} c_{|C^i|-1}^i \xrightarrow{a} c_0^i$ ;
- the remaining transitions connect the end of the path to each cycle:  $s_k \xrightarrow{a} c_0^i$  for all  $1 \leq i \leq m$ .

Any unary NFA can be translated to this representation with at most quadratic blow-up in the size of the machine [9], such representation can be found in polynomial time [45, 32]. In addition, to simplify our arguments, we introduce a *restricted* Chrobak normal form, which requires that there is exactly one accepting state in each cycle. This restricted form can be found with at most a further quadratic blow-up over Chrobak normal form, by creating copies of cycles - one for each accepting state in the cycle.

Observe that  $S \subseteq F$  is a necessary condition for the universality of a unary NFA in Chrobak normal form. Consequently, the universality problem for unary NFA in *restricted Chrobak normal form* such that  $k = 1$  is already coNP-hard. This is the problem we are going to reduce from in the following.

**Proof of Theorem 55.** Let  $\mathcal{N} = \langle Q, \rightarrow, q_s, F \rangle$  be a unary NFA in restricted Chrobak normal form with  $k = 1$ . We will construct a unary Markov chain  $\mathcal{M}$ , depicted in Figure 7, with states  $Q' = Q \cup \{s, u, v, t\}$ , where  $t$  is final. The branch starting from  $s$ , defined below, guarantees  $f_s(a^n) = \Theta((\frac{1}{2})^n)$ .

$$s \xrightarrow{1} u \quad u \xrightarrow{\frac{1}{2}} u \quad u \xrightarrow{\frac{1}{2}} t$$



■ **Figure 7** Reduction from NFA (left) to LMC (right)

We take  $s' = q_s$  and create a similar branch from  $s'$ , albeit with a smaller weight, to create paths of weight  $\Theta((\frac{1}{4})^n)$  when reading  $a^n$ .

$$s' \xrightarrow{\frac{1}{m+1}} v \quad v \xrightarrow{\frac{1}{4}} v \quad v \xrightarrow{\frac{3}{4}} t$$

Moreover, we add weights to the original NFA transitions from  $\mathcal{N}$  as follows:

$$\begin{aligned} s' \xrightarrow{\frac{1}{m+1}} c_0^i \quad (1 \leq i \leq m) \quad & c_{j \ominus 1}^i \xrightarrow{(\frac{1}{2})^{|C^i|}} c_j^i \quad (c_j^i \in F) \\ c_{j \ominus 1}^i \xrightarrow{1 - (\frac{1}{2})^{|C^i|}} t \quad (c_j^i \in F) \quad & c_{j \ominus 1}^i \xrightarrow{1} c_j^i \quad (c_j^i \notin F) \end{aligned}$$

where  $j \ominus 1 = (|C^i| + j - 1) \bmod |C^i|$ . Note that the weights have been selected as if each letter were read with weight  $\frac{1}{2}$  except for a bounded number of transitions, where the bound is  $\max |C^i|$ . Consequently, whenever there are accepting paths for  $a^n$  in  $\mathcal{N}$ , their overall weight in  $\mathcal{M}$  will be  $\Theta((\frac{1}{2})^n)$ .

It is easy to check that the reduction produces an LMC and can be carried out in polynomial time. In Appendix F we show that the reduction is correct. ◀

**Proof of Theorem 55 continued.** It remains to argue that the reduction is correct.

If  $\mathcal{N}$  is not universal, there exists  $n$  such that  $a^n \notin F$ . Because of the cyclic structure of Chrobak normal form,  $a^{n_k} \notin F$  for  $n_k = n + kq$ , where  $q = \text{lcm}\{|C^1|, \dots, |C^m|\}$  and  $k \in \mathbb{N}$ . Then, by the earlier observations about growth, there exists  $C > 0$  such that  $\sup_k \frac{f_s(a^{n_k})}{f_{s'}(a^{n_k})} = \sup_k C \frac{(1/2)^{n_k}}{(1/4)^{n_k}} = \sup_k C 2^{n_k} = \infty$ , i.e.  $s$  is not big-O of  $s'$ .

