Selective Monitoring

Radu Grigore[1] and Stefan Kiefer[2]

[1] University of Kent, UK
[2] University of Oxford, UK

Abstract. We study selective monitors for labelled Markov chains. Monitors observe the outputs that are generated by a Markov chain during its run. A monitor is selective if it skips observations in order to reduce monitoring overhead. We are interested in monitors that minimize the expected number of observations. We establish several hardness and undecidability results for selectively monitoring general Markov chains. On the other hand, we show for non-hidden Markov chains (where any output identifies the state the Markov chain is in) that simple optimal monitors exist and can be computed efficiently, based on DFA language equivalence. These monitors do not depend on the precise transition probabilities in the Markov chain. We report on experiments where we compute these monitors for several open-source Java projects.

Keywords: runtime monitoring, probabilistic systems, Markov chains, automata, language equivalence

1 Introduction

An MC (Markov chain) emits letters that are fed into a DFA (deterministic finite automaton). If some letters are lost on the way from the MC to the DFA, then one can compute the probability that the MC emitted a word that is accepted by the DFA. This problem is known as *RVSE (runtime verification with state estimation)* [12,8]. RVSE is motivated by the possibility that messages from a program to its monitor may be lost, which may happen in distributed systems. Here, we are motivated by efficiency. Suppose that the program and its monitor run on the same computer. In such a situation, messages will not get lost en-route, but sending many messages deteriorates performance. The *selective monitoring* problem is to find an observation policy which minimizes the expected number of messages to be sent, while still allowing the monitor to decide whether a run is good or bad.

Previous Work. Before worrying about the performance of a monitor, one might want to check if faults in a given system can be diagnosed at all. This problem has been studied under the term *diagnosability*, first for non-stochastic finite discrete event systems [11], which are labelled transition systems. It was shown in [7] that diagnosability can be checked in polynomial time, although the associated monitors may have exponential size. Later the notion of diagnosability was extended to stochastic discrete-event systems, which are labelled Markov chains [13]. Several notions of diagnosability in stochastic systems exist, and some of them have several names. Bertrand et al. [2] study the relations between them. For instance, they show that for one variant of the problem (referred to as A-diagnosability or SS-diagnosability or IF-diagnosability) a previously proposed polynomial-time algorithm is incorrect, and prove that this notion of diagnosability is PSPACE-complete. Indeed, most variants of diagnosability for stochastic systems are PSPACE-complete [2], with the notable exception of AA-diagnosability (where the monitor is allowed to diagnose wrongly with arbitrarily small probability), which can be solved in polynomial time [3].

Selective Monitoring. In this paper, we seem to make the problem harder: since observations by a monitor come with a performance overhead, we allow the monitor to skip observations. In order to decide how many observations to skip, the monitor employs an *observation policy.* In the following we often equate a monitor with its observation policy. Skipping observations might decrease the probability of deciding (whether the current run of the system is faulty or correct). We do not study this tradeoff: we require policies to be *feasible*, i.e., the probability of deciding must be as high as under the policy that observes everything. We do not require the system to be diagnosable; i.e., the probability of deciding may be less than 1. Checking whether the system is diagnosable is PSPACE-complete ([2], Theorem 8).

The Cost of Decision in General Markov Chains. The *cost* (of decision) is the number of observations that the policy makes during a run of the system We are interested in minimizing the expected cost among all feasible policies. We show that if the system is diagnosable then then there exists a policy with finite expected cost, i.e., the policy may stop observing after finite expected time. (The converse is not true.) Whether the infimum cost (among feasible policies) is finite is also PSPACE-complete (Theorem 14). Whether there is a feasible policy whose expected cost is smaller than a given threshold is undecidable (Theorem 15), even for diagnosable systems.

Non-Hidden Markov Chains. We identify a class of MCs, namely non-hidden MCs, where the picture is much brighter. An MC is called *non-hidden* when each label identifies the state. Non-hidden MCs are always diagnosable. Moreover, we show that *maximally procrastinating* policies are (almost) optimal (Theorem 27). A policy is called maximally procrastinating when it skips observations up to the point where one further skip would put a decision on the current run in question. We also show that one can construct an (almost) optimal maximally procrastinating policy in polynomial time. This policy *does not depend* on the exact probabilities in the MC, although the expected cost under that policy does. That is, we can efficiently construct a policy that is (almost) optimal regardless of the transition probabilities on the MC transitions. We also show that the infimum cost (among all feasible policies) can be computed in polynomial time

(Theorem 28). Underlying these results is a rich, non-obvious theory, which involves checking language equivalence of DFAs.

Experiments. We evaluated the algorithms presented in this paper by implementing them in Facebook Infer, and trying them on 11 of the most forked Java projects on GitHub. We found that, on average, selective monitoring can reduce the number of observations to a half.

2 Preliminaries

Let S be a finite set. We view elements of $\mathbb{R}^S$ as *vectors*, more specifically as row vectors. We write $\mathbf{1}$ for the all-1 vector, i.e., the element of $\{1\}^S$. For a vector $\mu \in \mathbb{R}^S$, we denote by μ^T its transpose, a column vector. A vector $\mu \in [0,1]^S$ is a *distribution over* S if $\mu \mathbf{1}^\mathsf{T} = 1$. For $s \in S$ we write e_s for the (*Dirac*) distribution over S with $e_s(s) = 1$ and $e_s(t) = 0$ for $t \in S \setminus \{s\}$. We view elements of $\mathbb{R}^{S \times S}$ as *matrices*. A matrix $M \in [0,1]^{S \times S}$ is called *stochastic* if each row sums up to one, i.e., $M \mathbf{1}^\mathsf{T} = \mathbf{1}^\mathsf{T}$.

For a finite alphabet Σ, we write Σ^* and Σ^ω for the finite and infinite words over Σ, respectively. We write ε for the empty word. We represent languages $L \subseteq \Sigma^\omega$ using deterministic finite automata, and we represent probability measures $\Pr$ over Σ^ω using Markov chains.

A (discrete-time, finite-state, labelled) *Markov chain (MC)* is a quadruple (S, Σ, M, s_0) where S is a finite set of states, Σ a finite alphabet, s_0 an initial state, and $M : \Sigma \to [0,1]^{S \times S}$ specifies the transitions, such that $\sum_{a \in \Sigma} M(a)$ is a stochastic matrix. Intuitively, if the MC is in state s, then with probability $M(a)(s, s')$ it emits a and moves to state s'. For the complexity results in this paper, we assume that all numbers in the matrices $M(a)$ for $a \in \Sigma$ are rationals given as fractions of integers represented in binary. We extend M to the mapping $M : \Sigma^* \to [0,1]^{S \times S}$ with $M(a_1 \cdots a_k) = M(a_1) \cdots M(a_k)$ for $a_1, \ldots, a_k \in \Sigma$. Intuitively, if the MC is in state s then with probability $M(u)(s, s')$ it emits the word $u \in \Sigma^*$ and moves (in $|u|$ steps) to state s'. An MC is called *non-hidden* if for each $a \in \Sigma$ all non-zero entries of $M(a)$ are in the same column. Intuitively, in a non-hidden MC, the emitted letter identifies the next state. An MC (S, Σ, M, s_0) defines the standard probability measure $\Pr$ over Σ^ω, uniquely defined by assigning probabilities to cylinder sets $\{u\}\Sigma^\omega$, with $u \in \Sigma^*$, as follows:

$$\Pr(\{u\}\Sigma^\omega) \;:=\; e_{s_0} M(u) \mathbf{1}^\mathsf{T}$$

A *deterministic finite automaton (DFA)* is a quintuple $(Q, \Sigma, \delta, q_0, F)$ where Q is a finite set of states, Σ a finite alphabet, $\delta : Q \times \Sigma \to Q$ a transition function, q_0 an initial state, and $F \subseteq Q$ a set of accepting states. We extend δ to $\delta : Q \times \Sigma^* \to Q$ as usual. A DFA defines a language $L \subseteq \Sigma^\omega$ as follows:

$$L \;:=\; \{\, w \in \Sigma^\omega \mid \delta(q_0, u) \in F \text{ for some prefix } u \text{ of } w \,\}$$

Note that we do not require accepting states to be visited infinitely often: just once suffices. Therefore we can and will assume without loss of generality that there is f with $F = \{f\}$ and $\delta(f, a) = f$ for all $a \in \Sigma$.

For the rest of the paper we fix an MC $\mathcal{M} = (S, \Sigma, M, s_0)$ and a DFA $\mathcal{A} = (Q, \Sigma, \delta, q_0, F)$. We define their composition as the MC $\mathcal{M} \times \mathcal{A} := (S \times Q, \Sigma, M', (s_0, q_0))$ where $M'(a)((s, q), (s', q'))$ equals $M(a)(s, s')$ if $q' = \delta(q, a)$ and 0 otherwise. Thus, $\mathcal{M}$ and $\mathcal{M} \times \mathcal{A}$ induce the same probability measure Pr.

An *observation* $o \in \Sigma_\bot$ is either a letter or the special symbol $\bot \notin \Sigma$, which stands for 'not seen'. An *observation policy* $\rho : \Sigma_\bot^* \to \{0, 1\}$ is a function that, given the observations made so far, says whether we should observe the next letter. An observation policy ρ determines a projection $\pi_\rho : \Sigma^\omega \to \Sigma_\bot^\omega$: we have $\pi_\rho(a_1 a_2 \dots) = o_1 o_2 \dots$ when

$$o_{n+1} \;=\; \begin{cases} a_{n+1} & \text{if } \rho(o_1 \dots o_n) = 1 \\ \bot & \text{if } \rho(o_1 \dots o_n) = 0 \end{cases} \qquad\qquad \text{for all } n \geq 0$$

We denote the *see-all policy* by $\bullet$; thus, $\pi_\bullet(w) = w$.

In the rest of the paper we reserve a for letters, o for observations, u for finite words, w for infinite words, υ for finite observation prefixes, s for states from an MC, and q for states from a DFA. We write $o_1 \sim o_2$ when o_1 and o_2 are the same or at least one of them is $\bot$. We lift this relation to (finite and infinite) sequences of observations (of the same length). We write $w \gtrsim \upsilon$ when $u \sim \upsilon$ holds for the length-$|\upsilon|$ prefix u of w.

We say that υ is *negatively deciding* when $\Pr(\{w \gtrsim \upsilon \mid w \in L\}) = 0$. Intuitively, υ is negatively deciding when υ is incompatible (up to a null set) with L. Similarly, we say that υ is *positively deciding* when $\Pr(\{w \gtrsim \upsilon \mid w \notin L\}) = 0$. An observation prefix υ is *deciding* when it is positively or negatively deciding. An observation policy ρ *decides* w when $\pi_\rho(w)$ has a deciding prefix.

Lemma 1. *For any w, if some policy decides w then $\bullet$ decides w.*

Proof. Let ρ decide w. Then there is a deciding prefix, υ, of $\pi_\rho(w)$. Suppose υ is positively deciding, i.e., $\Pr(\{w' \gtrsim \upsilon \mid w' \notin L\}) = 0$. Let u be the length-$|\upsilon|$ prefix of w. Then $\Pr(\{w' \gtrsim u \mid w' \notin L\}) = 0$, since υ can be obtained from u by possibly replacing some letters with $\bot$. Hence u is also positively deciding. Since u is a prefix of $w = \pi_\bullet(w)$, we have that $\bullet$ decides w. The case where υ is negatively deciding is similar. $\square$

It follows that $\max_\rho \Pr(\{w \mid \rho \text{ decides } w\}) = \Pr(\{w \mid \bullet \text{ decides } w\})$. We say that a policy ρ is *feasible* when it also attains the maximum, i.e., when

$$\Pr(\{w \mid \rho \text{ decides } w\}) \;=\; \Pr(\{w \mid \bullet \text{ decides } w\})\,.$$

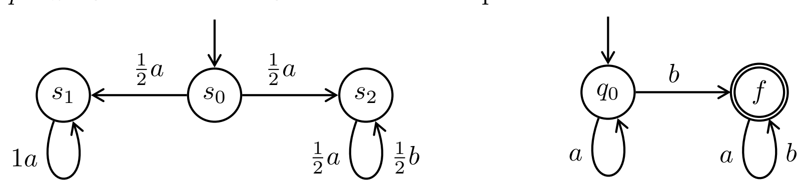
Equivalently, ρ is feasible when $\Pr(\{w \mid \bullet \text{ decides } w \text{ implies } \rho \text{ decides } w\}) = 1$, i.e., almost all words that are decided by the see-all policy are also decided by ρ. If $\upsilon = o_1 o_2 \dots$ is the shortest prefix of $\pi_\rho(w)$ that is deciding, then the *cost of decision* $C_\rho(w)$ is $\sum_{k=0}^{|\upsilon|-1} \rho(o_1 \dots o_k)$. This paper is about finding feasible observation policies ρ that minimize $\mathrm{Ex}(C_\rho)$, the expectation of the cost of decision with respect to Pr.

3 Qualitative Analysis of Observation Policies

In this section we study properties of observation policies that are qualitative, i.e., not directly related to the cost of decision. We focus on properties of observation prefixes that a policy may produce.

Observation Prefixes. Recall that we have defined what it means for an observation prefix to be positively or negatively deciding. An observation prefix $\upsilon \in \Sigma_\perp^*$ is called *enabled* when $\Pr(\{w \gtrsim \upsilon\}) > 0$. Further, υ is *confused* when $\Pr(\{uw \mid u \sim \upsilon,\ \text{no prefix of } \upsilon w \text{ is deciding}\}) > 0$. (Confused implies enabled and not deciding.) Intuitively, when an observation policy produces a confused observation prefix, then it may (with positive probability) fail to decide. Further, υ is called *very confused* when $\upsilon u'$ is non-deciding for all enabled $\upsilon u'$. (Enabled and very confused implies confused.) Intuitively, when an observation policy produces a very confused observation prefix, then it may as well give up observing, as there is no chance to decide. Further, υ is called *finitary* when $\Pr(\{uw \mid u \sim \upsilon,\ \text{no prefix of } \upsilon w \text{ is deciding or very confused}\}) = 0$. Why this is called finitary will become clear later (Proposition 12).

Example 2. Consider the MC and the DFA depicted here:



All observation prefixes that do not start with b are enabled. The observation prefixes ab and $\perp b$ and, in fact, all observation prefixes that contain b, are positively deciding. For all $n \in \mathbb{N}$ we have $\Pr(\{w \gtrsim a^n \mid w \in L\}) > 0$ and $\Pr(\{w \gtrsim a^n \mid w \notin L\}) > 0$, so a^n is not deciding. If the MC takes the right transition first then almost surely it emits b at some point. Thus $\Pr(\{aaa \cdots\}) = \frac{1}{2}$. Hence ε is confused. In this example only non-enabled observation prefixes are very confused. It follows that ε is not finitary. $\square$

Beliefs. For any s we write $\Pr_s$ for the probability measure of the MC $\mathcal{M}_s$ obtained from $\mathcal{M}$ by making s the initial state. For any q we write $L_q \subseteq \Sigma^\omega$ for the language of the DFA $\mathcal{A}_q$ obtained from $\mathcal{A}$ by making q the initial state. We call a pair (s, q) *negatively deciding* when $\Pr_s(L_q) = 0$; similarly, we call (s, q) *positively deciding* when $\Pr_s(L_q) = 1$. A subset of $S \times Q$ is called *belief*. We call a belief *negatively* (*positively*, respectively) *deciding* when all its elements are. We fix the notation $B_0 \coloneqq \{(s_0, q_0)\}$ (for the *initial belief*) for the remainder of the paper. Define the *belief NFA* as the NFA $\mathcal{B} = (S \times Q, \Sigma_\perp, \Delta, B_0, \emptyset)$ with:

$$\begin{aligned} \Delta((s,q),a) \;&=\; \{(s',q') \mid \ M(a)(s,s') > 0,\ \delta(q,a) = q'\} \quad \text{for } a \in \Sigma \\ \Delta((s,q),\perp) \;&=\; \bigcup_{a \in \Sigma} \Delta((s,q),a) \end{aligned}$$

We extend the transition function $\Delta : (S \times Q) \times \Sigma_\perp \to 2^{S\times Q}$ to $\Delta : 2^{S\times Q} \times \Sigma_\perp^* \to 2^{S\times Q}$ in the way that is usual for NFAs. Intuitively, interpreting a belief B as a set of states (s, q) where the MC $\mathcal{M} \times \mathcal{A}$ could be in after having made certain observations, the belief $\Delta(B, \upsilon)$ is the belief adjusted by additionally observing υ. To reason about observation prefixes υ algorithmically, it will be convenient to reason about the belief $\Delta(B_0, \upsilon)$.

We call a belief B *confused* when there is $(s, q) \in B$ with

$$\Pr_s(\{uw \mid \Delta(B, u) \text{ is deciding}\}) \;<\; 1\,.$$

We call a belief B *very confused* when for all u we have that $\Delta(B, u)$ is empty or not deciding. Finally, we call a belief B *finitary* when for all $(s, q) \in B$ we have

$$\Pr_s(\{uw \mid \Delta(B, u) \text{ is deciding or very confused}\}) \;=\; 1\,.$$

Example 3. In Example 2 we have $B_0 = \{(s_0, q_0)\}$, and $\Delta(B_0, a^n) = \{(s_1, q_0), (s_2, q_0)\}$ for all $n \geq 1$, and $\Delta(B_0, b) = \emptyset$, and $\Delta(B_0, a\perp) = \{(s_1, q_0), (s_2, q_0), (s_2, f)\}$, and $\Delta(B_0, \perp\upsilon) = \{(s_2, f)\}$ for all υ that contain b. The latter belief $\{(s_2, f)\}$ is positively deciding. We have $\Pr_{s_1}(\{uw \mid \Delta(\{(s_1, q_0)\}, u) \text{ is deciding}\}) = 0$, so any belief that contains (s_1, q_0) is confused. Also, B_0 is confused as $\Pr_{s_0}(\{uw \mid \Delta(\{(s_0, q_0)\}, u) \text{ is deciding}\}) = \frac{1}{2}$. □

Relation Between Observation Prefixes and Beliefs. By the following lemma, the corresponding properties of observation prefixes and beliefs are closely related.

Lemma 4. *Let υ be an observation prefix.*

1. *υ is enabled if and only if $\Delta(B_0, \upsilon) \neq \emptyset$.*
2. *υ is negatively deciding if and only if $\Delta(B_0, \upsilon)$ is negatively deciding.*
3. *υ is positively deciding if and only if $\Delta(B_0, \upsilon)$ is positively deciding.*
4. *υ is confused if and only if $\Delta(B_0, \upsilon)$ is confused.*
5. *υ is very confused if and only if $\Delta(B_0, \upsilon)$ is very confused.*
6. *υ is finitary if and only if $\Delta(B_0, \upsilon)$ is finitary.*

The following lemma gives complexity bounds for computing these properties.

Lemma 5. *Let υ be an observation prefix, and B a belief.*

1. *Whether υ is enabled can be decided in P.*
2. *Whether υ (or B) is negatively deciding can be decided in P.*
3. *Whether υ (or B) is positively deciding can be decided in P.*
4. *Whether υ (or B) is confused can be decided in PSPACE.*
5. *Whether υ (or B) is very confused can be decided in PSPACE.*
6. *Whether υ (or B) is finitary can be decided in PSPACE.*

Proof (sketch). The belief NFA $\mathcal{B}$ and the MC $\mathcal{M} \times \mathcal{A}$ can be computed in polynomial time (even in deterministic logspace). For items 1–3, there are efficient graph algorithms that search these product structures. For instance, to show that a given pair (s_1, q_1) is not negatively deciding, it suffices to show that $\mathcal{B}$ has a path from (s_1, q_1) to a state (s_2, f) for some s_2. This can be checked in polynomial time (even in NL).

For items 4–6, one searches the (exponential-sized) product of $\mathcal{M}$ and the *determinization* of $\mathcal{B}$. This can be done in PSPACE. For instance, to show that a given belief B is confused, it suffices to show that there are $(s_1, q_1) \in B$ and u_1 and s_2 such that $\mathcal{M}$ has a u_1-labelled path from s_1 to s_2 such that there do *not* exist u_2 and s_3 such that $\mathcal{M}$ has a u_2-labelled path from s_2 to s_3 such that $\Delta(B, u_1 u_2)$ is deciding. This can be checked in NPSPACE = PSPACE by nondeterministically guessing paths in the product of $\mathcal{M}$ and the determinization of $\mathcal{B}$. □

Diagnosability. We call a policy a *diagnoser* when it decides almost surely.

Example 6. In Example 2 a diagnoser does not exist. Indeed, the policy $\bullet$ does not decide when the MC takes the left transition, and decides (positively) almost surely when the MC takes the right transition in the first step. Hence $\Pr(\{w \mid \bullet \text{ decides } w\}) = \Pr(\Sigma^* \{b\} \Sigma^\omega) = \frac{1}{2}$. So $\bullet$ is not a diagnoser. By Lemma 1, it follows that there is no diagnoser. □

Diagnosability can be characterized by the notion of confusion:

Proposition 7. *There exists a diagnoser if and only if ε is not confused.*

The following proposition shows that diagnosability is hard to check.

Theorem 8 (cf. [2, Theorem 6]). *Given an MC $\mathcal{M}$ and a DFA $\mathcal{A}$, it is PSPACE-complete to check if there exists a diagnoser.*

Theorem 8 essentially follows from a result by Bertrand et al. [2]. They study several different notions of diagnosability; one of them (*FA-diagnosability*) is very similar to our notion of diagnosability. There are several small differences; e.g., their systems are not necessarily products of an MC and a DFA. Therefore we give a self-contained proof of Theorem 8.

Proof (sketch). By Proposition 7 it suffices to show PSPACE-completeness of checking whether ε is confused. Membership in PSPACE follows from Lemma 5.4. For hardness we reduce from the following problem: given an NFA $\mathcal{U}$ over $\Sigma = \{a, b\}$ where all states are initial and accepting, does $\mathcal{U}$ accept all (finite) words? This problem is PSPACE-complete [9, Lemma 6]. □

Allowing Confusion. We say an observation policy *allows confusion* when, with positive probability, it produces an observation prefix $\upsilon\bot$ such that $\upsilon\bot$ is confused but υ is not.

Proposition 9. *A feasible observation policy does not allow confusion.*

Hence, in order to be feasible, a policy must observe when it would get confused otherwise. In § 5 we show that in the non-hidden case there is almost a converse of Proposition 9; i.e., in order to be feasible, a policy need not do much more than not allow confusion.

4 Analyzing the Cost of Decision

In this section we study the computational complexity of finding feasible policies that minimize the expected cost of decision. Since the complexity turns out to be high and it is not clear in general how to finitely represent arbitrary policies, we focus on an "easier" problem, namely determining whether there exists a feasible policy whose expected cost of decision is smaller than a given threshold. Define:

$$c_{inf} \;\coloneqq\; \inf_{\text{feasible } \rho} \mathrm{Ex}(C_\rho)$$

Since the see-all policy $\bullet$ never stops observing, we have $\Pr(C_\bullet = \infty) = 1$, so $\mathrm{Ex}(C_\bullet) = \infty$. However, once an observation prefix υ is deciding or very confused, there is no point in continuing observation. Hence, we define a *light see-all* policy $\circ$, which observes until the observation prefix u is deciding or very confused; formally, $\circ(\upsilon) = 0$ if and only if υ is deciding or very confused. It follows from the definition of very confused that the policy $\circ$ is feasible. Concerning the cost $C_\circ$ we have for all w

$$C_\circ(w) \;=\; \sum_{n=0}^{\infty} \big(1 - D_n(w)\big)\,, \tag{1}$$

where $D_n(w) = 1$ if the length-n prefix of w is deciding or very confused, and $D_n(w) = 0$ otherwise.

Lemma 10. *If ε is finitary then $\mathrm{Ex}(C_\circ)$ is finite.*

Proof (sketch). Consider the MC with states of the form $(s, B) \in S \times 2^{S \times Q}$. The expected time to reach a bottom strongly connected component is finite. ☐

Lemma 11. *Let ρ be a feasible observation policy. If $\Pr(C_\rho < \infty) = 1$ then ε is finitary.*

Lemmas 10 and 11 imply:

Proposition 12. *c_{inf} is finite if and only if ε is finitary.*

Proposition 13. *If a diagnoser exists then c_{inf} is finite.*

It is hard to compare c_{inf} with ∞:

Theorem 14. *Given an MC $\mathcal{M}$ and a DFA $\mathcal{A}$, it is PSPACE-complete to check if c_{inf} is finite.*

Proof (sketch). Use Proposition 12 and adapt the proof of Theorem 8. □

One cannot compute c_{inf}:

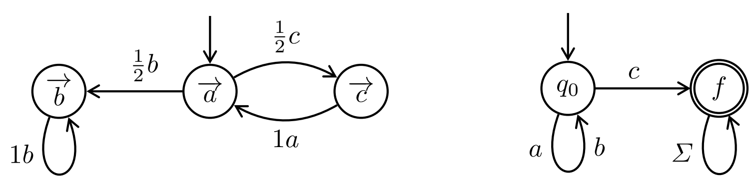
Theorem 15. *Given an MC $\mathcal{M}$ and a DFA $\mathcal{A}$, it is undecidable to check if $c_{inf} < 3$, even when a diagnoser exists.*

Proof (sketch). By a reduction from the undecidable problem whether a given probabilistic automaton accepts some word with probability $> \frac{1}{2}$. The proof is somewhat complicated. In fact, in the appendix we give two versions of the proof: a short incorrect one (with the correct main idea) and a long correct one. □

5 The Non-Hidden Case

In the rest of the paper we assume that the MC $\mathcal{M}$ is non-hidden, i.e., there exists a function $\overrightarrow{\cdot} : \Sigma \to S$ such that $M(a)(s, s') > 0$ implies $s' = \overrightarrow{a}$. We extend $\overrightarrow{\cdot}$ to finite words so that $\overrightarrow{ua} = \overrightarrow{a}$. We write $s \xrightarrow{u}$ to indicate that there is s' with $M(u)(s, s') > 0$.

Example 16. Consider the following non-hidden MC and DFA:



Here we have $B_0 := \{(\overrightarrow{a}, q_0)\}$ and:

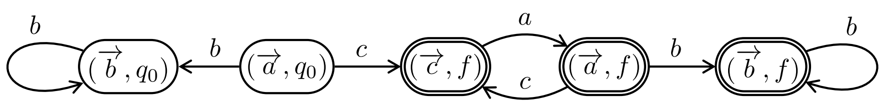
$$\begin{aligned} B_1 &:= \Delta(B_0, \bot) &&= \{(\overrightarrow{b}, q_0), (\overrightarrow{c}, f)\} \\ B_2 &:= \Delta(B_0, \bot^2) &&= \{(\overrightarrow{b}, q_0), (\overrightarrow{a}, f)\} \\ B_3 &:= \Delta(B_0, \bot^2 b) &&= \{(\overrightarrow{b}, q_0), (\overrightarrow{b}, f)\} \end{aligned}$$

The beliefs B_0 and B_1 are not confused: indeed, $\Delta(B_1, b) = \{(\overrightarrow{b}, q_0)\}$ is positively deciding, and $\Delta(B_1, a) = \{(\overrightarrow{a}, f)\}$ is negatively deciding. The belief B_2 is confused, and B_3 is very confused. □

In the non-hidden case there always exists a diagnoser. It follows that feasible policies need to decide almost surely and, by Proposition 13, that c_{inf} is finite. We have seen in Proposition 9 that feasible policies do not allow confusion. In this section we construct policies that procrastinate so much that they avoid confusion just barely. We will see that such policies have an expected cost that comes arbitrarily close to c_{inf}.

Language Equivalence. We characterize confusion by language equivalence in a certain DFA. Consider the belief NFA $\mathcal{B}$. In the non-hidden case, if we disallow $\perp$-transitions then $\mathcal{B}$ becomes a DFA $\mathcal{B}'$. For $\mathcal{B}'$ we define a set of accepting states by $F_{\mathcal{B}'} := \{(s,q) \mid \Pr_s(L_q) = 1\}$.

Example 17. For the previous example, a part of the DFA $\mathcal{B}'$ looks as follows:



Some states, e.g., $(\overrightarrow{c}, q_0)$, and their transitions are not drawn here. □

We associate with each (s,q) the language $L_{s,q} \subseteq \Sigma^*$ that $\mathcal{B}'$ accepts starting from initial state (s,q). We call $(s,q),(s',q')$ *language equivalent*, denoted by $(s,q) \approx (s',q')$, when $L_{s,q} = L_{s',q'}$.

Lemma 18. *One can compute the relation $\approx$ in polynomial time.*

Proof. For any (s,q) one can use standard MC algorithms to check in polynomial time if $\Pr_s(L_q) = 1$ (using a graph search in the composition $\mathcal{M} \times \mathcal{A}$, as in the proof of Lemma 5.3). Language equivalence in the DFA $\mathcal{B}'$ can be computed in polynomial time, e.g., by minimization. □

We call a belief $B \subseteq S \times Q$ *settled* when all $(s,q) \in B$ are language equivalent.

Lemma 19. *A belief $B \subseteq S \times Q$ is confused if and only if there is $a \in \Sigma$ such that $\Delta(B,a)$ is not settled.*

It follows that one can check in polynomial time whether a given belief is confused. We generalize this fact in Lemma 22 below.

Example 20. In Example 16 the belief B_3 is not settled. Indeed, from the DFA in Example 17 we see that $L_{\overrightarrow{b},q_0} = \emptyset \neq \{b\}^* = L_{\overrightarrow{b},f}$. Since $B_3 = \Delta(B_2, b)$, by Lemma 19, the belief B_2 is confused. □

Procrastination. For a belief $B \subseteq S \times Q$ and $k \in \mathbb{N}$, if $\Delta(B, \perp^k)$ is confused then so is $\Delta(B, \perp^{k+1})$. We define:

$$\mathit{cras}(B) \;:=\; \sup\{k \in \mathbb{N} \mid \Delta(B, \perp^k) \text{ is not confused}\} \in \mathbb{N} \cup \{-1, \infty\}$$

We set $\mathit{cras}(B) := -1$ if B is confused. We may write $\mathit{cras}(s,q)$ for $\mathit{cras}(\{(s,q)\})$.

Example 21. In Example 16 we have $\mathit{cras}(B_0) = \mathit{cras}(\overrightarrow{a}, q_0) = 1$ and $\mathit{cras}(B_1) = 0$ and $\mathit{cras}(B_2) = -1$ and $\mathit{cras}(\overrightarrow{b}, q_0) = \mathit{cras}(\overrightarrow{a}, f) = \infty$. □

Lemma 22. *Given a belief B, one can compute $\mathit{cras}(B)$ in polynomial time. Further, if $\mathit{cras}(B)$ is finite then $\mathit{cras}(B) \le |S|^2 \cdot |Q|^2$.*

Proof. Let $k \in \mathbb{N}$. By Lemma 19, $\Delta(B, \bot^k)$ is confused if and only if:

$$\exists\, a.\, \exists\, (s,q),(t,r) \in \Delta(B, \bot^k) : s \xrightarrow{a},\ t \xrightarrow{a},\ (\overrightarrow{a}, \delta(q,a)) \not\approx (\overrightarrow{a}, \delta(r,a))$$

This holds if and only if there is $B_2 \subseteq B$ with $|B_2| \le 2$ such that:

$$\exists\, a.\, \exists\, (s,q),(t,r) \in \Delta(B_2, \bot^k) : s \xrightarrow{a},\ t \xrightarrow{a},\ (\overrightarrow{a}, \delta(q,a)) \not\approx (\overrightarrow{a}, \delta(r,a))$$

Let G be the directed graph with nodes in $S \times Q \times S \times Q$ and edges

$$((s,q,t,r),(s',q',t',r')) \qquad \Longleftrightarrow \qquad \Delta(\{(s,q),(t,r)\}, \bot) \ \supseteq\ \{(s',q'),(t',r')\}\,.$$

Also define the following set of nodes:

$$U \ \coloneqq\ \{(s,q,t,r) \mid \exists\, a : s \xrightarrow{a},\ t \xrightarrow{a},\ (\overrightarrow{a}, \delta(q,a)) \not\approx (\overrightarrow{a}, \delta(r,a))\}$$

By Lemma 18 one can compute U in polynomial time. It follows from the argument above that $\Delta(B, \bot^k)$ is confused if and only if there are $(s,q),(t,r) \in B$ such that there is a length-k path in G from (s,q,t,r) to a node in U. Let $k \le |S \times Q \times S \times Q|$ be the length of the shortest such path, and set $k \coloneqq \infty$ if no such path exists. Then k can be computed in polynomial time by a search of the graph G, and we have $\mathit{cras}(B) = k - 1$. ◻

The Procrastination Policy. For any belief B and any observation prefix υ, the language equivalence classes represented in $\Delta(B, \upsilon)$ depend only on υ and the language equivalence classes in B. Therefore, when tracking beliefs along observations, it is ok to restrict B to a single representative of each equivalence class. We denote this operation by $B{\downarrow}$. A belief B is settled if and only if $|B{\downarrow}| \le 1$.

A *procrastination policy* $\rho_{pro}(K)$ is parameterized with (a large) $K \in \mathbb{N}$. Define (and precompute) $k(s,q) \coloneqq \min\{K, \mathit{cras}(s,q)\}$ for all (s,q). The policy $\rho_{pro}(K)$ operates as follows:

1. $i \coloneqq 0$
2. while (s_i, q_i) is not deciding:
   (a) observe only after exactly $k(s_i,q_i)+1$ steps, yielding an observation prefix $\upsilon_i \coloneqq \bot^{k(s_i,q_i)} a_i$;
   (b) $\{(s_{i+1}, q_{i+1})\} \coloneqq \Delta((s_i,q_i), \upsilon_i){\downarrow}$;
   (c) $i \coloneqq i + 1$;

It follows from the definition of *cras* and Lemma 19 that $\Delta((s_i,q_i), \upsilon_i){\downarrow}$ is indeed a singleton for all i. We have:

Lemma 23. *For all $K \in \mathbb{N}$ the procrastination policy $\rho_{pro}(K)$ is a diagnoser.*

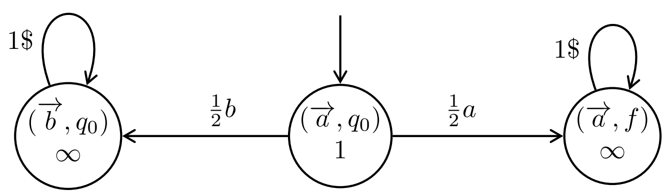
Proof. The singleton belief $\{(s_0, q_0)\}$ cannot be confused in a non-hidden MC, i.e., we have $\Pr_s(\{uaw \mid (\overrightarrow{a}, \delta(q, ua)) \text{ is deciding}\}) = 1$. It follows that $\rho_{pro}(K)$ produces, almost surely, eventually an observation prefix υa_i such that $B \coloneqq \Delta(B_0, \upsilon a_i)$ contains a deciding pair (s,q). But, as remarked above, B is settled, so B is deciding. ◻

The Procrastination MC $\mathcal{M}_{pro}(K)$. The policy $\rho_{pro}(K)$ produces a (random, almost surely finite) word $a_1 a_2 \cdots a_n$ with $n = C_{\rho_{pro}(K)}$. Indeed, the observations that $\rho_{pro}(K)$ makes can be described by an MC. Recall that we have previously defined a composition MC $\mathcal{M} \times \mathcal{A} = (S \times Q, \Sigma, M', (s_0, q_0))$. Now define an MC $\mathcal{M}_{pro}(K) \coloneqq (S \times Q, \Sigma \cup \{\$\}, M_{pro}(K), (s_0, q_0))$ where $\$ \notin \Sigma$ is a fresh letter and the transitions are as follows: when (s, q) is deciding then $M_{pro}(K)(\$)\big((s, q), (s, q)\big) \coloneqq 1$, and when (s, q) is not deciding then

$$M_{pro}(K)(a)\big((s,q),(\overrightarrow{a},q')\big) \;\coloneqq\; \Big(M'(\bot)^{k(s,q)} M'(a)\Big)\left((s,q),(\overrightarrow{a},q')\right),$$

where the matrix $M'(\bot) \coloneqq \sum_a M'(a)$ is powered by $k(s, q)$. The MC $\mathcal{M}_{pro}(K)$ may not be non-hidden, but could be made non-hidden by (i) collapsing all language equivalent $(s, q_1), (s, q_2)$ in the natural way, and (ii) redirecting all \$-labelled transition to a new state $\overrightarrow{\$}$ that has a self-loop. In the understanding that $\$\$\$\cdots$ indicates 'decision made', the probability distribution defined by the MC $\mathcal{M}_{pro}(K)$ coincides with the probability distribution on sequences of non-$\bot$ observations made by $\rho_{pro}(K)$.