If  $\mathcal{N}$  is universal then, starting from  $s'$  in  $\mathcal{M}$ , every word  $a^n$  will have a path weighted  $\Theta((\frac{1}{4})^n)$  as well as paths weighted  $\Theta((\frac{1}{2})^n)$ . Hence, there exists  $C > 0$  such that

$$\sup_n \frac{f_s(a^n)}{f_{s'}(a^n)} \leq \sup_n C \frac{(\frac{1}{2})^n}{(\frac{1}{4})^n + (\frac{1}{2})^n} \leq C,$$

i.e.  $s$  is big-O of  $s'$ . ◀

► **Remark 57.** We note that the  $\frac{1}{4}$  branch via state  $v$  is not strictly necessary, but it demonstrates that the problem is hard even if the LC condition is satisfied (i.e., “it can be the numbers that make the hardness”).

## G

 Additional material for Section 6

### G.1 Additional material for Example 29

Let  $p = 0.62$  and then note that

$$\frac{f_s(a^m b^n)}{f_{s'}(a^m b^n)} = \frac{1 \cdot 0.6^m \cdot 0.4 \cdot 0.4^n \cdot 0.6}{0.5 \cdot 0.59^m \cdot 0.41 \cdot 0.39^n \cdot 0.61 + 0.5 \cdot 0.62^m \cdot 0.38 \cdot 0.41^n \cdot 0.59}$$

Let  $m = n = 0$  then  $\frac{f_s(a^m b^n)}{f_{s'}(a^m b^n)} = \frac{1600}{1579}$ . For all larger  $m, n$  the ratio is smaller.

To see that, when when  $p = 0.61$  we have  $\frac{f_s(a^n b^{0.66n})}{f_{s'}(a^n b^{0.66n})} \xrightarrow{n \rightarrow \infty} \infty$ , observe there is a solution to  $x$  with  $0.61 \cdot 0.39^x < 0.6 \cdot 0.4^x$  and  $0.59 \cdot 0.41^x < 0.6 \cdot 0.4^x$ , e.g.  $x = 0.66$ , then let  $m = xn$  and observe Whilst useful for illustration in this example, this effect is not limited to a linear relation between the characters, and so heavier machinery is required.

### G.2 Additional proofs

► **Claim 58.** In the plus-letter-bounded cases, without loss of generality, we assume  $a_i \neq a_j$  (for  $i \neq j$ ).

**Proof of Claim 58.** We show how to reduce the big-O problem in the plus-letter-bounded case to the version of the same problem where  $a_i \neq a_j$  (for  $i \neq j$ ). Suppose, as above,  $\mathcal{L}_{s'}(\mathcal{W}) \subseteq a_1^+ \cdots a_m^+$ . We can assume  $a_i \neq a_{i+1}$  ( $1 \leq i < m$ ) because  $a^+ a^+$  can be replaced with  $a^+$ . If  $\mathcal{W}$  had an  $a$ -labelled transition that can be used in two different blocks  $a_i^+$  and  $a_j^+$  ( $j \geq i + 2$ ) within  $a_1^+ \cdots a_m^+$ , then  $a = a_i = a_j$  and this transition could be used to “skip” the block  $a_{i+1}^+$ , i.e., there would exist a word  $w \in \mathcal{L}_{s'}(\mathcal{W})$  that does not use the  $a_{i+1}^+$  block, contradicting  $\mathcal{L}_{s'}(\mathcal{W}) \subseteq a_1^+ \cdots a_m^+$ . Therefore, every transition can be associated with exactly one block. Define a fresh alphabet  $\Sigma' = \{b_1, \dots, b_m\}$  and relabel each transition associated with the  $i$ th block by  $b_i$ . ◀

**Proof of Lemma 32.**

$$\begin{aligned} f_s(a_1^{n_1} a_2^{n_2} \dots a_m^{n_m}) &= (M(a_1)^{n_1} \times M(a_2)^{n_2} \times \dots \times M(a_m)^{n_m})_{s,t} \\ &= \sum_{q_1 \in Q} M(a_1)_{s,q_1}^{n_1} (\times M(a_2)^{n_2} \times \dots \times M(a_m)^{n_m})_{q_1,t} \\ &\quad \vdots \\ &= \sum_{(q_1, \dots, q_{m-1}) \in Q^{m-1}} M(a_1)_{s,q_1}^{n_1} \times M(a_2)_{q_1,q_2}^{n_2} \times \dots \times M(a_m)_{q_{m-1},t}^{n_m} \end{aligned}$$