Example 24. For Example 16 the MC $\mathcal{M}_{pro}(K)$ for $K \geq 1$ is as follows:



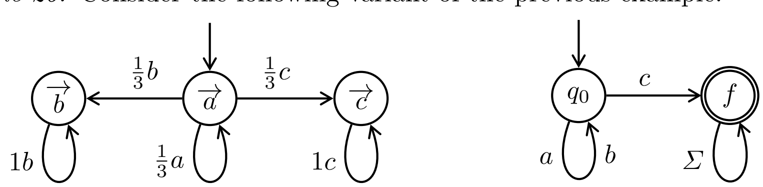
Here the lower number in a state indicate the *cras* number. The left state is negatively deciding, and the right state is positively deciding. The policy $\rho_{pro}(K)$ skips the first observation and then observes either b or a, each with probability $\frac{1}{2}$, each leading to a deciding belief. $\square$

Maximal Procrastination is Optimal. The following lemma states, loosely speaking, that when a belief $\{(s, q)\}$ with $cras(s, q) = \infty$ is reached and K is large, then a single further observation is expected to suffice for a decision.

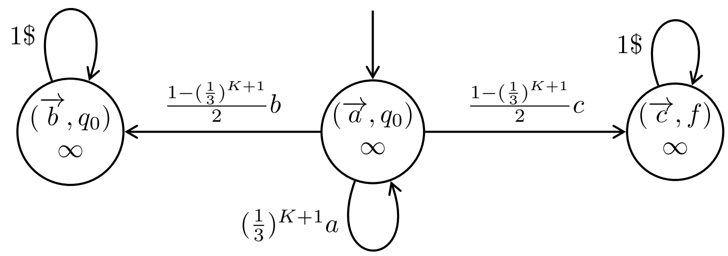
Lemma 25. *Let $c(K, s, q)$ denote the expected cost of decision under $\rho_{pro}(K)$ starting in (s, q). For each $\varepsilon > 0$ there exists $K \in \mathbb{N}$ such that for all (s, q) with $cras(s, q) = \infty$ we have $c(K, s, q) \leq 1 + \varepsilon$.*

Proof (sketch). Quantitative version of the proof of Lemma 23. $\square$

Example 26. Consider the following variant of the previous example:



The MC $\mathcal{M}_{pro}(K)$ for $K \geq 0$ is as follows:



The left state is negatively deciding, and the right state is positively deciding. We have $c(K, \overrightarrow{b}, q_0) = c(K, \overrightarrow{c}, f) = 0$ and $c(K, \overrightarrow{a}, q_0) = 1/(1 - (\frac{1}{3})^{K+1})$. $\square$

Now we can prove:

Theorem 27. *For any feasible policy ρ there is $K \in \mathbb{N}$ such that:*

$$\mathrm{Ex}(C_{\rho_{pro}(K)}) \;\leq\; \mathrm{Ex}(C_\rho)$$

Proof (sketch). Let ρ be a feasible policy. We choose $K > |S|^2 \cdot |Q|^2$, so, by Lemma 22, $\rho_{pro}(K)$ coincides with $\rho_{pro}(\infty)$ until time, say, n_∞ when $\rho_{pro}(K)$ encounters a pair (s, q) with $cras(s, q) = \infty$. (The time n_∞ may, with positive probability, never come.) Let us compare $\rho_{pro}(K)$ with ρ up to time n_∞. For $n \in \{0, \ldots, n_\infty\}$, define $\upsilon_{pro}(n)$ and $\upsilon_\rho(n)$ as the observation prefixes obtained by ρ_{pro} and ρ, respectively, after n steps. Write $\ell_{pro}(n)$ and $\ell_\rho(n)$ for the number of non-$\perp$ observations in $\upsilon_{pro}(n)$ and $\upsilon_\rho(n)$, respectively. For beliefs B, B' we write $B \preceq B'$ when for all $(s, q) \in B$ there is $(s', q') \in B'$ with $(s, q) \approx (s', q')$. One can show by induction that we have for all $n \in \{0, \ldots, n_\infty\}$:

$$\ell_{pro}(n) \leq \ell_\rho(n) \quad \text{ and } \quad \big(\varDelta(B_0, \upsilon_{pro}(n)) \preceq \varDelta(B_0, \upsilon_\rho(n)) \quad \text{or} \quad \ell_{pro}(n) < \ell_\rho(n)\big)$$

If time n_∞ does not come then the inequality $\ell_{pro}(n) \leq \ell_\rho(n)$ from above suffices. Similarly, if at time n_∞ the pair (s, q) is deciding, we are also done. If after time n_∞ the procrastination policy $\rho_{pro}(K)$ observes at least one more letter then ρ also observes at least one more letter. By Lemma 25, one can choose K large so that for $\rho_{pro}(K)$ one additional observation probably suffices. If it is the case that ρ almost surely observes only one letter after n_∞, then $\rho_{pro}(K)$ also needs only one more observation, since it has observed at time n_∞. $\square$

It follows that, in order to compute c_{inf}, it suffices to analyze $\mathrm{Ex}(C_{\rho_{pro}(K)})$ for large K. This leads to the following theorem:

Theorem 28. *Given a non-hidden MC $\mathcal{M}$ and a DFA $\mathcal{A}$, one can compute c_{inf} in polynomial time.*

Proof. For each (s, q) define $c(K, s, q)$ as in Lemma 25, and define $c(s, q) \coloneqq \lim_{K\to\infty} c(K, s, q)$. By Lemma 25, for each non-deciding (s, q) with $cras(s, q) = \infty$

we have $c(s,q) = 1$. Hence the $c(s,q)$ satisfy the following system of linear equations where some coefficients come from the procrastination MC $\mathcal{M}_{pro}(\infty)$:

$$\begin{aligned} c(s,q) &= \begin{cases} 0 & \text{if } (s,q) \text{ is deciding} \\ 1 & \text{if } (s,q) \text{ is not deciding and } \mathit{cras}(s,q) = \infty \\ 1 + c'(s,q) & \text{otherwise} \end{cases} \\ c'(s,q) &= \sum_a \sum_{q'} M_{pro}(\infty)\big((s,q),(\overrightarrow{a},q')\big) \cdot c(\overrightarrow{a},q') \qquad \text{if } \mathit{cras}(s,q) < \infty \end{aligned}$$

By solving the system one can compute $c(s_0,q_0)$ in polynomial time. We have:

$$\begin{aligned} c_{\mathit{inf}} &= \inf_{\text{feasible } \rho} \mathrm{Ex}(C_\rho) && \text{definition of } c_{\mathit{inf}} \\ &= \lim_{K\to\infty} \mathrm{Ex}(C_{\rho_{pro}(K)}) && \text{Theorem 27} \\ &= c(s_0,q_0) && \text{definitions} \end{aligned}$$

Hence one can compute c_{inf} in polynomial time. ☐

Example 29. In Example 26 we have $c_{\mathit{inf}} = c(\overrightarrow{a},q_0) = 1$. ☐

6 Experiments

We have shown that maximal procrastination is optimal (Theorem 27). With experiments, we answer the following question: *How much better is maximal procrastination than the light see-all policy* $\circ$*, on real data?* To answer this question, we implemented our algorithms in a fork of the Facebook Infer static analyzer [4], and applied them to 11 open-source projects, totaling 80 thousand Java methods.

Design. Our setting requires a DFA and an MC representing, respectively, a program property and a program. For these experiments, the DFA represents the following property: 'there are no two calls to *next* without an intervening call to *hasNext*'. For the MC, we could have used an inter-procedural control flowgraph, but we opted to utilize Infer's symbolic paths because they are more precise.

Infer [4,5] is a static analyzer that, for each method, infers several preconditions and, attached to each precondition, a symbolic path. For a simple example, consider a method whose body is 'if $(b)\, x.\mathit{next}()$; if $(!b)\, x.\mathit{next}()$'. Infer would generate two preconditions for it, b and $\neg b$. In each of the two attached symbolic paths, we can see that *next* is not called twice, which we would not notice with a control flowgraph. The symbolic paths are inter-procedural. If a method f calls a method g, then the path of f will link to a path of g and, moreover, it will pick one of the paths of g that corresponds to what is currently known at the call site. For example, if $g(b)$ is called from a state in which $\neg b$ holds, then Infer will select a path of g compatible with the condition $\neg b$.

The symbolic paths are finite because abstraction is applied, including across mutually recursive calls. But, still, multiple vertices of the symbolic path correspond to the same vertex of the control flowgraph. For example, Infer may go around a for-loop five times before noticing the invariant. By coalescing those vertices of the symbolic path that correspond to the same vertex of the control flowgraph we obtain an *SFG (symbolic flowgraph)*. We use such SFGs as the skeleton of MCs. Intuitively, one can think of SFGs as inter-procedural control flowgraphs restricted based on semantic information. Vertices correspond to locations in the program text, and transitions correspond to method calls or returns. Transition probabilities should then be interpreted as a from of static branch prediction. One could learn these probabilities by observing many runs of the program on typical input data. Instead, we opt to show that the improvement in expected observation cost is robust over a wide range of possible transition probabilities, which we do by drawing several samples from Dirichlet distributions. Besides, recall that the (optimal) procrastination policy does not depend on transition probabilities.

Once we have a DFA and an MC we compute their product. In some cases, it is clear that the product is empty or universal. These are the cases in which we can give the verdict right-away, because no observation is necessary. We then focus on the non-trivial cases.

For non-trivial MC $\times$ DFA products, we compute the expected cost of the light see-all policy $\mathrm{Ex}(C_\circ)$, which observes all letters until a decision is made and then stops. We can do so by using standard algorithms [1, Chapter 10.5]. Then, we compute $\mathcal{M}_{pro}$, which we use to compute the expected observation cost c_{inf} of the procrastination policy (Theorem 28).

The procrastination policy only makes sense under the assumption that the MC is non-hidden. In terms of the implementation in a runtime verifier, this assumption means that the program should be instrumented such that the monitor can distinguish different calls to the same method, which is not difficult.

Methodology. We selected 11 Java projects among those that are most forked on GitHub (Table 2). We ran Infer on each of these projects. From the inferred specifications, we built SFGs and monitors that employ light see-all policies and maximal procrastination policies. From these monitors, we computed the respective expected costs, solving the linear systems using Gurobi [6]. Our implementation is in a fork of Infer.

Results. The results are given in Table 1. We first note that the number of monitors is much smaller than the number of methods, by a factor of 10 or 100. This is because in most cases we are able to determine the answer statically, by analyzing the symbolic paths produced by Infer. The large factor should not be too surprising: we are considering a fixed property about iterators, not all Java methods use iterators, and, when they do, it is usually easy to tell that they do so correctly. Still, each project has a few hundred monitors, which handle the cases that are not so obvious.

Table 1. Reduction in expected observation cost, on real-world data. Each SFG (symbolic flowgraph) corresponds to one inferred precondition of a method. The size of monitors is given in number of states after $(s, q) \approx (s, q')$ are coalesced. LOC stands for lines of code; GAvg stands for geometric average.

	Project Size			Monitors ($\mathcal{M}_{pro}$)			$c_{inf}/\mathrm{Ex}(C_\circ)$	
Name	Methods	SFGs	LOC	Count	Avg-Size	Max-Size	Med	GAvg
tomcat	26K	52K	946K	343	69	304	0.53	0.50
okhttp	3K	6K	49K	110	263	842	0.46	0.42
dubbo	8K	16K	176K	91	111	385	0.53	0.51
jadx	4K	9K	48K	204	96	615	0.58	0.50
RxJava	12K	45K	192K	83	41	285	0.52	0.53
guava	22K	43K	1218K	1126	134	926	0.41	0.41
clojure	5K	19K	66K	219	120	767	0.44	0.44
AndroidUtilCode	3K	7K	436K	39	89	288	0.66	0.58
leakcanary	1K	1K	11K	12	79	268	0.66	0.59
deeplearning4j	21K	40K	408K	262	51	341	0.58	0.58
fastjson	2K	7K	47K	204	63	597	0.59	0.53

We note that $\frac{c_{inf}}{\mathrm{Ex}(C_\circ)} \approx 0.5$. The table supports this by presenting the median and the geometric average, which are close to each-other; the arithmetic average is also close. There is, however, quite a bit of variation from monitor to monitor, as shown in Figure 1. We conclude that selective monitoring can significantly reduce the overhead of runtime monitoring.

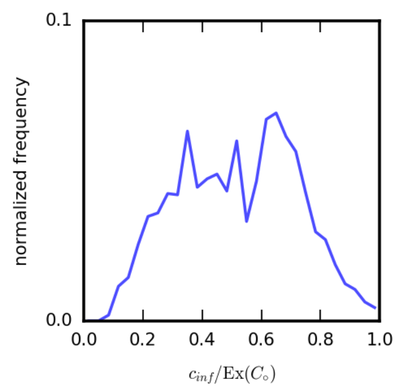


Fig. 1. Empirical distribution of $c_{inf}/\mathrm{Ex}(C_\circ)$, across all projects.

7 Future Work

In this paper we required policies to be feasible. One may relax this and study the tradeoff between efficiency (skipping even more observations) and precision (probability of making a decision). Further, one could replace the diagnosability notion of this paper by other notions from the literature; one could investigate how to compute c_{inf} for other classes of MCs, such as acyclic MCs; one could study the sensitivity of c_{inf} to changes in transition probabilities; and one could identify classes of MCs for which selective monitoring helps and classes of MCs for which selective monitoring does not help. Finally, the monitors we computed could be used in a runtime verifier.

References

1. C. Baier and J.-P. Katoen. *Principles of model checking.* MIT Press, 2008.

2. N. Bertrand, S. Haddad, and E. Lefaucheux. Foundation of diagnosis and predictability in probabilistic systems. In *Proceedings of FSTTCS*, volume 29 of *LIPIcs*, pages 417–429, 2014.
3. N. Bertrand, S. Haddad, and E. Lefaucheux. Accurate approximate diagnosability of stochastic systems. In *Proceedings of LATA*, pages 549–561. Springer, 2016.
4. C. Calcagno, D. Distefano, J. Dubreil, D. Gabi, P. Hooimeijer, M. Luca, P. O'Hearn, I. Papakonstantinou, J. Purbrick, and D. Rodriguez. Moving fast with software verification. In *NASA Formal Methods Symposium*, 2015.
5. C. Calcagno, D. Distefano, P.W. O'Hearn, and H. Yang. Compositional shape analysis by means of bi-abduction. *JACM*, 2011.
6. Gurobi Optimization, Inc. Gurobi optimizer reference manual. http://www.gurobi.com, 2017.
7. S. Jiang, Z. Huang, V. Chandra, and R. Kumar. A polynomial algorithm for testing diagnosability of discrete-event systems. *IEEE Transactions on Automatic Control*, 46(8):1318–1321, 2001.
8. K. Kalajdzic, E. Bartocci, S.A. Smolka, S.D. Stoller, and R. Grosu. Runtime verification with particle filtering. In *RV*, 2013.
9. J.-Y. Kao, N. Rampersad, and J. Shallit. On NFAs where all states are final, initial, or both. *Theoretical Computer Science*, 410(47):5010–5021, 2009.
10. A. Paz. *Introduction to Probabilistic Automata*. Academic Press, 1971.
11. M. Sampath, R. Sengupta, S. Lafortune, K. Sinnamohideen, and D. Teneketzis. Diagnosability of discrete-event systems. *IEEE Transactions on Automatic Control*, 40(9):1555–1575, 1995.
12. S.D. Stoller, E. Bartocci, J. Seyster, R. Grosu, K. Havelund, S.A. Smolka, and E. Zadok. Runtime verification with state estimation. In *RV*, 2011.
13. D. Thorsley and D. Teneketzis. Diagnosability of stochastic discrete-event systems. *IEEE Transactions on Automatic Control*, 50(4):476–492, 2005.

A Experimental Details

Table 2. Open Source projects, from GitHub.