By Lemma 21 in the unary case, for each  $M(a_i)_{q_{i-1},q_i}^{n_i}$ , there is a  $(\rho_{q_{i-1},q_i}, k_{q_{i-1},q_i}), c, C$ , such that if  $n_i > |Q|$

$$c \rho_{q_{i-1},q_i}^{n_i} n_i^{k_{q_{i-1},q_i}} \leq M(a_i)_{q_{i-1},q_i}^{n_i} \leq C \rho_{q_{i-1},q_i}^{n_i} n_i^{k_{q_{i-1},q_i}}.$$

Otherwise if  $n_i \leq |Q|$ , since there are at most  $|Q|$  instances it is clear there exists  $c, C$ ,

$$c\delta^{n_i} \leq M(a_i)_{q_{i-1}, q_i}^{n_i} \leq C\delta^{n_i}.$$

Take  $c, C$  so that  $C$  is maximised over all such  $C$  and  $c$  is minimised over all such  $c$ .

$$\begin{aligned} c^{m-1} \sum_{(q_1, \dots, q_{m-1}) \in Q^{m-1}} \rho_{s, q_1}^{n_1} n_1^{k_{s, q_1}} \cdot \dots \cdot \rho_{q_{m-1}, t}^{n_m} n_m^{k_{q_{m-1}, t}} \\ \leq f_s(a_1^{n_1} a_2^{n_2} \dots a_m^{n_m}) \leq \\ C^{m-1} \sum_{(q_1, \dots, q_{m-1}) \in Q^{m-1}} \rho_{s, q_1}^{n_1} n_1^{k_{s, q_1}} \cdot \dots \cdot \rho_{q_{m-1}, t}^{n_m} n_m^{k_{q_{m-1}, t}} \end{aligned} \quad (7)$$

By standard manipulations, any such that if for all  $i$   $(\hat{\rho}_i, \hat{k}_i) \leq (\rho_1, k_1)$ , then

$\hat{\rho}_1^{n_1} n_1^{k_1} \cdot \dots \cdot \hat{\rho}_m^{n_m} n_m^{k_m} + \rho_1^{n_1} n_1^{k_1} \cdot \dots \cdot \rho_m^{n_m} n_m^{k_m} = \Theta(\rho_1^{n_1} n_1^{k_1} \cdot \dots \cdot \rho_m^{n_m} n_m^{k_m})$  and by sufficient modification of  $C, c$ , paths admitting  $(\hat{\rho}_1, \hat{k}_1), \dots, (\hat{\rho}_m, \hat{k}_m)$  can be omitted.

Since the sum is finite, any two sums with the same  $\rho, k$  values can be reduced to a single one, changing  $c, C$  by a factor of two.

The remaining  $(\rho, k)$  paths correspond exactly with  $d_s(n_1, \dots, n_m)$ .  $\blacktriangleleft$

**Proof of Lemma 34.** Let  $\hat{\rho} = (\rho_1, k_1) \dots (\rho_m, k_m)$ . One can construct an automaton  $\mathcal{N}_{\geq \hat{\rho}}^s$  with

$$\mathcal{L}(\mathcal{N}_{\geq \hat{\rho}}^s) = \{a_1^{n_1} \dots a_m^{n_m} \mid \exists \hat{\sigma} \in d_s(n_1, \dots, n_m) \hat{\sigma} \geq \hat{\rho}\}$$

by tracking the current maximum spectral radius seen and the number of different SCCs with this spectral radius. If the only states seen so far have been singletons with no loops (formally having spectral radius 0), the value should be tracked as  $(\delta, 0)$  regardless of how many have been seen.

Passage from states reading  $a_j$  to states reading  $a_{j+1}$  is allowed only if the tracked value is at least  $(\rho_j, k_j)$ , and states should be final if the tracked value of  $a_m$  is at least  $(\rho_m, k_m)$ .

Similarly, one can construct  $\mathcal{N}_{> \hat{\rho}}^s$  with

$$\mathcal{L}(\mathcal{N}_{> \hat{\rho}}^s) = \{a_1^{n_1} \dots a_m^{n_m} \mid \exists \hat{\sigma} \in d_s(n_1, \dots, n_m) \hat{\sigma} > \hat{\rho}\}.$$

The construction is the same as for  $\mathcal{N}_{\geq \hat{\rho}}^s$  except that, in order to accept, we need to be sure that at least one of the ‘at least’ comparisons was strict. This can be achieved by maintaining an extra bit at run time.

Note that  $\mathcal{L}(\mathcal{N}_{\geq \hat{\rho}}^s) \setminus \mathcal{L}(\mathcal{N}_{> \hat{\rho}}^s)$  contains all  $a_1^{n_1} \dots a_m^{n_m}$  such that there exists  $\hat{\sigma} \in d_s(n_1, \dots, n_m)$  with  $\hat{\sigma} \geq \hat{\rho}$  and, for all  $\hat{\tau} \in d_s(n_1, \dots, n_m)$ , we do *not* have  $\hat{\tau} > \hat{\rho}$ . Consequently, we must have  $\hat{\rho} \in d_s(n_1, \dots, n_m)$ , which implies (by maximality) that we cannot have  $\hat{\tau} > \hat{\rho}$  for any  $\hat{\sigma} \in d_s(n_1, \dots, n_m)$ . Hence,

$$\mathcal{L}(\mathcal{N}_{\geq \hat{\rho}}^s) \setminus \mathcal{L}(\mathcal{N}_{> \hat{\rho}}^s) = \{a_1^{n_1} \dots a_m^{n_m} \mid \hat{\rho} \in d_s(n_1, \dots, n_m)\}.$$

Consequently, we can take  $\mathcal{N}_{\hat{\rho}}^s$  to be the corresponding automaton.

Given  $\mathcal{Y} \subseteq \mathcal{D}$ , we can then take  $\mathcal{N}_{\mathcal{Y}}^s$  to be the automaton corresponding to

$$\bigcap_{\hat{\rho} \in \mathcal{Y}} \mathcal{L}(\mathcal{N}_{\hat{\rho}}^s) \cap \bigcap_{\hat{\rho} \in \mathcal{D} \setminus \mathcal{Y}} (a_1^+ \dots a_m^+ \setminus \mathcal{L}(\mathcal{N}_{\hat{\rho}}^s)).$$

The relevant automaton  $\mathcal{N}_{X, \mathcal{Y}}$  is then found by taking the intersection of  $\mathcal{L}(\mathcal{N}_X^s)$  and  $\mathcal{L}(\mathcal{N}_{\mathcal{Y}}^s)$ .  $\blacktriangleleft$

**Proof of Lemma 35.** Consider the machine  $\mathcal{N}_{X,Y}$ , accepting a language which is a subset of  $a_1^+ a_2^+ \dots a_m^+$ , with any state not reachable from the starting state or not leading to an accepting state removed. To induce a form with the property we want, we intersect  $\mathcal{N}_{X,Y}$  with the standard DFA<sup>3</sup> for  $a_1^+ a_2^+ \dots a_m^+$ , without changing the language.

Hence every state corresponds to reading from exactly one character block of  $a_1, a_2, \dots, a_m$ . At each state there can be at most two characters enabled, either the character to remain in the current character block, or the character to move to the next. Every state can be labelled as

- *only having transition for  $a_i$ ; or*
- *also having transition with  $a_{i+1}$ .*

Consider all possible choices of automaton formed by restricting  $\mathcal{N}_{X,Y}$  so that there is a single state which is allowed to transition from  $a_i$  to  $a_{i+1}$  for each  $i$  and any other state which had this property in  $\mathcal{N}_{X,Y}$  has its  $a_{i+1}$  transitions removed (but keeps its  $a_i$  transitions). Each such choice corresponds with a partition of the accepting runs of  $\mathcal{N}_{X,Y}$ .

Thus  $\mathcal{L}(\mathcal{N}_{X,Y})$  is the finite union over the languages induced by all such machines. We further show that such machines can further be expressed as a finite union of linear sets in the form prescribed.

Let us assume  $\mathcal{N}_{X,Y}^j$  is such a machine with a single state capable of transitioning from  $a_i$  to  $a_{i+1}$  for each  $i$ , and again remove any state not reachable from the starting state or not leading to an accepting state. The part of the machine reading  $a_i$  has a single starting state and a single final state, which is a unary NFA when the transitions to  $a_{i+1}$  are discarded.

This unary NFA can be converted to Chrobak normal form; the section of  $\mathcal{N}_{X,Y}^j$  corresponding to  $a_i$  can be replaced with this unary NFA, and any accepting state has additionally the transitions for transitioning from  $a_i$  to  $a_{i+1}$  of the single such state in  $\mathcal{N}_{X,Y}^j$ .