Owner	Project	Description
Apache	tomcat	Java Servlet, Server Pages, and WebSocket
Square	okhttp	an HTTP/HTTP2 client for Android
Alibaba	dubbo	a high-performance RPC framework
Skylot	jadx	Dex to Java decompiler
ReactiveX	RxJava	Reactive Extensions for the JVM
Google	guava	Google core libraries for Java
Clojure	clojure	the Clojure programming language
Blankj	AndroidUtilCode	a powerful and easy to use library for Android
Square	leakcanary	a memory leak detection library for Android
Deeplearning4j	deeplearning4j	Deep Learning for Java on Hadoop and Spark
Alibaba	fastjson	a fast JSON parser/generator

B Proofs

B.1 Proof of Lemma 4

Here is Lemma 4 from the main body:

Lemma 4. *Let υ be an observation prefix.*

1. *υ is enabled if and only if $\Delta(B_0, \upsilon) \neq \emptyset$.*
2. *υ is negatively deciding if and only if $\Delta(B_0, \upsilon)$ is negatively deciding.*
3. *υ is positively deciding if and only if $\Delta(B_0, \upsilon)$ is positively deciding.*
4. *υ is confused if and only if $\Delta(B_0, \upsilon)$ is confused.*
5. *υ is very confused if and only if $\Delta(B_0, \upsilon)$ is very confused.*
6. *υ is finitary if and only if $\Delta(B_0, \upsilon)$ is finitary.*

Proof. We have:

$$\begin{aligned} \Pr(\{w \gtrsim \upsilon\}) &= \sum_{u \sim \upsilon} \Pr(\{u\}\Sigma^\omega) \\ &= \sum_{u \sim \upsilon} \sum_{s} M(u)(s_0, s) \end{aligned} \tag{2}$$

Similarly we have:

$$\begin{aligned} \Pr(\{w \gtrsim \upsilon \mid w \in L\}) &= \sum_{u \sim \upsilon} \Pr(\{u\}\Sigma^\omega \cap L) \\ &= \sum_{u \sim \upsilon} \sum_{s} M(u)(s_0, s) \cdot \Pr_s(L_{\delta(q_0, u)}) \end{aligned} \tag{3}$$

Further, we have for all $B \subseteq S \times Q$:

$$\begin{aligned} \Delta(B, \upsilon) &= \bigcup_{u \sim \upsilon} \Delta(B, u) \\ &= \bigcup_{u \sim \upsilon} \{(s', q') \mid \exists\, (s, q) \in B : M(u)(s, s') > 0,\ \delta(q, u) = q'\} \end{aligned} \tag{4}$$

We prove item 1:

$$\begin{array}{lll} & \upsilon \text{ is enabled} & \\ \iff & \Pr(\{w \gtrsim \upsilon\}) > 0 & \text{definition} \\ \iff & \exists\, u \sim \upsilon.\, \exists\, s \text{ with } M(u)(s_0, s) > 0 & \text{by (2)} \\ \iff & \exists\, (s, q) \in \Delta(\{(s_0, q_0)\}, \upsilon) & \text{by (4)} \\ \iff & \Delta(B_0, \upsilon) \neq \emptyset & \text{definition} \end{array}$$

We prove item 2:

$$\begin{array}{lll} & \upsilon \text{ is negatively deciding} & \\ \iff & \Pr(\{w \gtrsim \upsilon \mid w \in L\}) = 0 & \text{definition} \\ \iff & \forall\, u \sim \upsilon.\, \forall s \text{ with } M(u)(s_0, s) > 0 : \Pr_s(L_{\delta(q_0, u)}) = 0 & \text{by (3)} \\ \iff & \forall\, (s, q) \in \Delta(B_0, \upsilon) : \Pr_s(L_q) = 0 & \text{by (4)} \\ \iff & \text{all } (s, q) \in \Delta(B_0, \upsilon) \text{ are negatively deciding} & \text{definition} \\ \iff & \Delta(B_0, \upsilon) \text{ is negatively deciding} & \text{definition} \end{array}$$

The proof of item 3 is similar. Towards item 4 note that if υ is not deciding then none of its prefixes is. This property explains the second equivalence in the following proof of item 4. There we write $u' < w$ to denote that u' is a finite prefix of w.

$$\begin{array}{lll} & \upsilon \text{ is confused} & \\ \iff & \Pr(\{uw \mid u \sim \upsilon,\ \text{no prefix of } \upsilon w \text{ is deciding}\}) > 0 & \text{definition} \\ \iff & \Pr(\{uw \mid u \sim \upsilon,\ \forall\, u' < w : \upsilon u' \text{ is not deciding}\}) > 0 & \text{see above} \\ \iff & \displaystyle\sum_{u \sim \upsilon} \sum_{s} M(u)(s_0, s) \cdot & \text{as before} \\ & \quad \cdot \Pr_s(\{w \mid \forall\, u' < w : \upsilon u' \text{ is not deciding}\}) > 0 & \\ \iff & \exists\, u \sim \upsilon.\, \exists\, s : M(u)(s_0, s) > 0 \text{ and} & \text{as before} \\ & \qquad \Pr_s(\{w \mid \forall\, u' < w : \upsilon u' \text{ is not deciding}\}) > 0 & \\ \iff & \exists\, (s, q) \in \Delta(B_0, \upsilon) : & \text{by (4)} \\ & \qquad \Pr_s(\{w \mid \forall\, u' < w : \upsilon u' \text{ is not deciding}\}) > 0 & \\ \iff & \exists\, (s, q) \in \Delta(B_0, \upsilon) : & \text{items 2, 3} \\ & \qquad \Pr_s(\{w \mid \forall\, u' < w : \Delta(\Delta(B_0, \upsilon), u') \text{ is not deciding}\}) > 0 & \\ \iff & \Delta(B_0, \upsilon) \text{ is confused} & \text{definition} \end{array}$$

We prove item 5:

$$\begin{array}{lll}
& \upsilon \text{ is very confused} & \\
\iff & \forall\, u : (\upsilon u \text{ is enabled} \to \upsilon u \text{ is not deciding}) & \text{definition} \\
\iff & \forall\, u : (\Delta(B_0, \upsilon u) \neq \emptyset \to \Delta(B_0, \upsilon u) \text{ is not deciding}) & \text{items 2, 3} \\
\iff & \Delta(B_0, \upsilon) \text{ is very confused} & \text{definition}
\end{array}$$

The proof of item 6 is similar to the proof of item 4. We abbreviate "not deciding and not very confused" to "continuing". Note that if υ is continuing then all its prefixes are. This property explains the second equivalence in the following proof of item 6. There we write $u' < w$ to denote that u' is a finite prefix of w.

$$\begin{array}{lll}
& \upsilon \text{ is finitary} & \\
\iff & \Pr(\{uw \mid u \sim \upsilon,\ \text{all } u' < \upsilon w \text{ are continuing}\}) = 0 & \text{definition} \\
\iff & \Pr(\{uw \mid u \sim \upsilon,\ \forall\, u' < w : \upsilon u' \text{ is continuing}\}) = 0 & \text{see above} \\
\iff & \displaystyle\sum_{u \sim \upsilon} \sum_{s} M(u)(s_0, s) \cdot & \text{as before} \\
& \quad \cdot \Pr_s(\{w \mid \forall\, u' < w : \upsilon u' \text{ is continuing}\}) = 0 & \\
\iff & \forall\, u \sim \upsilon.\, \forall\, s : M(u)(s_0, s) = 0 \text{ or} & \text{as before} \\
& \qquad \Pr_s(\{w \mid \forall\, u' < w : \upsilon u' \text{ is continuing}\}) = 0 & \\
\iff & \forall\, (s, q) \in \Delta(B_0, \upsilon) : & \text{by (4)} \\
& \qquad \Pr_s(\{w \mid \forall\, u' < w : \upsilon u' \text{ is continuing}\}) = 0 & \\
\iff & \forall\, (s, q) \in \Delta(B_0, \upsilon) : & \text{items 2, 3, 5} \\
& \qquad \Pr_s(\{w \mid \forall\, u' < w : \Delta(B_0, \upsilon u') \text{ is continuing}\}) = 0 & \\
\iff & \forall\, (s, q) \in \Delta(B_0, \upsilon) : & \text{definitions} \\
& \qquad \Pr_s(\{u'w \mid \Delta(\Delta(B_0, \upsilon), u') \text{ is not continuing}\}) = 1 & \\
\iff & \Delta(B_0, \upsilon) \text{ is finitary} & \text{definition}
\end{array}$$

This proves item 6 and completes the proof of the lemma. ◻

B.2 Proof of Lemma 5

Here is Lemma 5 from the main body:

Lemma 5. *Let υ be an observation prefix, and B a belief.*

1. *Whether υ is enabled can be decided in P.*
2. *Whether υ (or B) is negatively deciding can be decided in P.*
3. *Whether υ (or B) is positively deciding can be decided in P.*
4. *Whether υ (or B) is confused can be decided in PSPACE.*
5. *Whether υ (or B) is very confused can be decided in PSPACE.*
6. *Whether υ (or B) is finitary can be decided in PSPACE.*

Proof. Let G be the following graph:

– the set of vertices is $S \times Q \times P$ where P is the set of prefixes of υ;
– there is an edge $(s_1, q_1, \upsilon_1) \to (s_2, q_2, \upsilon_2)$ if and only if $\upsilon_1 = o\upsilon_2$ for some o and $\Delta((s_1, q_1), o) \ni (s_2, q_2)$.

This graph G can be computed in deterministic logspace. Also note that the belief NFA can be computed in deterministic logspace.

Proof of item 1. By Lemma 4.1, we have that υ is enabled if and only if $\Delta(B_0, \upsilon) \neq \emptyset$. We have $\Delta(B_0, \upsilon) \neq \emptyset$ if and only if G has a path from (s_0, q_0, υ) to a node (s, q, ε). But graph reachability is in NL. This proves item 1.

Proof of items 2 and 3. Assume that, for a given pair (s_1, q_1), one can determine in NL whether (s_1, q_1) is negatively deciding.

– Then we can check in NL whether the belief B is *not* negatively deciding: guess $(s_1, q_1) \in B$ nondeterministically and check whether (s_1, q_1) is *not* negatively deciding. The latter can be done in NL, as NL is closed under complement. It follows that one can check in NL whether B is negatively deciding.
– Under the same assumption we can check in NL whether the observation prefix υ is negatively deciding: By Lemma 4.2 we have that υ is not negatively deciding if and only if $\Delta(B_0, \upsilon)$ is not negatively deciding. The latter can be checked in NL by following nondeterministically a path in G from (s_0, q_0, υ) to a node (s_1, q_1, ε) and then checking if (s_1, q_1) is not negatively deciding. It follows that one can check in NL whether υ is negatively deciding.

The same reasoning applies when "negatively deciding" is replaced with "positively deciding". Therefore, for items 2 and 3, it remains to show that one can determine in NL whether a given pair (s_1, q_1) is negatively (positively, respectively) deciding. We have:

$$\begin{aligned}
& (s_1, q_1) \text{ is not negatively deciding} \\
\iff & \Pr_{s_1}(L_{q_1}) > 0 \\
\iff & \exists\, u.\, \exists\, s_2 : M(u)(s_1, s_2) > 0 \text{ and } \delta(q_1, u) = f \\
\iff & \exists\, u.\, \exists\, s_2 : \Delta(\{(s_1, q_1)\}, u) \ni (s_2, f)
\end{aligned}$$

The latter can be checked in NL by nondeterministically guessing a word u letter-by-letter and by nondeterministically following, in the belief NFA, a path that is labelled by u and leads from (s_1, q_1) to a node (s_2, f). This proves item 2.

For item 3 it remains to show how to determine in NL whether a given pair (s_1, q_1) is positively deciding. We have:

$$\begin{aligned}
& (s_1, q_1) \text{ is not positively deciding} \\
\iff\ & \mathrm{Pr}_{s_1}(L_{q_1}) < 1 \\
\iff\ & \exists\, u.\, \exists\, s_2.\, \exists\, q_2 : M(u)(s_1, s_2) > 0,\ \delta(q_1, u) = q_2,\ \mathrm{Pr}_{s_2}(L_{q_2}) = 0 \\
\iff\ & \exists\, u.\, \exists\, (s_2, q_2) \in \Delta(\{(s_1, q_1)\}, u) : (s_2, q_2) \text{ is negatively deciding} \\
\iff\ & \exists\, u.\, \exists\, (s_2, q_2) \in \Delta(\{(s_1, q_1)\}, u) : (s_2, q_2) \text{ is negatively deciding}, \\
& \qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad |u| \le |S \times Q|
\end{aligned}$$

The last equivalence follows from the fact that there are at most $|S \times Q|$ different pairs of the form (s, q). Therefore, one can check in NL whether (s_1, q_1) is not positively deciding:

1. nondeterministically guess a word u letter-by-letter;
2. nondeterministically follow, in the belief NFA, a path that is labelled by u and leads from (s_1, q_1) to a node (s_2, q_2);
3. check that (s_2, q_2) is negatively deciding; we have shown previously that this can be done in NL.

This proves item 3.

Proof of item 4. By Lemma 4.4 it suffices to prove membership in PSPACE for the case where a belief B is given. For all $B \subseteq S \times Q$, define:

$$V_B \ \coloneqq\ \{uw \mid \Delta(B, u) \text{ is deciding}\}$$

We first prove the following claim:

Claim. For given s and $B \subseteq S \times Q$ one can determine in PSPACE whether $\mathrm{Pr}_s(V_B) = 0$.

We prove the claim. We have:

$$\begin{aligned}
& \mathrm{Pr}_s(V_B) > 0 \\
\iff\ & \exists\, u.\, \exists\, s' : M(u)(s, s') > 0,\ \Delta(B, u) \text{ is deciding} \\
\iff\ & \exists\, u.\, \exists\, s' : M(u)(s, s') > 0,\ \Delta(B, u) \text{ is deciding},\ |u| \le 2^{|S \times Q|}
\end{aligned}$$

The last equivalence follows from the fact that there are at most $2^{|S \times Q|}$ different beliefs of the form $\Delta(B, u)$. Therefore, one can check in NPSPACE = PSPACE whether $\mathrm{Pr}_s(V_B) > 0$:

1. guess a word $u = a_1 \cdots a_n$ with $n \le 2^{|S \times Q|}$ letter-by-letter and check that there are states $s_1, \ldots, s_n$ with $M(a_1)(s, s_1) > 0$ and $M(a_{i+1})(s_i, s_{i+1}) > 0$ for all $i \in \{1, \ldots, n-1\}$;
2. compute, on the fly, the belief $B' \coloneqq \Delta(B, u) = \Delta(\cdots \Delta(\Delta(B, a_1), a_2) \cdots a_n)$;
3. check that B' is deciding; we have shown in items 2 and 3 that this can be done in polynomial time.

Since PSPACE is closed under complement, we have proved the claim.

Towards item 4, let B be any belief. We have:

$$
\begin{aligned}
& B \text{ is confused} \\
\iff\ & \exists\,(s,q) \in B : \Pr_s(V_B) < 1 \\
\iff\ & \exists\,(s,q) \in B.\, \exists\,u.\, \exists\,s' : M(u)(s,s') > 0,\ \Pr_{s'}(V_{\Delta(B,u)}) = 0 \\
\iff\ & \exists\,(s,q) \in B.\, \exists\,u.\, \exists\,s' : M(u)(s,s') > 0,\ \Pr_{s'}(V_{\Delta(B,u)}) = 0, \\
& \hspace{16em} |u| \le |S| \cdot 2^{|S \times Q|}
\end{aligned}
$$

The last equivalence follows from the fact that there are at most $|S| \cdot 2^{|S \times Q|}$ different pairs of the form $(s', \Delta(B,u))$. Therefore, one can check in NPSPACE = PSPACE whether B is confused:

1. guess a word $u = a_1 \cdots a_n$ with $n \le |S| \cdot 2^{|S \times Q|}$ letter-by-letter and check that there are states $s_1, \ldots, s_n$ with $M(a_1)(s, s_1) > 0$ and $M(a_{i+1})(s_i, s_{i+1}) > 0$ for all $i \in \{1, \ldots, n-1\}$;
2. compute, on the fly, the belief $B' := \Delta(B,u) = \Delta(\cdots \Delta(\Delta(B,a_1),a_2) \cdots a_n)$;
3. check that $\Pr_{s_n}(V_{B'}) = 0$; we have shown in the claim above that this can be done in PSPACE.

Proof of item 5. By Lemma 4.5 it suffices to prove membership in PSPACE for the case where a belief B is given. We have:

$$
\begin{aligned}
& B \text{ is not very confused} \\
\iff\ & \exists\,u : \Delta(B,u) \neq \emptyset \text{ is deciding} && \text{definition} \\
\iff\ & \exists\,u : \Delta(B,u) \neq \emptyset \text{ is deciding},\ |u| \le 2^{|S \times Q|}
\end{aligned}
$$

The last equivalence follows from the fact that there are at most $2^{|S \times Q|}$ different beliefs of the form $\Delta(B,u)$. Therefore, one can check in NPSPACE = PSPACE whether B is not very confused:

1. guess a word u with $|u| \le 2^{|S \times Q|}$ letter-by-letter and compute, on the fly, the belief $B' := \Delta(B,u)$;
2. check that $B' \neq \emptyset$ and B' is deciding; we have shown in items 2 and 3 that this can be done in polynomial time.

Since PSPACE is closed under complement, we have proved item 5.

Proof of item 6. By Lemma 4.6 it suffices to prove membership in PSPACE for the case where a belief B is given. The proof is analogous to the one of item 4. We abbreviate "deciding or very confused" to "dv". For all $B \subseteq S \times Q$, define:

$$
W_B \ := \ \{uw \mid \Delta(B,u) \text{ is dv}\}
$$

We first prove the following claim:

Claim. For given s and $B \subseteq S \times Q$ one can determine in PSPACE whether $\Pr_s(W_B) = 0$.

We prove the claim. We have:

$$\begin{aligned} & \Pr_s(W_B) > 0 \\ \iff & \exists\, u.\, \exists\, s' : M(u)(s,s') > 0,\ \ \Delta(B,u) \text{ is dv} \\ \iff & \exists\, u.\, \exists\, s' : M(u)(s,s') > 0,\ \ \Delta(B,u) \text{ is dv},\ |u| \le 2^{|S \times Q|} \end{aligned}$$

The last equivalence follows from the fact that there are at most $2^{|S \times Q|}$ different beliefs of the form $\Delta(B,u)$. Therefore, one can check in NPSPACE = PSPACE whether $\Pr_s(W_B) > 0$:

1. guess a word $u = a_1 \cdots a_n$ with $n \le 2^{|S \times Q|}$ letter-by-letter and check that there are states $s_1, \ldots, s_n$ with $M(a_1)(s, s_1) > 0$ and $M(a_{i+1})(s_i, s_{i+1}) > 0$ for all $i \in \{1, \ldots, n-1\}$;
2. compute, on the fly, the belief $B' \coloneqq \Delta(B,u) = \Delta(\cdots \Delta(\Delta(B,a_1),a_2) \cdots a_n)$;
3. check that B' is dv; we have shown in items 2, 3 and 5 that this can be done in PSPACE.

Since PSPACE is closed under complement, we have proved the claim.