Let us repeat the process above for all  $i$ , decomposing  $\mathcal{N}_{X,Y}^j$  into the subsets of languages where there are exactly one state transitioning from  $a_i$  to  $a_{i+1}$ . Let  $\mathcal{N}_{X,Y}^j = \bigcup_k \mathcal{N}_{X,Y}^{j,k}$ , a finite union; where each  $k$  corresponds to a selection of accepting states  $(q_1, \dots, q_m)$  with  $q_l$  being the accepting state in the Chrobak normal form for  $a_l$ .

Consider such an  $\mathcal{N}_{X,Y}^{j,k}$ . The steps spent in each block corresponding to  $a_i$  is either formed by the finite path or the a single cycle at the end of the path. If the transition occurs in the finite path then  $b_{ki}$  is the length of the path to that transition and  $r_{ki}$  is zero. If the transition occurs in the cycle at the end of the path, then  $b_{ki}$  is the length of the path to that transition from the start of the path and  $r_{ki}$  is the length of the cycle. In  $\mathcal{N}_{X,Y}^{j,k}$  the time spent in block  $a_i$  has no influence on the time spent in  $a_j$  for  $j \neq i$ . Then  $\mathcal{L}(\mathcal{N}_{X,Y}^{j,k}) = \{a^{n_1} a^{n_2} \dots a^{n_m} \mid \exists \vec{\lambda} \in \mathbb{N}^m \text{ s.t. } \forall i \in [m] n_i = b_{ki} + r_{ki} \cdot \lambda_i\}$ . The language  $\mathcal{L}(\mathcal{N}_{X,Y})$  is the union over all  $\mathcal{L}(\mathcal{N}_{X,Y}^{j,k})$ . ◀

**Proof of Lemma 37.** By Lemma 36 we have  $s$  is not big-O of  $s'$  if and only if there exist  $X \in \mathcal{D}$ ,  $\mathcal{Y} \subseteq \mathcal{D}$ ,  $1 \leq k \leq S_{X,Y}$  such that

$$\forall C \exists \vec{\lambda} \in \mathbb{N}^m \bigwedge_{j \in h_Y} \sum_{i=1}^m \alpha_{j,i} (b_{ki} + r_{ki} \lambda_i) + p_{j,i} \log(b_{ki} + r_{ki} \lambda_i) < C. \quad (8)$$

First we argue that we can restrict to some subset of the components which enable the satisfying choice of  $\lambda$  to be sufficiently large in all components.

<sup>3</sup> By DFA we permit a partial transition function, that is 0 or 1 transition for each character from every state, rather than exactly 1.

▷ **Claim 59.** Equation (8) holds if and only if the following holds for some  $U \subseteq [m]$ :

$$\forall C \exists \vec{\lambda} \in \mathbb{N}_{\geq \max_i b_{ki}}^U \quad \bigwedge_{j \in h_Y} \sum_{i \in U} \alpha_{j,i} \cdot (b_{ki} + r_{ki} \cdot \lambda_i) + p_{j,i} \log(b_{ki} + r_{ki} \cdot \lambda_i) < C \quad (9)$$

Proof of Claim 59. First note that Equation (9) immediately implies Equation (8). We show the converse.

Recall we can alternatively characterise the formulation as a sequence  $n : \mathbb{N} \rightarrow \mathbb{N}^m$ . That is, for each negative integer  $C$ , the choice of  $\vec{\lambda}$  corresponds to  $n(C)$  in the sequence.

Note that in the sequence  $n$  some components may be bounded. Either because  $r_{ki} = 0$ , or the choice of  $n$  makes it so. Suppose there exists a  $\theta > 0$  such that  $n(t)_x \leq \theta$  for some  $x \in [m]$ , then  $\sum_{i=1}^m \alpha_{j,i} \cdot n(t)_i + p_{j,i} \log(n(t)_i) \leq \sum_{i=1, i \neq x}^m \alpha_{j,i} \cdot n(t)_i + p_{j,i} \log(n(t)_i) + |\alpha_{j,x}| \cdot \theta + |p_{j,x}| \theta$ . Hence the sequence  $\sum_{i=1, i \neq x}^m \alpha_{j,i} \cdot n(t)_i + p_{j,i} \log(n(t)_i)$  goes to  $-\infty$  as well.

Consider each choice of components  $B \subseteq [m]$  which will be bounded. For some components there will be no choice as  $r_{ki} = 0$ . Let us assume that the chosen set is maximal with respect to set-inclusion; that is, there should be no subsequence maintaining the property with fewer components unbounded. Let the remaining unbounded components be  $U = [m] \setminus B$ .

Since each remaining component is not bounded, there is always a later point in the sequence in which the value is larger; thus one can take a subsequence of  $n(t)$  so that  $n(t)_i \leq n(t+1)_i$  for every  $t$ . Repeat for every remaining component  $i \in U$ ; this can be done as the minimal choice of unbounded components has been selected. Hence, without loss of generality if there exists some sequence, then for any  $\theta$ , there exists a subsequence of  $n(t)$ , such that  $n(t)_i > \theta$  for all  $i \in U$ . To enable a more succinct analysis later, restrict  $n(t)$  to those in which  $\lambda_i \geq \max_i b_{ki}$  where  $n(t)_i = b_{ki} + r_{ki} \cdot \lambda_i$  for some  $\lambda_i$ .  $\triangleleft$

Next we argue that the offset component  $\vec{b}$  does not affect whether the formula holds and that we can relax the restriction of  $\vec{\lambda}$  from naturals to positive reals and maintain the satisfiability of the formula. The advantage here is that this relaxation can be solved with the first order theory of the reals with exponential function; which is decidable subject to Schanuel's conjecture.

▷ **Claim 60.**

$$\forall C \exists \vec{\lambda} \in \mathbb{N}_{\geq \max_i b_{ki}}^U \quad \bigwedge_{j \in h_Y} \sum_{i \in U} \alpha_{j,i} \cdot (b_{ki} + r_{ki} \cdot \lambda_i) + p_{j,i} \log(b_{ki} + r_{ki} \cdot \lambda_i) < C \quad (10)$$

holds if and only if the following holds:

$$\forall C \exists \vec{x} \in \mathbb{R}_{\geq \max_i b_{ki}}^U \quad \bigwedge_{j \in h_Y} \sum_{i \in U} \alpha_{j,i} \cdot r_{ki} \cdot x_i + \sum_{i \in U} p_{j,i} \log(x_i) < C \quad (11)$$

Proof of Claim 60. Observe that

$$\sum_{i \in U} \alpha_{j,i} \cdot (b_{ki} + r_{ki} \cdot \lambda_i) = \sum_{i \in U} \alpha_{j,i} \cdot b_{ki} + \sum_{i \in U} \alpha_{j,i} \cdot r_{ki} \cdot \lambda_i$$

and that  $\sum_{i \in U} \alpha_{j,i} \cdot b_{ki}$  is constant so it does not affect whether the sequence goes to  $-\infty$ , hence Equation (10) holds if and only if :

$$\forall C \exists \vec{\lambda} \in \mathbb{N}_{\geq \max_i b_{ki}}^U \quad \bigwedge_{j \in h_Y} \sum_{i \in U} \alpha_{j,i} \cdot r_{ki} \cdot \lambda_i + p_{j,i} \log(b_{ki} + r_{ki} \cdot \lambda_i) < C \quad (12)$$

Now let us extract the log component by using the following rewriting

$$\log(b_{ki} + r_{ki} \cdot \lambda_i) = \log(\lambda_i \cdot (\frac{b_{ki}}{\lambda_i} + r_{ki})) = \log(\lambda_i) + \log(\frac{b_{ki}}{\lambda_i} + r_{ki}).$$

Since  $r_{ki} \geq 1$  and  $\lambda_i \geq b_{ki}$  we have  $\log(\frac{b_{ki}}{\lambda_i} + r_{ki}) \leq \log(r_{ki} + 1)$ , which is constant. Hence Equation (10) is equivalent to:

$$\forall C' \exists \vec{\lambda} \in \mathbb{N}_{\geq \max_i b_{ki}}^U \quad \bigwedge_{j \in h_Y} \sum_{i \in U} \alpha_{j,i} \cdot r_{ki} \cdot \lambda_i + \sum_{i \in U} p_{j,i} \log(\lambda_i) < C' \quad (13)$$

We now show that this is equivalent to Equation (11). Clearly Equation (13) implies Equation (11). Now consider Equation (11) holding, and we show the Equation (13) is satisfied, by exhibiting a choice of  $\vec{\lambda} \in \mathbb{N}_{\geq \max_i b_{ki}}^U$  for every  $C'$ .