Towards item 6, let B be any belief. We have:

$$\begin{aligned} & B \text{ is not finitary} \\ \iff & \exists\, (s,q) \in B : \Pr_s(W_B) < 1 \\ \iff & \exists\, (s,q) \in B.\, \exists\, u.\, \exists\, s' : M(u)(s,s') > 0,\ \Pr_{s'}(W_{\Delta(B,u)}) = 0 \\ \iff & \exists\, (s,q) \in B.\, \exists\, u.\, \exists\, s' : M(u)(s,s') > 0,\ \Pr_{s'}(W_{\Delta(B,u)}) = 0, \\ & \qquad\qquad\qquad\qquad\qquad\qquad |u| \le |S| \cdot 2^{|S \times Q|} \end{aligned}$$

The last equivalence follows from the fact that there are at most $|S| \cdot 2^{|S \times Q|}$ different pairs of the form $(s', \Delta(B,u))$. Therefore, one can check in NPSPACE = PSPACE whether B is not finitary:

1. guess a word $u = a_1 \cdots a_n$ with $n \le |S| \cdot 2^{|S \times Q|}$ letter-by-letter and check that there are states $s_1, \ldots, s_n$ with $M(a_1)(s, s_1) > 0$ and $M(a_{i+1})(s_i, s_{i+1}) > 0$ for all $i \in \{1, \ldots, n-1\}$;
2. compute, on the fly, the belief $B' \coloneqq \Delta(B,u) = \Delta(\cdots \Delta(\Delta(B,a_1),a_2) \cdots a_n)$;
3. check that $\Pr_{s_n}(W_{B'}) = 0$; we have shown in the claim above that this can be done in PSPACE.

Since PSPACE is closed under complement, we have proved item 6. $\square$

B.3 Proof of Proposition 7

Here is Proposition 7 from the main body:

Proposition 7. *There exists a diagnoser if and only if ε is not confused.*

Proof. We have:

	there exists a diagnoser	
$\iff$	there exists a policy that decides almost surely	definition of diagnoser
$\iff$	$\bullet$ decides almost surely	Lemma 1
$\iff$	$\Pr(\{w \mid w \text{ has a deciding prefix}\} = 1$	definitions
$\iff$	ε is not confused	definition of confused

□

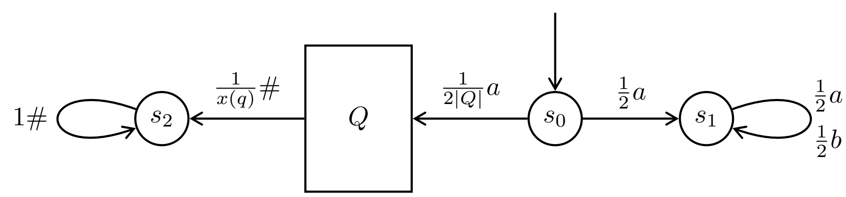
B.4 Proof of Theorem 8

Here is Theorem 8 from the main body:

Theorem 8 (cf. [2, Theorem 6]). *Given an MC $\mathcal{M}$ and a DFA $\mathcal{A}$, it is PSPACE-complete to check if there exists a diagnoser.*

Proof. By Proposition 7 it suffices to show PSPACE-completeness of checking whether ε is confused. Membership in PSPACE follows from Lemma 5.4.

For hardness we reduce from the following problem: given an NFA $\mathcal{U}$ over $\Sigma = \{a, b\}$ where all states are initial and accepting, does $\mathcal{U}$ accept all (finite) words? This problem is PSPACE-complete [9, Lemma 6]. Let $\mathcal{U} = (Q, \Sigma, \delta, Q, Q)$ be the given NFA. We construct an MC $\mathcal{M} = (Q \cup \{s_0, s_1, s_2\}, \Sigma \cup \{\#\}, M, s_0)$ where $s_0, s_1, s_2 \notin Q$, and $\# \notin \Sigma = \{a, b\}$, and the transitions are as follows:



In this picture, the rectangle labelled with Q indicates states and transitions that involve the states in Q, i.e., those coming from the NFA $\mathcal{U}$. In more detail we define:

- $M(a)(s_0, q) := \frac{1}{2|Q|}$ for all $q \in Q$;
- $x(q) := |\delta(q, a) \cup \delta(q, b)| + 1$ for all $q \in Q$;
- $M(\sigma)(q, q') := \frac{1}{x(q)}$ for all $q \in Q$ and both $\sigma \in \{a, b\}$ and all $q' \in \delta(q, \sigma)$;
- $M(\#)(q, s_2) := \frac{1}{x(q)}$ for all $q \in Q$.

Define $\mathcal{A}$ to be a DFA that accepts $L = \Sigma^*\{\#\}(\Sigma \cup \{\#\})^*$. We show that ε is confused if and only if $\mathcal{U}$ accepts all words.

Suppose $\mathcal{U}$ does not accept the word $u \in \Sigma^*$. Then one of the following two events happens almost surely, depending on whether $\mathcal{M}$ takes the left or the right transition in the first step:

- $\mathcal{M}$ emits $au_0\#$ for some $u_0 \in \Sigma^*$;

– $\mathcal{M}$ emits au_0u for some $u_0 \in \Sigma^*$.

We claim that both $au_0\#$ and au_0u are deciding, implying that ε is not confused. It is clear that $au_0\#$ is positively deciding. We argue that au_0u is negatively deciding. Indeed, since $\mathcal{U}$ does not accept u, we have $\delta(q, u) = \emptyset$ for all $q \in Q$. Hence, starting from any $q \in Q$, the MC $\mathcal{M}$ cannot emit u. So if $\mathcal{M}$ emits au_0u, it must have taken the right transition in the first step and thus will never emit $\#$, which means that au_0u is negatively deciding.

Conversely, suppose that ε is not confused. Then, almost surely, $\mathcal{M}$ emits a deciding prefix u'. By our construction, the word u' is positively deciding with probability $\frac{1}{2}$, and negatively deciding with probability $\frac{1}{2}$ (depending on which transition $\mathcal{M}$ takes in the first step). Hence there exists $u \in \Sigma^*$ such that au is negatively deciding. So $\mathcal{M}$ cannot take the left transition in the first step and then emit u. It follows that there is no $q \in Q$ with $\delta(q, u) \neq \emptyset$, i.e., $\mathcal{U}$ does not accept u. □

B.5 Proof of Proposition 9

Here is Proposition 9 from the main body:

Proposition 9. *A feasible observation policy does not allow confusion.*

Proof. Suppose that ρ allows confusion, i.e., with positive probability, it produces an observation prefix $\upsilon\bot$ such that $\upsilon\bot$ is confused but υ is not. We have:

$$\begin{aligned}
&\Pr(\{w \gtrsim \upsilon \mid \bullet \text{ decides } w\}) && \\
&= \Pr(\{uw \mid u \sim \upsilon,\ uw \text{ has a deciding prefix}\}) && \text{definitions} \\
&\geq \Pr(\{uw \mid u \sim \upsilon,\ \upsilon w \text{ has a deciding prefix}\}) && \\
&= \Pr(\{uw \mid u \sim \upsilon\}) && \upsilon \text{ is not confused} \\
&= \Pr(\{w \gtrsim \upsilon\}) && \text{definition of } \gtrsim
\end{aligned} \tag{5}$$

Thus we have:

$$\begin{aligned}
&\Pr(\{w \mid \bullet \text{ decides } w,\ \rho \text{ does not decide } w\}) && \\
&\geq \Pr(\{w \gtrsim \upsilon \mid \bullet \text{ decides } w,\ \rho \text{ does not decide } w\}) && \\
&\geq \Pr(\{w \gtrsim \upsilon \mid \rho \text{ does not decide } w\}) && \text{by (5)} \\
&= \Pr(\{w \gtrsim \upsilon\bot \mid \rho \text{ does not decide } w\}) && \\
&= \Pr(\{uw \mid u \sim \upsilon\bot,\ \rho \text{ does not decide } w\}) && \text{definition of } \gtrsim \\
&= \Pr(\{uw \mid u \sim \upsilon\bot,\ \pi_\rho(uw) \text{ has no deciding prefix}\}) && \text{definition of decide} \\
&\geq \Pr(\{uw \mid u \sim \upsilon\bot,\ \upsilon\bot w \text{ has no deciding prefix}\}) && \text{definition of } \rho \\
&> 0 && \upsilon\bot \text{ is confused}
\end{aligned}$$

Hence ρ is not feasible. □

B.6 Proof of Lemma 10

Here is Lemma 10 from the main body:

Lemma 10. *If ε is finitary then* $\mathrm{Ex}(C_\circ)$ *is finite.*

Proof. We abbreviate "deciding or very confused" to "dv". Note that if a belief B is dv then all $\Delta(B, a)$ are dv. We use this to show the following similar property:

Claim. For any finitary belief B, all $\Delta(B, a)$ are finitary.

We prove the claim. Let B be a finitary belief. Then we have:

$$\begin{aligned} 1 &= \mathrm{Pr}_s(\{uw \mid \Delta(B, u) \text{ is dv}\}) \\ &= \sum_{a \in \Sigma} \sum_{s'} M(a)(s, s') \cdot \mathrm{Pr}_{s'}(\{uw \mid \Delta(B, au) \text{ is dv}\}) \end{aligned}$$

Here, the second equality follows from the property of dv mentioned above. Hence, for all $a \in \Sigma$ and all $(s', q') \in \Delta(B, a)$ we have $\mathrm{Pr}_{s'}(\{uw \mid \Delta(B, au) \text{ is dv}\}) = 1$, so $\Delta(B, a)$ is finitary for all a. This proves the claim.

Define:

$$\mathcal{F} \;\coloneqq\; \{(s, B) \in S \times 2^{S \times Q} \mid B \text{ finitary},\ \exists\, q : (s, q) \in B\}$$

For any belief B define:

$$e_{dv}(B) \;\coloneqq\; \begin{cases} 1 & \text{if } B \text{ is dv} \\ 0 & \text{otherwise} \end{cases} \tag{6}$$

For any $(s, B) \in \mathcal{F}$ and any $n \in \mathbb{N}$ define

$$c_n(s, B) \;\coloneqq\; \mathrm{Ex}_s\big(1 - D_{B,n}\big)\,, \tag{7}$$

where by Ex_s we denote the expectation with respect to Pr_s and we define $D_{B,n}(w) \coloneqq e_{dv}(\Delta(B, u_n))$ where u_n is the length-n prefix of w. We have $c_0(s, B) = 1 - e_{dv}(B)$. Further, due to the claim above, we have for all $n \in \mathbb{N}$:

$$c_{n+1}(s, B) \;=\; \sum_{a \in \Sigma} \sum_{\substack{s' \\ M(a)(s,s')>0}} M(a)(s, s') \cdot c_n(s', \Delta(B, a))$$

We may write those equations in vector form:

$$\begin{aligned} c_0^\top &= \mathbf{1}^\top - e_{dv}^\top \\ c_{n+1}^\top &= U \cdot c_n^\top \end{aligned} \tag{8}$$

where

- $e_{dv} \in \{0, 1\}^{\mathcal{F}}$ where $e_{dv}(s, B) = e_{dv}(B)$ as in (6);
- $c_n \in \mathbb{R}^{\mathcal{F}}$ where $c_n(s, B)$ is as in (7);

– $U \in [0,1]^{\mathcal{F}\times\mathcal{F}}$ where

$$U((s,B),(s',B')) \;=\; \begin{cases} \displaystyle\sum_{\substack{a\in\Sigma\\ \Delta(B,a)=B'}} M(a)(s,s') & \text{if } B \text{ is not dv} \\ 0 & \text{otherwise.} \end{cases}$$

The matrix U satisfies $U\mathbf{1}^\mathsf{T} = \mathbf{1}^\mathsf{T} - e_{dv}^\mathsf{T}$. By a straightforward induction it follows:

$$U^n\mathbf{1}^\mathsf{T} \;=\; \mathbf{1}^\mathsf{T} - \sum_{i=0}^{n-1} U^i e_{dv}^\mathsf{T} \qquad \text{for all } n\in\mathbb{N} \tag{9}$$

From the definition of finitary, for all $(s,B)\in\mathcal{F}$ there is u such that $\Pr_s(\{u\}\Sigma^\omega) > 0$ and $\Delta(B,u)$ is dv. It follows that there is $n\in\mathbb{N}$ such that $\sum_{i=0}^{n-1} U^i e_{dv}^\mathsf{T} > \mathbf{0}^\mathsf{T}$ where the inequality is strict in all entries. By (9), we have $U^n\mathbf{1}^\mathsf{T} < \mathbf{1}^\mathsf{T}$ where the inequality is strict in all entries. Hence the spectral radius of U is less than one, and so the matrix series $\sum_{n=0}^\infty U^n$ converges to a finite matrix, say $U^* \in \mathbb{R}^{\mathcal{F}\times\mathcal{F}}$.

Suppose ε is finitary. By Lemma 4.6, the belief $B_0 = \Delta(B_0,\varepsilon)$ is finitary. Hence $(s_0,B_0)\in\mathcal{F}$. Further we have:

$$\begin{aligned}
\mathrm{Ex}(C_\circ) &= \sum_{n=0}^\infty \mathrm{Ex}\big(1-D_n\big) && \text{by (1)}\\
&= \sum_{n=0}^\infty \mathrm{Ex}_{s_0}\big(1-D_{B_0,n}\big) && \text{def. of } D_n, D_{B_0,n}, \text{ Lemma 4}\\
&= \sum_{n=0}^\infty c_n(s_0,B_0) && \text{by (7)}\\
&= \sum_{n=0}^\infty \Big(U^n\big(\mathbf{1}^\mathsf{T} - e_{dv}^\mathsf{T}\big)\Big)(s_0,B_0) && \text{by (8)}\\
&= \Big(U^*\big(\mathbf{1}^\mathsf{T} - e_{dv}^\mathsf{T}\big)\Big)(s_0,B_0) && \text{definition of } U^*\\
&< \infty && U^* \text{ is finite}
\end{aligned}$$

This completes the proof. □

B.7 Proof of Lemma 11

Here is Lemma 11 from the main body:

Lemma 11. *Let ρ be a feasible observation policy. If $\Pr(C_\rho < \infty) = 1$ then ε is finitary.*

Proof. Let ρ be an observation policy. Suppose ε is not finitary and $\Pr(C_\rho < \infty) = 1$. We show that ρ is not feasible.

Observe that for any w, if $C_\rho(w) < \infty$ then there is a (unique) shortest finite prefix of w, say $\tilde{u}(w)$, such that ρ never observes a letter after $\tilde{u}(w)$. Abbreviating "deciding or very confused" to "dv", we have:

$$
\begin{aligned}
0 &< \Pr(\{w \mid \text{no prefix of } w \text{ is dv}\}) && \varepsilon \text{ is not finitary} \\
&= \Pr(\{w \mid \text{no prefix of } w \text{ is dv},\ C_\rho(w) < \infty\}) && \Pr(C_\rho < \infty) = 1 \\
&= \Pr(\{uw \mid \text{no prefix of } uw \text{ is dv},\ u = \tilde{u}(uw)\}) && \text{observation above} \\
&\le \Pr(\{uw \mid u \text{ is not dv},\ u = \tilde{u}(uw)\}) && u \text{ is a prefix of } uw \\
&= \sum_{u \text{ is not dv}} \Pr(\{uw \mid u = \tilde{u}(uw)\}) && \Sigma^* \text{ is countable}
\end{aligned}
$$

It follows that there is u that is (i) not deciding, (ii) not very confused, and (iii) such that ρ never observes a letter after u. Since u is not very confused, there is u' such that uu' is enabled and deciding. Hence $\bullet$ decides all words of the form $uu'w$. Since ρ never observes a letter after u, we have that ρ does not decide any words of the form $uu'w$. It follows:

$$
\begin{aligned}
&\Pr(\{w \mid \bullet \text{ decides } w,\ \rho \text{ does not decide } w\}) \\
\ge\ &\Pr(\{uu'w \mid \bullet \text{ decides } uu'w,\ \rho \text{ does not decide } uu'w\}) \\
=\ &\Pr(\{uu'w\}) && \text{as explained above} \\
>\ &0 && uu' \text{ is enabled}
\end{aligned}
$$

Hence ρ is not feasible. □

B.8 Proof of Proposition 12

Here is Proposition 12 from the main body:

Proposition 12. *c_{inf} is finite if and only if ε is finitary.*

Proof. Suppose ε is finitary. By Lemma 10 we then have that $\mathrm{Ex}(C_\circ)$ is finite. Hence $c_{inf} \le \mathrm{Ex}(C_\circ)$ is finite.

Conversely, suppose ε is not finitary. By Lemma 11 we then have $\Pr(C_\rho = \infty) > 0$ for all feasible observation policies. Thus $\mathrm{Ex}(C_\rho) = \infty$ holds for all feasible observation policies. Hence $c_{inf} = \infty$. □

B.9 Proof of Proposition 13

Here is Proposition 13 from the main body:

Proposition 13. *If a diagnoser exists then c_{inf} is finite.*

Proof. We have:

$$\begin{array}{lll} & \text{a diagnoser exists} & \\ \iff & \varepsilon \text{ is not confused} & \text{Prop. 7} \\ \iff & \Pr(\{w \mid \text{some prefix of } w \text{ is deciding}\}) \;=\; 1 & \text{definition} \\ \implies & \Pr(\{w \mid \text{some prefix of } w \text{ is deciding or very confused}\}) \;=\; 1 & \\ \iff & \varepsilon \text{ is finitary} & \text{definition} \\ \iff & c_{inf} \text{ is finite} & \text{Prop. 12} \end{array}$$

□

B.10 Proof of Theorem 14

Here is Theorem 14 from the main body:

Theorem 14. *Given an MC $\mathcal{M}$ and a DFA $\mathcal{A}$, it is PSPACE-complete to check if c_{inf} is finite.*

Proof. By Proposition 12 it suffices to show PSPACE-completeness of checking whether ε is finitary. Membership in PSPACE follows from Lemma 5.6.

For hardness we use the same reduction as in the proof of Theorem 8. There we reduce from the following PSPACE-complete problem: given an NFA $\mathcal{U}$ over $\Sigma = \{a, b\}$ where all states are initial and accepting, does $\mathcal{U}$ accept all (finite) words? The reduction produces an MC $\mathcal{M}$ and a DFA $\mathcal{A}$.