Given  $C' < 0$ , let  $C = C' - \max_j \sum_{i \in U} |\alpha_{j,i}| r_{ki} - \max_j \sum_{i \in U} |p_{j,i}|$ , and choose  $\vec{x} \in \mathbb{R}_{\geq \max_i b_{ki}}^{|U|}$  satisfying Equation (11).

Now let  $x_i = \lambda_i + y_i$ , with  $y_i < 1$ ,  $\lambda_i = \lfloor x_i \rfloor$ . First observe that since  $x_i \geq \max_i b_{ki}$ , an integer, also  $\lambda_i \geq \max_i b_{ki}$ .

Observe that  $|\sum_{i \in U} \alpha_{j,i} \cdot r_{ki} \cdot y_i| \leq \sum_{i \in U} |\alpha_{j,i}| r_{ki}$ . Since

$$\sum_{i \in U} \alpha_{j,i} \cdot r_{ki} \cdot \lambda_i + \sum_{i \in U} \alpha_{j,i} \cdot r_{ki} \cdot y_i + \sum_{i \in U} p_{j,i} \log(\lambda_i + y_i) < C$$

we have

$$\sum_{i \in U} \alpha_{j,i} \cdot r_{ki} \cdot \lambda_i + \sum_{i \in U} p_{j,i} \log(\lambda_i + y_i) < C + \sum_{i \in U} |\alpha_{j,i}| r_{ki}$$

Let us again rewrite  $\log(\lambda_i + y_i) = \log(\lambda_i(1 + \frac{y_i}{\lambda_i})) = \log(\lambda_i) + \log(1 + \frac{y_i}{\lambda_i})$ . Then since  $\lambda_i > y_i$ ,  $\log(1 + \frac{y_i}{\lambda_i}) \leq 1$ , so

$$|\sum_{i \in U} p_{j,i} \log(1 + \frac{y_i}{\lambda_i})| \leq \sum_{i \in U} |p_{j,i}|.$$

We thus have

$$\sum_{i \in U} \alpha_{j,i} \cdot r_{ki} \cdot \lambda_i + \sum_{i \in U} p_{j,i} \log(\lambda_i) < C + \sum_{i \in U} |\alpha_{j,i}| r_{ki} + \sum_{i \in U} |p_{j,i}| \leq C'$$

and hence, Equation (13) holds. ◁

◀



### G.3 The bounded case

**Proof of Lemma 40.** Let  $\mathcal{W} = \langle Q, \Sigma, M, F \rangle$ . Then we have  $w_1, \dots, w_m$  such that for all  $w$  with  $f_s(w) > 0$ ,  $w = w_1^{n_1} \dots w_m^{n_m}$  for some  $n_1, \dots, n_m \in \mathbb{N}$ . Let us assume  $w_i = b_{i,1}b_{i,2}, \dots, b_{i,|w_i|}$ .

Given a word  $w$ , there may be multiple paths  $\pi_1, \pi_2, \dots$  from  $s$  to  $t$  respecting that word. Further there may be multiple decomposition vectors  $\vec{n}_1, \vec{n}_2, \dots \in \mathbb{N}^m$  such that  $\vec{n}_i = (n_1, \dots, n_m)$  and  $w = w_1^{n_1} \dots w_m^{n_m}$ . Our goal will be to construct a weighted automaton  $\mathcal{W}'$  with states  $\hat{s}$  and  $\hat{s}'$  letter-bounded over  $a_1^* \dots a_m^*$  such that, for every word  $w$ , the weight of  $a_1^{n_1} \dots a_m^{n_m}$  in  $\mathcal{W}'$  from  $\hat{s}$  (resp.  $\hat{s}'$ ), for every valid decomposition vector  $\vec{n} \in \mathbb{N}^m$  of  $w$ , will be the sum of the weights of all paths  $\pi_1, \pi_2, \dots$  respecting  $w$  in  $\mathcal{W}$  from  $s$  (resp.  $s'$ ). To compute  $\mathcal{W}'$ , we will define a transducer and apply it to our automaton  $\mathcal{W}$ .

A nondeterministic finite transducer is an NFA with transitions labelled by pairs from  $\Sigma \times (\Sigma' \cup \{\epsilon\})$ . In our construction, we only require edges of this form, i.e. we do not consider a definition with transitions labelled with  $\epsilon$  in the first component (e.g.  $\epsilon/a$ ). Our transducer induces a translation  $\mathcal{T} : \Sigma^* \rightarrow \Sigma'^*$ .