First we show that in the result of that reduction, no enabled word is very confused. If a word u contains the letter # then u is negatively deciding, hence not very confused. Let $u_0 \in \Sigma^*$.

- If the NFA $\mathcal{U}$ accepts all words then $au_0\#$ is enabled and positively deciding;
- if B does not accept some word u then au_0u is enabled and negatively deciding.

In either case it follows that au_0 is not very confused and also that ε is not very confused. We conclude that no enabled word is very confused.

Thus we have:

$$\begin{array}{lll} & \varepsilon \text{ is finitary} & \\ \iff & \Pr(\{w \mid \text{no prefix of } w \text{ is deciding or very confused}\}) = 0 & \text{definition} \\ \iff & \Pr(\{w \mid \text{no prefix of } w \text{ is deciding}\}) = 0 & \text{as argued} \\ \iff & \varepsilon \text{ is not confused} & \text{definition} \\ \iff & \text{NFA } \mathcal{U} \text{ does not accept all words}\,, & \end{array}$$

where the last equivalence was shown in the proof of Theorem 8. It follows that checking if c_{inf} is finite is PSPACE-complete. □

B.11 Wrong Proof of Theorem 15

Here is Theorem 15 from the main body:

Theorem 15. *Given an MC $\mathcal{M}$ and a DFA $\mathcal{A}$, it is undecidable to check if $c_{inf} < 3$, even when a diagnoser exists.*

First we give a wrong proof. This proof contains useful ideas and is similar to and simpler than the correct one, but is flawed. We point out the flaw. In § B.12 we amend the proof, making it more complicated but correct. The incorrect proof contains only ideas that feature also in the correct one; but the correct proof can be read without having read the incorrect one.

Proof (wrong). We reduce from the emptiness problem for probabilistic automata. A *probabilistic automaton (PA)* is a tuple $\mathcal{P} = (S, \Sigma, M, s_0, \eta)$ where S is a finite set of states, Σ is a finite alphabet, the mapping $M : \Sigma \to [0,1]^{S \times S}$, where $M(a)$ is stochastic for each $a \in \Sigma$, specifies the transitions, s_0 is an initial state, and $\eta \in [0,1]^S$ is a vector of acceptance probabilities. Extend M to $M : \Sigma^* \to [0,1]^{S \times S}$ as in the case of MCs. In the case of PAs, $M(u)$ is stochastic for each $u \in \Sigma^*$. For each u define $\Pr_{\mathcal{P}}(u) := e_{s_0} M(u) \eta^\top$. The probability $\Pr_{\mathcal{P}}(u)$ can be interpreted as the probability that $\mathcal{P}$ accepts u. The *emptiness problem* asks, given a PA $\mathcal{P}$, whether there is u such that $\Pr_{\mathcal{P}}(u) > \frac{1}{2}$. This problem is undecidable [10, p. 190, Theorem 6.17].

Let $\mathcal{P} = (S_{\mathcal{P}}, \Sigma_{\mathcal{P}}, M_{\mathcal{P}}, s_{0\mathcal{P}}, \eta)$ be the given PA. We will construct a DFA $\mathcal{A}$ and an MC $\mathcal{M}$ over the alphabet $\Sigma := \Sigma_{\mathcal{P}} \cup \{0, 1, ?\}$, where $0, 1, ?$ are fresh letters. Define $\mathcal{A}$ to be a DFA that accepts $L = 0(\Sigma\Sigma)^*\Sigma 1 \Sigma^\omega$. We might characterize L by saying that 1 appears on an odd position.

We construct an MC $\mathcal{M} = (S, \Sigma, M, s_0)$ with

$$S := \{s_0\} \cup (S_{\mathcal{P}} \times \{0, 1, 2, 3\}),$$

such that s_0 is a fresh state. The MC $\mathcal{M}$ initially splits randomly into a "0-copy" (with states in $S \times \{0, 2\}$) and a "1-copy" (with states in $S \times \{1, 3\}$), in either case emitting the letter 0. Formally, $M(0)(s_0, (s_{0\mathcal{P}}, 0)) = M(0)(s_0, (s_{0\mathcal{P}}, 1)) = \frac{1}{2}$. The MC $\mathcal{M}$ is constructed such that if it goes into the 0-copy then surely it emits an infinite word that is not in L; and if it goes into the 1-copy then almost surely it emits an infinite word in L. Therefore, for an observation policy it suffices to identify which copy $\mathcal{M}$ has entered.

The transitions in $\mathcal{M}$ depend on $M_{\mathcal{P}}$ and η. In Figure 2 we illustrate this dependence with an example, where $\Sigma_{\mathcal{P}} = \{a, b\}$. For all $s, t \in S_{\mathcal{P}}$ and both $i \in \{0, 1\}$ we have the following transitions:

$$\begin{aligned} M(a)((s, i+2), (t, i)) &:= \frac{2}{3} \cdot \frac{1}{|\Sigma_{\mathcal{P}}|} \cdot M_{\mathcal{P}}(a)(s, t) \qquad\qquad \forall\, a \in \Sigma_{\mathcal{P}} \\ M(i)((s, i+2), (t, i)) &:= \frac{1}{3} \cdot \frac{1}{|\Sigma_{\mathcal{P}}|} \cdot \sum_{a \in \Sigma_{\mathcal{P}}} M_{\mathcal{P}}(a)(s, t) \end{aligned}$$

Note that any state $(s, i+2)$ emits, with probability $\frac{1}{3}$, the letter i (thus giving away in which copy $\mathcal{M}$ is), or, with probability $\frac{2}{3}$, a letter in $\Sigma_{\mathcal{P}}$ that is chosen

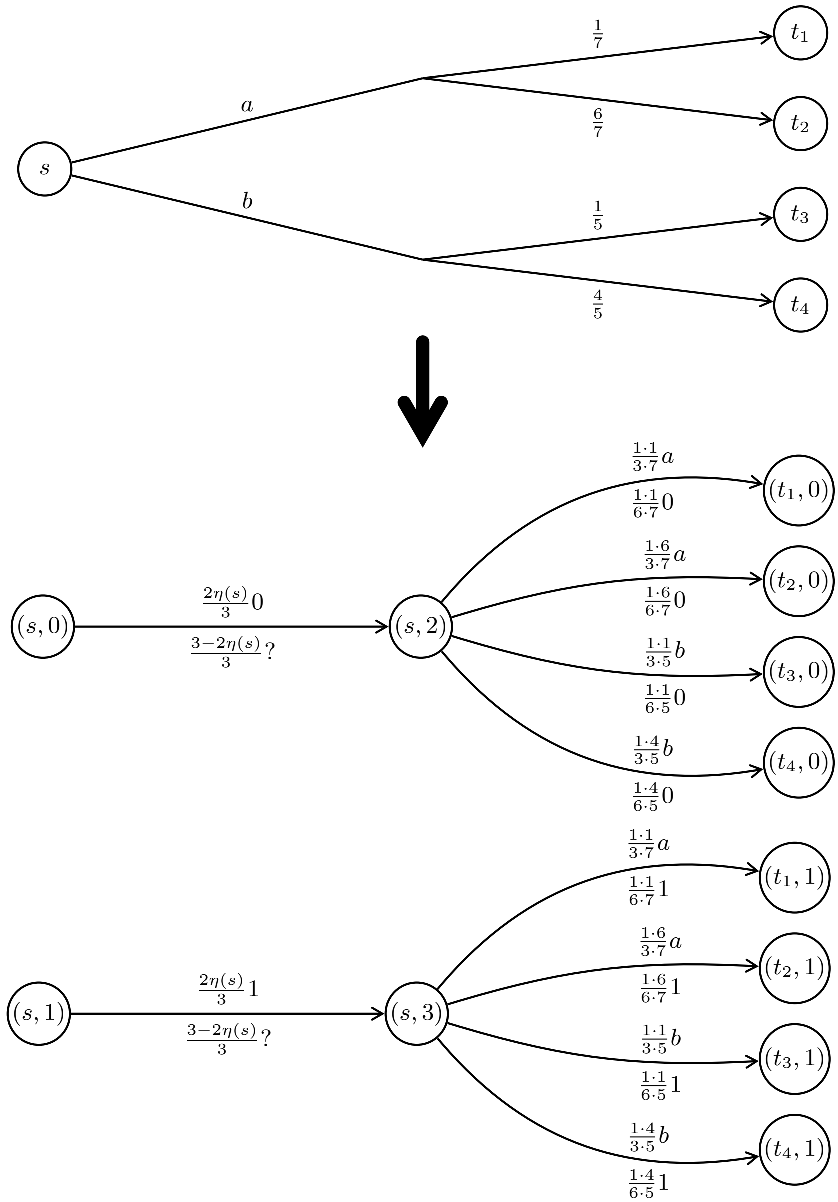


Fig. 2. Illustration of the wrong reduction. The PA at the top has a state s whose outgoing transitions are such that $M(a)(s,t_1) = \frac{1}{7}$, $M(a)(s,t_2) = \frac{6}{7}$, $M(b)(s,t_3) = \frac{1}{5}$, $M(b)(s,t_4) = \frac{4}{5}$. The resulting MC has two corresponding states, $(s,0)$ and $(s,1)$. From such a state (s,i) it first emits, with a probability depending on $\eta(s)$, either the letter i (thus giving away in which copy the MC is) or the letter ?, and then emits, with probability $\frac{1}{3}$, the letter i (thus giving away in which copy the MC is), or, with probability $\frac{2}{3} \cdot \frac{1}{|\Sigma_{\mathcal{P}}|} = \frac{1}{3}$ each, the letters a or b.

uniformly at random. (Thus, if $|\Sigma_{\mathcal{P}}| = 2$, all letters in $\Sigma_{\mathcal{P}} \cup \{i\}$ have probability $\frac{1}{3}$.) In more detail, one can view the behaviour of $\mathcal{M}$ in a state $(s, i+2)$ as follows: $\mathcal{M}$ first samples a letter a from $\Sigma_{\mathcal{P}}$ uniformly at random, then samples a successor state from $S \times \{i\}$ (each (t, i) with probability $M_{\mathcal{P}}(a)(s, t)$), and then, upon transitioning to (t, i), emits, with probability $\frac{2}{3}$, the sampled letter a, or, with probability $\frac{1}{3}$, the letter i. This completes the description of the construction.

There exists a diagnoser: Consider the policy $\overline{\rho}$, which, after the initial 0, observes every 2nd letter; each time this letter will be either from $\Sigma_{\mathcal{P}}$ (with probability $\frac{2}{3}$) or from $\{0, 1\}$ (with probability $\frac{1}{3}$). With probability 1 the latter case occurs eventually. Once it has occurred, the copy has been revealed; thus the observation prefix becomes deciding and $\overline{\rho}$ stops making any observations. The required number of observations under $\overline{\rho}$ is geometrically distributed, with expectation $1/\frac{1}{3} = 3$. Hence $\mathrm{Ex}(C_{\overline{\rho}}) = 3$ and thus $c_{inf} \leq 3$.

It remains to show that $c_{inf} < 3$ if and only if there is u such that $\Pr_{\mathcal{P}}(u) > \frac{1}{2}$. Suppose u_0 is such that $\Pr_{\mathcal{P}}(u_0) > \frac{1}{2}$. Consider the following policy ρ_0:

- do not observe the initial 0 and then observe every 2nd letter until either the prefix is deciding (because 0 or 1 has been observed) or the observation prefix becomes equal to u_0;
- in the former case: stop observing forever;
- in the latter case: observe the immediately following letter;
  - if this letter is 0 or 1 then the observation prefix has become deciding, so stop observing;
  - if this letter is ? then observe the next letter and then every 2nd letter as before.

This policy coincides mostly with the diagnoser $\overline{\rho}$ described above. It only deviates if and when u_0 has been observed. One can show that this deviation improves the expected cost: the conditional probability that 0 or 1 (hence not the letter ?) will be observed conditioned under having observed u_0 is equal to $\frac{2}{3} \cdot \Pr_{\mathcal{P}}(u_0) > \frac{2}{3} \cdot \frac{1}{2} > \frac{1}{3}$. It follows that $c_{inf} < 3$.

It remains to show the converse. To this end, suppose all u satisfy $\Pr_{\mathcal{P}}(u) \leq \frac{1}{2}$. Then one is tempted to think that it is not beneficial to deviate from the diagnoser $\overline{\rho}$ described above: conditioned under having observed some observation prefix u using $\overline{\rho}$, the conditional probability that the immediately following letter is 0 or 1 (hence not the letter ?) is equal to $\frac{2}{3} \cdot \Pr_{\mathcal{P}}(u) \leq \frac{2}{3} \cdot \frac{1}{2} \leq \frac{1}{3}$, so not better than what one would get by proceeding with $\overline{\rho}$.

The last argument is flawed though; it is valid only for the very first deviation from $\overline{\rho}$. Indeed, suppose there is some u_0 with $\Pr_{\mathcal{P}}(u_0) = \frac{1}{2}$. Suppose further we follow $\overline{\rho}$ until the observation prefix is u_0. At this point it does not come with a risk to observe the immediately following letter, as the probability to observe 0 or 1 is $\frac{1}{3}$, which is equal to the success probability of each single observation of $\overline{\rho}$. Suppose we do that and observe ?. Now we have not learned anything about which copy the MC is in; however, after this observation, the conditional probability (conditioned on all observations so far) that we are in a state $(s, 2)$ or $(s, 3)$ with *low* $\eta(s)$ has increased, as a state (s, i) with high $\eta(s)$ would probably have produced the letter i instead of ?. This information might be exploitable later: For instance, suppose that the PA is such that states s with low and high values of $\eta(s)$ alternate. Then in the next round we believe to be in a state (s, i) with high $\eta(s)$. Now it might be beneficial to make another non-$\overline{\rho}$ observation, even if $\Pr_{\mathcal{P}}(u_0 a) \le \frac{1}{2}$ holds for all $a \in \Sigma_{\mathcal{P}}$.

To fix this problem we need to change the construction in a way that a single deviation from $\overline{\rho}$ leaks less information. We do this in the following § B.12. $\square$

B.12 Correct Proof of Theorem 15

Here is Theorem 15 from the main body:

Theorem 15. *Given an MC $\mathcal{M}$ and a DFA $\mathcal{A}$, it is undecidable to check if $c_{inf} < 3$, even when a diagnoser exists.*

Proof. We reduce from the emptiness problem for probabilistic automata. A *probabilistic automaton (PA)* is a tuple $\mathcal{P} = (S, \Sigma, M, s_0, \eta)$ where S is a finite set of states, Σ is a finite alphabet, the mapping $M : \Sigma \to [0, 1]^{S \times S}$, where $M(a)$ is stochastic for each $a \in \Sigma$, specifies the transitions, s_0 is an initial state, and $\eta \in [0, 1]^S$ is a vector of acceptance probabilities. Extend M to $M : \Sigma^* \to [0, 1]^{S \times S}$ as in the case of MCs. In the case of PAs, $M(u)$ is stochastic for each $u \in \Sigma^*$. For each u define $\Pr_{\mathcal{P}}(u) := e_{s_0} M(u) \eta^\top$. The probability $\Pr_{\mathcal{P}}(u)$ can be interpreted as the probability that $\mathcal{P}$ accepts u. The *emptiness problem* asks, given a PA $\mathcal{P}$, whether there is u such that $\Pr_{\mathcal{P}}(u) > \frac{1}{2}$. This problem is undecidable [10, p. 190, Theorem 6.17].

We assume that for all u there is s with $M(u)(s_0, s) > 0$ and $0 < \eta(s) < 1$. This is without loss of generality, as we can make the PA branch, in its first transition and with positive probability, to a sub-PA with a single state from which every word is accepted with probability $\frac{1}{2}$. Formally, from the original PA $\mathcal{P} = (S, \Sigma, M, s_0, \eta)$ obtain another PA $\mathcal{P}' = (S' \cup \{t_0, t\}, \Sigma, M', t_0, \eta')$ where:

- t_0, t are fresh states;
- $\eta'(t_0) := \eta(s_0)$ and $\eta'(t) := \frac{1}{2}$ and $\eta'(s) := \eta(s)$ for all s;
- $M'(a)(t_0, t) := \frac{1}{2}$ and $M'(a)(t, t) := 1$ for all $a \in \Sigma$;
- $M'(a)(t_0, s) := \frac{1}{2} M(a)(s_0, s)$ for all $a \in \Sigma$ and all s;
- $M'(a)(s, s') = M(a)(s, s')$ for all s, s'.

We have for all u that $\Pr_{\mathcal{P}'}(u) - \frac{1}{2} = \frac{1}{2}(\Pr_{\mathcal{P}}(u) - \frac{1}{2})$. It follows that $\Pr_{\mathcal{P}}(u) > \frac{1}{2}$ if and only if $\Pr_{\mathcal{P}'}(u) > \frac{1}{2}$.

Let $\mathcal{P} = (S_{\mathcal{P}}, \Sigma_{\mathcal{P}}, M_{\mathcal{P}}, s_{0\mathcal{P}}, \eta)$ be the given PA. We will construct a DFA $\mathcal{A}$ and an MC $\mathcal{M}$ over the alphabet $\Sigma := \Sigma_{\mathcal{P}} \cup \{0, 1\}$, where $0, 1$ are fresh letters. Define $\mathcal{A}$ to be a DFA that accepts $L = 0(\Sigma\Sigma\Sigma\Sigma\Sigma)^* \Sigma\Sigma\Sigma\Sigma 1 \Sigma^\omega$. Ignoring the very first letter 0, we might characterize L by saying that 1 appears on a position that is divisible by 5.

We construct an MC $\mathcal{M} = (S, \Sigma, M, s_0)$ with

$$S := \{s_0\} \cup (S_{\mathcal{P}} \times \{0, 1, 2, 3\}) \cup \tilde{S},$$

such that s_0 and the states in $\tilde{S}$ are fresh states. The MC $\mathcal{M}$ initially splits randomly into a "0-copy" (with states in $S \times \{0,2\}$) and a "1-copy" (with states in $S \times \{1,3\}$), in either case emitting the letter 0. Formally, $M(0)(s_0,(s_{0\mathcal{P}},0)) = M(0)(s_0,(s_{0\mathcal{P}},1)) = \frac{1}{2}$. The MC $\mathcal{M}$ is constructed such that if it goes into the 0-copy then surely it emits an infinite word that is not in L; and if it goes into the 1-copy then almost surely it emits an infinite word in L. Therefore, for an observation policy it suffices to identify which copy $\mathcal{M}$ has entered.

The transitions in $\mathcal{M}$ depend on $M_{\mathcal{P}}$ and η. In Figure 3 we illustrate this dependence with an example, where $\Sigma_{\mathcal{P}} = \{a,b\}$.

Formally, for all $(s,i) \in S_{\mathcal{P}} \times \{0,1\}$ we define transitions (using states in $\tilde{S}$ that are not further specified) such that:

$$
\begin{aligned}
M(0000)((s,0),(s,2)) &= \eta(s)/4 & M(0101)((s,0),(s,2)) &= (1-\eta(s))/4\\
M(0001)((s,0),(s,2)) &= \eta(s)/4 & M(0110)((s,0),(s,2)) &= (1-\eta(s))/4\\
M(0010)((s,0),(s,2)) &= \eta(s)/4 & M(1001)((s,0),(s,2)) &= (1-\eta(s))/4\\
M(0011)((s,0),(s,2)) &= \eta(s)/4 & M(1010)((s,0),(s,2)) &= (1-\eta(s))/4\\
M(1100)((s,1),(s,3)) &= \eta(s)/4 & M(0100)((s,1),(s,3)) &= (1-\eta(s))/4\\
M(1101)((s,1),(s,3)) &= \eta(s)/4 & M(0111)((s,1),(s,3)) &= (1-\eta(s))/4\\
M(1110)((s,1),(s,3)) &= \eta(s)/4 & M(1000)((s,1),(s,3)) &= (1-\eta(s))/4\\
M(1111)((s,1),(s,3)) &= \eta(s)/4 & M(1011)((s,1),(s,3)) &= (1-\eta(s))/4
\end{aligned}
\tag{10}
$$

These 4-bit sequences (henceforth "blocks") are chosen such that if the first two bits agree (say they are both $b \in \{0,1\}$) then $\mathcal{M}$ is in the b-copy; if the first two bits of a block do not agree then the xor of all four bits (equivalently, the parity of the sum of the four bits) identifies in which copy $\mathcal{M}$ is. States (s,i) with higher acceptance probability $\eta(s)$ have a higher chance to emit a block where the first two bits agree. The intention of this construction is to make it cost-efficient for an observation policy to observe (some) letters of a block when the policy believes that it is in a state (s,i) with high $\eta(s)$. We will show later that this is beneficial on some runs if and only if there is u with $\Pr_{\mathcal{P}}(u) > \frac{1}{2}$.

The other transitions of $\mathcal{M}$ are as follows: For all $s,t \in S_{\mathcal{P}}$ and both $i \in \{0,1\}$ we have the following transitions:

$$
\begin{aligned}
M(a)((s,i+2),(t,i)) &\coloneqq \frac{2}{3} \cdot \frac{1}{|\Sigma_{\mathcal{P}}|} \cdot M_{\mathcal{P}}(a)(s,t) & \forall\, a \in \Sigma_{\mathcal{P}}\\
M(i)((s,i+2),(t,i)) &\coloneqq \frac{1}{3} \cdot \frac{1}{|\Sigma_{\mathcal{P}}|} \cdot \sum_{a \in \Sigma_{\mathcal{P}}} M_{\mathcal{P}}(a)(s,t)
\end{aligned}
$$

Note that any state $(s,i+2)$ emits, with probability $\frac{1}{3}$, the letter i (thus giving away in which copy $\mathcal{M}$ is), or, with probability $\frac{2}{3}$, a letter in $\Sigma_{\mathcal{P}}$ that is chosen uniformly at random. (Thus, if $|\Sigma_{\mathcal{P}}| = 2$, all letters in $\Sigma_{\mathcal{P}} \cup \{i\}$ have probability $\frac{1}{3}$.) In more detail, one can view the behaviour of $\mathcal{M}$ in a state $(s,i+2)$ as follows: $\mathcal{M}$ first samples a letter a from $\Sigma_{\mathcal{P}}$ uniformly at random, then samples a successor state from $S \times \{i\}$ (each (t,i) with probability $M_{\mathcal{P}}(a)(s,t)$), and then, upon

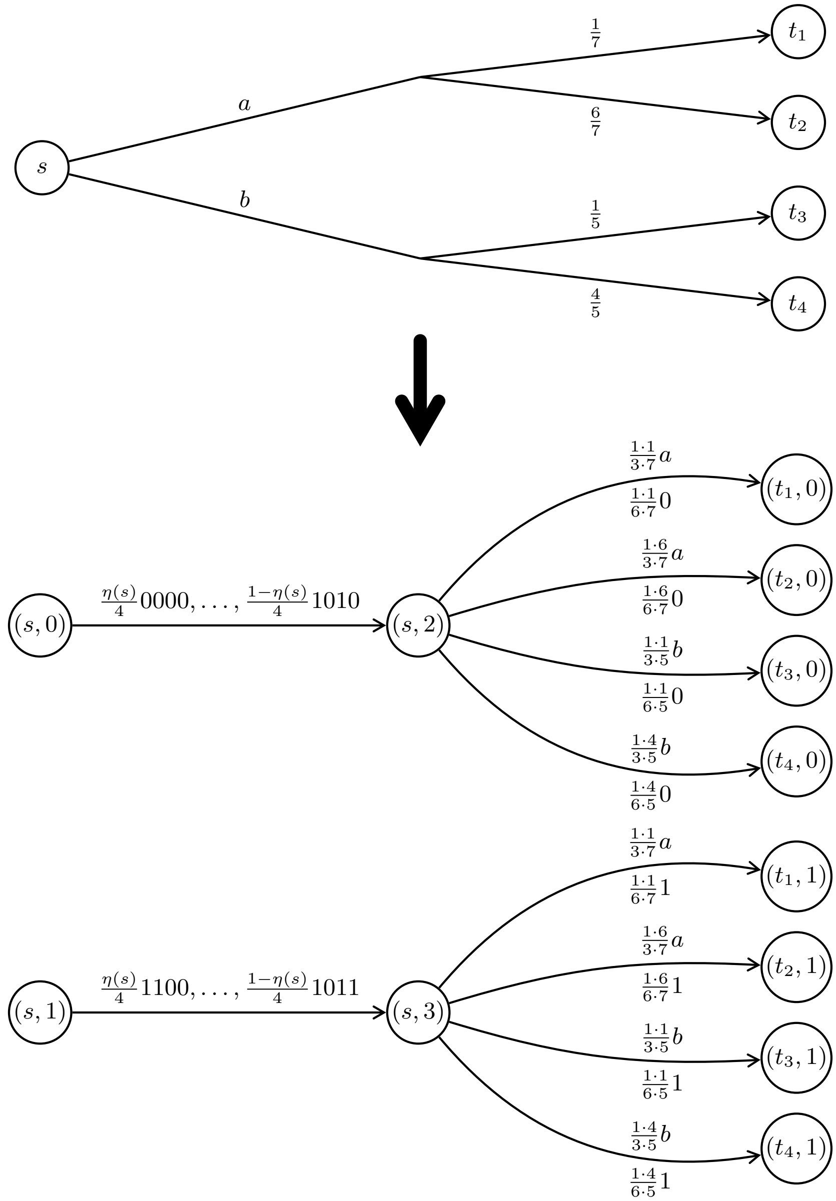


Fig. 3. Illustration of the reduction. The PA at the top has a state s whose outgoing transitions are such that $M(a)(s,t_1) = \frac{1}{7}$, $M(a)(s,t_2) = \frac{6}{7}$, $M(b)(s,t_3) = \frac{1}{5}$, $M(b)(s,t_4) = \frac{4}{5}$. The resulting MC has two corresponding states, $(s,0)$ and $(s,1)$. From such a state (s,i) it first emits, with a probability depending on $\eta(s)$, a 4-bit sequence ("block"), and then emits, with probability $\frac{1}{3}$, the letter i (thus giving away in which copy the MC is), or, with probability $\frac{2}{3} \cdot \frac{1}{|\Sigma_{\mathcal{P}}|} = \frac{1}{3}$ each, the letters a or b.

transitioning to (t, i), emits, with probability $\frac{2}{3}$, the sampled letter a, or, with probability $\frac{1}{3}$, the letter i. This completes the description of the construction.

There exists a diagnoser: Consider the policy $\overline{\rho}$, which, after the initial 0, observes every 5th letter; each time this letter will be either from $\Sigma_{\mathcal{P}}$ (with probability $\frac{2}{3}$) or from $\{0, 1\}$ (with probability $\frac{1}{3}$). With probability 1 the latter case occurs eventually. Once it has occurred, the copy has been revealed; thus the observation prefix becomes deciding and $\overline{\rho}$ stops making any observations. The required number of observations under $\overline{\rho}$ is geometrically distributed, with expectation $1/\frac{1}{3} = 3$. Hence $\mathrm{Ex}(C_{\overline{\rho}}) = 3$ and thus $c_{inf} \leq 3$.

It remains to show that $c_{inf} < 3$ if and only if there is u such that $\Pr_{\mathcal{P}}(u) > \frac{1}{2}$. Suppose u_0 is such that $\Pr_{\mathcal{P}}(u_0) > \frac{1}{2}$. Consider the following policy ρ_0:

- do not observe the initial 0 and then observe every 5th letter until either the prefix is deciding (because 0 or 1 has been observed) or the observation prefix becomes equal to u_0;
- in the former case: stop observing forever;
- in the latter case: observe the first two letters of the following block;
  - if they agree then the observation prefix has become deciding, so stop observing;
  - if they do not agree, observe also the next two letters; this produces a deciding prefix, so stop observing.

This policy coincides mostly with the diagnoser $\overline{\rho}$ described above. It only deviates if and when u_0 has been observed. We show that this deviation improves the expected cost.

To argue in more formal terms, we extend (for the PA $\mathcal{P}$) the mapping $M_{\mathcal{P}} : \Sigma_{\mathcal{P}}^* \to [0,1]^{S_{\mathcal{P}} \times S_{\mathcal{P}}}$ to $M_{\mathcal{P}} : (\Sigma_{\mathcal{P}} \cup \{\perp\})^* \to [0,1]^{S_{\mathcal{P}} \times S_{\mathcal{P}}}$ by defining

$$\begin{aligned} M_{\mathcal{P}}(\upsilon) &\coloneqq \sum_{u \sim \upsilon} M_{\mathcal{P}}(u) \Big/ |\{u \mid u \sim \upsilon\}| \qquad\qquad \text{and define} \\ \mu_{\mathcal{P}}(\upsilon) &\coloneqq e_{s_{0\mathcal{P}}} M_{\mathcal{P}}(\upsilon)\ . \end{aligned}$$

One can view the distribution $\mu_{\mathcal{P}}(\upsilon)$ as the expected distribution after having fed the PA $\mathcal{P}$ with a randomly sampled $u \sim \upsilon$. Similarly, we extend (for the MC $\mathcal{M}$) the mapping $M : \Sigma^* \to [0,1]^{S \times S}$ to $M : \Sigma_{\perp}^* \to [0,1]^{S \times S}$ by defining

$$\begin{aligned} M(\upsilon) &\coloneqq \sum_{u \sim \upsilon} M(u) \qquad\qquad\qquad\qquad \text{and define} \\ \mu(\upsilon) &\coloneqq \frac{e_{s_0} M(\upsilon)}{e_{s_0} M(\upsilon) \mathbf{1}^{\mathsf{T}}}\ . \end{aligned}$$

One can view the distribution $\mu(\upsilon)$ as the expected distribution after having observed υ. Finally, for any finite word $\upsilon = o_1 o_2 \cdots o_n \in (\Sigma_{\mathcal{P}} \cup \{\perp\})^*$ define the following padding:

$$\widehat{\upsilon} \coloneqq \begin{cases} \perp & \text{if } n = 0 \\ \perp\perp\perp\perp\perp o_1 \perp\perp\perp\perp o_2 \perp\perp\perp\perp o_3 \cdots \perp\perp\perp\perp o_n & \text{if } n \geq 1 \end{cases}$$

With these definitions, it is straightforward to check that we have:

$$\frac{1}{2}\mu_{\mathcal{P}}(\upsilon)(s) \;=\; \mu(\widehat{\upsilon})((s,0)) \;=\; \mu(\widehat{\upsilon})((s,1)) \qquad \forall\, \upsilon \in (\Sigma_{\mathcal{P}} \cup \{\perp\})^* \;\forall\, s \in S_{\mathcal{P}} \tag{11}$$

For the word u_0 from above we have $\mu_{\mathcal{P}}(u_0)\eta^{\mathsf{T}} = \Pr_{\mathcal{P}}(u_0) > \frac{1}{2}$. It follows from (11) and (10) that, conditioned under prefix $\widehat{u_0}$, the conditional probability of emitting 00 or 11 at the beginning of the following block is greater than $\frac{1}{2}$; formally:

$$\Pr(\{u00, u11\}\Sigma^\omega \mid u \sim \widehat{u_0}\} \mid \{w \gtrsim \widehat{u_0}\}) \;=\; \mu_{\mathcal{P}}(u_0)\eta^{\mathsf{T}} \;>\; \frac{1}{2}$$

Recall that ρ_0 is defined so that once it has observed $\widehat{u_0}$, it makes either exactly 2 or exactly 4 further observations. From the previous inequality it follows for ρ_0 that, conditioned under observing $\widehat{u_0}$, the conditional probability to make exactly 2 further observations is greater than the conditional probability to make exactly 4 further observations. Hence, the conditional expected number of observations after having observed u_0 is less than 3.

More formally, for any policy ρ and an observation prefix $\upsilon = o_1 \cdots o_k$ define a random variable C_ρ^υ by

$$C_\rho^\upsilon(w) \;\coloneqq\; C_\rho(w) - \sum_{k=0}^{|\upsilon|-1} \rho(o_1 \ldots o_k) \qquad \text{for all } w \gtrsim \upsilon\,,$$

i.e., C_ρ^υ is the number of observations that ρ makes after υ. By the argument above we have $\mathrm{Ex}(C_{\rho_0}^{\widehat{u_0}} \mid \{w \gtrsim \widehat{u_0}\}) < 3$. For all u that are not prefixes of u_0 we have $\mathrm{Ex}(C_{\rho_0}^{\widehat{u}} \mid \{w \gtrsim \widehat{u}\}) = 3$. It follows $\mathrm{Ex}(C_{\rho_0}) < 3$. Hence $c_{\mathit{inf}} < 3$.

It remains to show the converse. To this end, suppose all u satisfy $\Pr_{\mathcal{P}}(u) \leq \frac{1}{2}$. It suffices to show that all feasible policies ρ satisfy $\mathrm{Ex}(C_\rho) \geq 3$.

In the following we use regular expressions to describe observation prefixes. For improved readability we may indicate the borders of a block with a dot. For instance, the regular expression

$$\perp(.\perp^4.(\Sigma_{\mathcal{P}} + \perp))^*.0\perp\perp\perp.$$

indicates observation prefixes of the following form: first all observations (if any) are made in non-blocks and are in $\Sigma_{\mathcal{P}}$ (i.e., are not 0 or 1), and then 0 is observed at the beginning of a block, and the other three letters in the block are not observed.

We call $k \in (0{+}1{+}\perp)^4$ *block-deciding* when $k \in (0{+}1)^4 + (00{+}11)(0{+}1{+}\perp)^2$. We have the following lemma:

Lemma 30. *Let υ be an observation prefix that is not deciding and satisfies $|\upsilon| = 1 + 5n$ for some $n \in \mathbb{N}$. Let $k \in (0 + 1 + \perp)^4$. Then $\upsilon.k.$ is deciding if and only if k is block-deciding.*

Proof (of the lemma). Let υ and k be as in the statement. Suppose k is block-deciding. Then, by inspecting (10), it follows that $\upsilon.k.$ is deciding.

Conversely, suppose k is not block-deciding. From the assumption made about $\mathcal{P}$ in the beginning we obtain that there is $s \in S_{\mathcal{P}}$ with $0 < \eta(s) < 1$ such that $M(\upsilon)(s_0, (s, 0)) > 0$ and $M(\upsilon)(s_0, (s, 1)) > 0$. By inspecting (10), it follows that $\upsilon.k.$ is not deciding. $\square$

Let ρ be any feasible policy, and let υ be an observation prefix that ρ produces with positive probability.

1. Suppose $\upsilon \in \bot(.\bot^4.(\Sigma_{\mathcal{P}}+\bot))^*.k.(\bot^5)^*(\Sigma_{\mathcal{P}}+\bot)(\bot^5)^*.\ell$ where $k \in (0+1+\bot)^4$ is not block-deciding, and $\ell \in (0+1+\bot)^{\leq 4}$ has exactly one observation. By Lemma 30 the prefix up to and including k is not deciding. Another application of Lemma 30 shows that υ is not deciding, so $\mathrm{Ex}(C_\rho^\upsilon) \geq 1$.
2. Suppose $\upsilon \in \bot(.\bot^4.(\Sigma_{\mathcal{P}}+\bot))^*.k.(\bot^5)^*\Sigma_{\mathcal{P}}$ where $k \in (0+1+\bot)^4$ is not block-deciding. Similarly as before, it follows that υ is not deciding.
   - Suppose the next observation that ρ makes is in a block. Then, by item 1, we have $\mathrm{Ex}(C_\rho^\upsilon) \geq 1+1 = 2$.
   - Otherwise the next observation is in a non-block. If this observation yields 0 or 1 (which happens with probability $\frac{1}{3}$) then no further observation is needed; otherwise, a further observation will be needed. So $\mathrm{Ex}(C_\rho^\upsilon) \geq 1 + \frac{1}{3}\cdot 0 + \frac{2}{3}\cdot 1 \geq \frac{5}{3}$.