Consider the set of regular expressions  $w_{i_1}^+ \dots w_{i_{m'}}^+$ , each induced by a sequence  $\vec{i} = (i_1, \dots, i_{m'}) \in \mathbb{N}^{m'}$ ,  $m' \leq m$ , with  $1 \leq i_1 < \dots < i_{m'} \leq m$ . Note that two sequences  $(i'_1, \dots, i'_{m'}), (i''_1, \dots, i''_{m'})$  may yield the same expression  $w_{i_1}^+ \dots w_{i_{m'}}^+$ , in which case we need not consider more than one. The transducer  $\mathcal{T}$  will be defined as follows.

For each  $\vec{i} = (i_1, \dots, i_{m'})$  described above, build the following automaton. For each  $i_j$ , construct the following section, which simply reads the word  $w_{i_j}$ :

$$f_j^{\vec{i}} \xrightarrow{b_{i_j,1}/\epsilon} s_j^{\vec{i}} \xrightarrow{b_{i_j,2}/\epsilon} \dots \xrightarrow{b_{i_j,|w_{i_j}|-1}/\epsilon} e_j^{\vec{i}}.$$

Then, on the final character, nondeterministically restart or move to the next word, emitting a character representing the word:

$$e_j^{\vec{i}} \xrightarrow{b_{i_j,|w_{i_j}|}/a_{i_j}} f_j^{\vec{i}} \quad \text{and} \quad e_j^{\vec{i}} \xrightarrow{b_{i_j,|w_{i_j}|}/a_{i_j}} f_{j+1}^{\vec{i}}$$

The transducer  $\mathcal{T}$  is defined by the union of the above transitions over all  $\vec{i}$ . We also add a global start state  $q_0$ , from which we would like to move nondeterministically to  $f_1^{\vec{i}}$  for each  $\vec{i}$ . To achieve this and avoid  $\epsilon$  transitions, we duplicate the transitions  $f_1^{\vec{i}} \xrightarrow{x} s_1^{\vec{i}}$  with  $q_0 \xrightarrow{x} s_1^{\vec{i}}$ . Observe that the valid output sequences are  $(\epsilon^* a_1)^* (\epsilon^* a_2)^* \dots (\epsilon^* a_m)^*$ . However, there can be a finite number of  $\epsilon$ 's in a row, at most  $r = \max_{1 \leq i \leq m} |w_i| - 1$ .

Assume  $\mathcal{W} = \langle Q, \Sigma, M, \{t\} \rangle$  and  $\mathcal{T} = \langle Q', \Sigma \times (\Sigma' \cup \{\epsilon\}), \rightarrow, q_0 \rangle$ . Then construct the weighted automaton  $\mathcal{T}(\mathcal{W}) = \langle Q \times Q', \Sigma', M^{\mathcal{T}}, \{t\} \times Q' \rangle$  using a product construction. The probability is associated in the following way  $M^{\mathcal{T}}(a)((s, q), (s', q')) = p$  if there is a transition  $q \xrightarrow{b/a} q'$  in  $\mathcal{T}$  and  $s \xrightarrow{b} s'$  in  $\mathcal{W}$ . Note that, by this definition, there is a matrix  $M^{\mathcal{T}}(\epsilon)$ ; however, in every run of  $\mathcal{T}(\mathcal{W})$  at most  $r$  many  $\epsilon$ 's in a row are produced, where  $r = \max_{1 \leq i \leq m} |w_i| - 1$ .

Now let  $\mathcal{W}'$  be a copy of  $\mathcal{T}(\mathcal{W})$  with  $\epsilon$  removed:  $M'(a_i) = (\sum_{x=0}^r M^{\mathcal{T}}(\epsilon)^x) M^{\mathcal{T}}(a^i)$ . Then  $f_{\mathcal{W}'}(w) = f_{\mathcal{W}'}(a_1^{n_1} \dots a_m^{n_m})$  for all  $n_1, \dots, n_m$  such that  $w = w_1^{n_1} \dots w_m^{n_m}$ . Hence,  $\mathcal{W}'$  is a weighted automaton with letter-bounded languages from  $(s, q_0)$  and  $(s', q_0)$  such that  $(s, q_0)$  is big-O of  $(s', q_0)$  in  $\mathcal{W}'$  if and only if  $s$  is big-O of  $s'$  in  $\mathcal{W}$ . ◀