   Thus, in either case we have $\mathrm{Ex}(C_\rho^\upsilon) \geq \frac{5}{3}$.
3. Suppose $\upsilon \in \bot(.\bot^4.(\Sigma_{\mathcal{P}}+\bot))^*.k.$ where $k \in (0+1+\bot)^4$ is not block-deciding. Similarly as before, it follows that υ is not deciding.
   - Suppose the next observation that ρ makes is in a block. Then, by item 1, we have $\mathrm{Ex}(C_\rho^\upsilon) \geq 1+1 = 2$.
   - Otherwise the next observation is in a non-block. If this observation yields 0 or 1 (which happens with probability $\frac{1}{3}$) then no further observation is needed; otherwise, the resulting observation prefix will have the form from item 2. It follows from item 2 that $\mathrm{Ex}(C_\rho^\upsilon) \geq 1 + \frac{1}{3}\cdot 0 + \frac{2}{3}\cdot\frac{5}{3} > 2$.

   Thus, in either case we have $\mathrm{Ex}(C_\rho^\upsilon) \geq 2$.
4. Suppose $\upsilon \in \bot(.\bot^4.(\Sigma_{\mathcal{P}}+\bot))^*.\bot\bot b$ for $b \in \{0,1\}$. Then υ is not deciding.
   - Suppose the next observation is not in the same block. Then the resulting observation prefix has the form from either item 1 or item 2. It follows from these items that $\mathrm{Ex}(C_\rho^\upsilon) \geq 1 + \min\{1, \frac{5}{3}\} = 2$.
   - Otherwise the next observation follows immediately and yields $b' \in \{0,1\}$. The word $\bot\bot bb'$ is not block-deciding, hence, by Lemma 30, $\upsilon b'$ is not deciding, so $\mathrm{Ex}(C_\rho^\upsilon) \geq 2$.

   Thus, in either case we have $\mathrm{Ex}(C_\rho^\upsilon) \geq 2$.
5. Suppose $\upsilon \in \bot(.\bot^4.(\Sigma_{\mathcal{P}}+\bot))^*.bb'$ for $bb' \in (0+1+\bot)^2$ and $bb' \notin 00+11$. Then υ is not deciding.
   - Suppose the next observation is not in the same block. Then the resulting observation prefix has the form from either item 1 or item 2. It follows from these items that $\mathrm{Ex}(C_\rho^\upsilon) \geq 1 + \min\{1, \frac{5}{3}\} = 2$.

- Otherwise the next observation results in an observation prefix $\upsilon\upsilon'$ with $\upsilon' \in \{0, 1, \perp 0, \perp 1\}$. No word in $\{bb'\}\{0\perp, 1\perp, \perp 0, \perp 1\}$ is block-deciding. Hence, by Lemma 30, $\upsilon\upsilon'$ is not deciding, so $\mathrm{Ex}(C_\rho^\upsilon) \geq 2$.

Thus, in either case we have $\mathrm{Ex}(C_\rho^\upsilon) \geq 2$.

6. Suppose $\upsilon \in \perp(.\perp^4.(\Sigma_\mathcal{P} + \perp))^*.b$ for $b \in \{0, 1\}$. Then υ is not deciding.
   - Suppose the next observation is not in the same block. Then the resulting observation prefix has the form from either item 1 or item 2. It follows from these items that $\mathrm{Ex}(C_\rho^\upsilon) \geq 1 + \min\{1, \frac{5}{3}\} = 2$.
   - Suppose the next observation is in the same block but does not follow immediately. This results in an observation prefix $\upsilon\perp\upsilon'$ with $\upsilon' \in \{0, 1, \perp 0, \perp 1\}$. No word in $\{b\perp\}\{0\perp, 1\perp, \perp 0, \perp 1\}$ is block-deciding. Hence, by Lemma 30, $\upsilon\upsilon'$ is not deciding, so $\mathrm{Ex}(C_\rho^\upsilon) \geq 2$.
   - Otherwise the next observation follows immediately. Let υ_0 be such that $\upsilon = \upsilon_0 b$. Then there exists $\upsilon_1 \in (\Sigma_\mathcal{P} \cup \{\perp\})^*$ with $\upsilon_0 = \widehat{\upsilon_1}$. Since all $u \in \Sigma_\mathcal{P}^*$ satisfy $\mu_\mathcal{P}(u)\eta^\mathsf{T} = \mathrm{Pr}_\mathcal{P}(u) \leq \frac{1}{2}$, we also have $\mu_\mathcal{P}(\upsilon_1)\eta^\mathsf{T} \leq \frac{1}{2}$. It follows from (11) and (10) that, conditioned under prefix υ_0, the conditional probability of emitting 00 or 11 is at most $\frac{1}{2}$; formally:

$$p \;:=\; \mathrm{Pr}(\{u00, u11\}\Sigma^\omega \mid u \sim \upsilon_0\} \mid \{w \gtrsim \upsilon_0\}) \;=\; \mu_\mathcal{P}(\upsilon_1)\eta^\mathsf{T} \;\leq\; \frac{1}{2}$$

     For symmetry reasons we must have:

$$\mathrm{Pr}(\{ub\}\Sigma^\omega \mid u \sim \upsilon\} \mid \{w \gtrsim \upsilon\}) \;=\; p \;\leq\; \frac{1}{2}$$

     In words, the conditional probability that the next observation equals b is at most $\frac{1}{2}$. If this happens then no further observation is needed, as $bb\perp\perp$ is block-deciding; otherwise, the resulting observation prefix has the form from item 5. It follows from item 5 that $\mathrm{Ex}(C_\rho^\upsilon) \geq 1 + p \cdot 0 + (1-p) \cdot 2 \geq 1 + \frac{1}{2} \cdot 2 = 2$.

   Thus, in all three cases we have $\mathrm{Ex}(C_\rho^\upsilon) \geq 2$.

Let ρ be feasible. Call an observation prefix υ *conventional* when

- υ is not deciding;
- ρ produces υ with positive probability;
- and υ does not contain observations in blocks.

Towards a contradiction, assume that $\mathrm{Ex}(C_\rho) < 3$. Then there exist a conventional observation prefix υ and $x > 0$ such that:

- $\mathrm{Ex}(C_\rho^\upsilon) \leq 3 - x$;
- and for all conventional observation prefixes υ' we have $\mathrm{Ex}(C_\rho^{\upsilon'}) > 3 - \frac{3}{2}x$.

Since ρ is feasible, there must be a non-$\perp$ observation (at some point) after υ.

– Suppose this next observation is in a non-block, resulting in an observation prefix υ'. Then υ' is either deciding (with probability $\frac{1}{3}$) or conventional (with probability $\frac{2}{3}$). It follows:

$$3 - x \;\geq\; \mathrm{Ex}(C_\rho^\upsilon) \;\geq\; 1 + \frac{1}{3} \cdot 0 + \frac{2}{3} \cdot \mathrm{Ex}(C_\rho^{\upsilon'}) \;>\; 1 + \frac{2}{3} \cdot \left(3 - \frac{3}{2}x\right) \;=\; 3 - x\,,$$

which is a contradiction.

– Otherwise, the next observation is in a block, resulting in an observation prefix υ'. Then υ' is not deciding and has the form of items 3–6 above. It follows from these items that $\mathrm{Ex}(C_\rho^\upsilon) = 1 + \mathrm{Ex}(C_\rho^{\upsilon'}) \geq 1 + 2 = 3$, contradicting that $\mathrm{Ex}(C_\rho^\upsilon) \leq 3 - x$.

In either case we have a contradiction. Hence $\mathrm{Ex}(C_\rho) \geq 3$. ◻

B.13 Proof of Lemma 19

Here is Lemma 19 from the main body:

Lemma 19. *A belief $B \subseteq S \times Q$ is confused if and only if there is $a \in \Sigma$ such that $\Delta(B, a)$ is not settled.*

Proof. Since singleton beliefs cannot be confused in a non-hidden MC, we have:

$$\mathrm{Pr}_{\overrightarrow{a}}(\{uw \mid \mathrm{Pr}_{\overrightarrow{au}}(L_{\delta(q,u)}) \in \{0,1\}\}) \;=\; 1 \quad \forall\, a\; \forall\, q \tag{12}$$

Suppose $\Delta(B, a)$ is settled for all a. Then for all a and all $(\overrightarrow{a}, q_1), (\overrightarrow{a}, q_2) \in \Delta(B, a)$ and all u with $\overrightarrow{a} \xrightarrow{u}$ we have:

$$\mathrm{Pr}_{\overrightarrow{au}}(L_{\delta(q_1,u)}) = 1 \quad\Longleftrightarrow\quad \mathrm{Pr}_{\overrightarrow{au}}(L_{\delta(q_2,u)}) = 1$$

By combining this with (12) we get:

$$\mathrm{Pr}_{\overrightarrow{a}}(\{uw \mid \Delta(B, au) \text{ is deciding}\}) \;=\; 1 \quad \forall\, a$$

Hence:

$$\mathrm{Pr}_s(\{uw \mid \Delta(B, u) \text{ is deciding}\}) \;=\; 1 \quad \forall\,(s, q) \in B$$

Hence B is not confused.

Conversely, suppose there is a such that $\Delta(B, a)$ is not settled. Then there are $(\overrightarrow{a}, q_1), (\overrightarrow{a}, q_2) \in \Delta(B, a)$ and u_0 with $\overrightarrow{a} \xrightarrow{u_0}$ such that:

$$\mathrm{Pr}_{\overrightarrow{au_0}}(L_{\delta(q_1,u_0)}) \;=\; 1 \;>\; \mathrm{Pr}_{\overrightarrow{au_0}}(L_{\delta(q_2,u_0)})$$

It follows from (12) that there is u_1 with $\overrightarrow{au_0} \xrightarrow{u_1}$ such that:

$$\mathrm{Pr}_{\overrightarrow{au_0u_1}}(L_{\delta(q_1,u_0u_1)}) \;=\; 1 \;>\; 0 \;=\; \mathrm{Pr}_{\overrightarrow{au_0u_1}}(L_{\delta(q_2,u_0u_1)})$$

Hence for all u_2 with $\overrightarrow{au_0u_1} \xrightarrow{u_2}$ we have that $(\overrightarrow{au_0u_1u_2}, \delta(q_1, u_0u_1u_2))$ is positively deciding and $(\overrightarrow{au_0u_1u_2}, \delta(q_2, u_0u_1u_2))$ is negatively deciding, and therefore also that

$$\Delta(B, au_0u_1u_2) \supseteq \{(\overrightarrow{au_0u_1u_2}, \delta(q_1, u_0u_1u_2)), (\overrightarrow{au_0u_1u_2}, \delta(q_1, u_0u_1u_2))\}$$

is not deciding. So we have:

$$\Pr_{\overrightarrow{au_0u_1}}(\{u_2w \mid \Delta(B, au_0u_1u_2) \text{ is deciding}\}) \ = \ 0$$

It follows that there is $(s, q) \in B$ with

$$\Pr_s(\{uw \mid \Delta(B, u) \text{ is deciding}\}) \ < \ 1$$

Hence B is confused. □

B.14 Proof of Lemma 25

Here is Lemma 25 from the main body:

Lemma 25. *Let $c(K, s, q)$ denote the expected cost of decision under $\rho_{pro}(K)$ starting in (s, q). For each $\varepsilon > 0$ there exists $K \in \mathbb{N}$ such that for all (s, q) with $cras(s, q) = \infty$ we have $c(K, s, q) \le 1 + \varepsilon$.*

Proof. Let $(s, q) \in S \times Q$. The singleton belief $\{(s, q)\}$ cannot be confused in a non-hidden MC, i.e., we have:

$$1 \ = \ \Pr_s(\{uaw \mid (\overrightarrow{a}, \delta(q, ua)) \text{ is deciding}\})$$

It follows that for each $p < 1$ there is $K \in \mathbb{N}$ such that

$$\begin{aligned} p \ &\le \ \Pr_s(\{uaw \mid (\overrightarrow{a}, \delta(q, ua)) \text{ is deciding, } |u| \le K\}) \\ &= \ \Pr_s(\{uaw \mid (\overrightarrow{a}, \delta(q, ua)) \text{ is deciding, } |u| = K\}) \end{aligned}$$

Suppose $cras(s, q) = \infty$. Then for all $k \in \mathbb{N}$ the belief $\Delta(\{(s, q)\}, \perp^k)$ is not confused, and so, by Lemma 19, for all a the belief $\Delta(\{(s, q)\}, \perp^k a)$ is settled. It follows that for each $p < 1$ there is $K \in \mathbb{N}$ such that

$$p \ \le \ \Pr_s(\Sigma^K\{aw \mid \Delta(\{(s, q)\}, \perp^K a) \text{ is deciding}\}) \tag{13}$$

Since there are finitely many (s, q), it is also the case that for each $p < 1$ there is $K \in \mathbb{N}$ such that for all (s, q) Equation (13) holds.

Let $\varepsilon > 0$. Choose $K \in \mathbb{N}$ such that (13) holds for $p := 1/(1+\varepsilon)$. Let (s, q) be such that $cras(s, q) = \infty$ and let X denote the random number of observations that $\rho_{pro}(K)$ needs to make starting in (s, q). From the argument above, we have $\Pr_s(X > 1) \le 1 - p$. Since for the (random) pair (s', q') after the next observation (i.e., $\{(s', q')\} = \Delta(\{(s, q)\}, \perp^K a)$ for the observed a) we have $cras(s', q') = \infty$ again, it follows that $\Pr_s(X > i) \le (1-p)^i$ holds for all $i \in \mathbb{N}$. Hence we have:

$$c(K, s, q) \ := \ \mathrm{Ex}_s(X) \ = \ \sum_{i=0}^{\infty} \Pr_s(X > i) \ \le \ \sum_{i=0}^{\infty} (1-p)^i \ = \ \frac{1}{p} \ = \ 1 + \varepsilon$$

□

B.15 Proof of Theorem 27

Here is Theorem 27 from the main body:

Theorem 27. *For any feasible policy ρ there is $K \in \mathbb{N}$ such that:*

$$\mathrm{Ex}(C_{\rho_{pro}(K)}) \;\leq\; \mathrm{Ex}(C_\rho)$$

Proof. Let ρ be a feasible policy. First we compare $\rho_{pro} := \rho_{pro}(\infty)$ with ρ. Let w be such that all its prefixes are enabled. For $n \in \mathbb{N}$, define $\upsilon_{pro}(n)(w)$ and $\upsilon_\rho(n)(w)$ as the observation prefixes obtained by ρ_{pro} and ρ, respectively, after n steps. We write $\ell_{pro}(n)(w)$ and $\ell_\rho(n)(w)$ for the number of non-$\perp$ observations in $\upsilon_{pro}(n)(w)$ and $\upsilon_\rho(n)(w)$, respectively. Define $B_{pro}(n)(w) := \Delta(B_0, \upsilon_{pro}(n)(w))$ and $B_\rho(n)(w) := \Delta(B_0, \upsilon_\rho(n)(w))$. For beliefs B, B' we write $B \preceq B'$ when for all $(s, q) \in B$ there is $(s', q') \in B'$ with $(s, q) \approx (s', q')$. In the following we suppress w in the notation to avoid clutter. We show for all w and all $n \in \mathbb{N}$:

$$\ell_{pro}(n) \leq \ell_\rho(n) \quad \text{and} \quad \big(B_{pro}(n) \preceq B_\rho(n) \quad \text{or} \quad \ell_{pro}(n) < \ell_\rho(n)\big) \tag{14}$$

We proceed by induction on n. In the base case, $n = 0$, we have $\ell_{pro}(0) = 0 = \ell_\rho(0)$ and $B_{pro}(0) = B_0 = B_\rho(0)$. For the inductive step, suppose (14) holds for n.

1. Suppose ρ_{pro} does not observe the $(n+1)$st letter. Then $\ell_{pro}(n+1) = \ell_{pro}(n)$.
   (a) Suppose $\ell_{pro}(n+1) < \ell_\rho(n+1)$. Then (14) holds for $n+1$.
   (b) Otherwise, $\ell_\rho(n+1) \leq \ell_{pro}(n+1) = \ell_{pro}(n) \leq \ell_\rho(n) \leq \ell_\rho(n+1)$ by the induction hypothesis. So all these numbers are equal and we conclude that ρ does not observe the $(n+1)$st letter either and that $\ell_{pro}(n) = \ell_\rho(n)$. It follows by the induction hypothesis that $B_{pro}(n) \preceq B_\rho(n)$. Thus $B_{pro}(n+1) = \Delta(B_{pro}(n), \perp) \preceq \Delta(B_\rho(n), \perp) = B_\rho(n+1)$. Hence (14) holds for $n+1$.
2. Otherwise ρ_{pro} observes the $(n+1)$st letter. From the definition of ρ_{pro} it follows that $B_{pro}(n+1)$ is settled and thus $B_{pro}(n+1) \preceq B_\rho(n+1)$.
   (a) Suppose $\ell_{pro}(n) < \ell_\rho(n)$. Then $\ell_{pro}(n+1) \leq \ell_\rho(n) \leq \ell_\rho(n+1)$, i.e., (14) holds for $n+1$.
   (b) Otherwise, by the induction hypothesis, we have $B_{pro}(n) \preceq B_\rho(n)$. Since ρ_{pro} observes the $(n+1)$st letter, the belief $\Delta(B_{pro}(n), \perp)$ is confused. Since $B_{pro}(n) \preceq B_\rho(n)$, the belief $\Delta(B_\rho(n), \perp)$ is also confused. Hence, by Lemma 4.4, $\upsilon_\rho(n)\perp$ is confused. By Proposition 9, ρ does not allow confusion. So ρ observes the $(n+1)$st letter. Thus we have $\ell_{pro}(n+1) = \ell_{pro}(n) + 1 \leq \ell_\rho(n) + 1 = \ell_\rho(n+1)$, where the inequality is by the induction hypothesis. Hence (14) holds for $n+1$.

Thus we have shown (14).

Define $I := \{(s, q) \mid (s, q) \text{ is not deciding}, \ \mathit{cras}(s, q) = \infty\}$. We will choose $K > |S|^2 \cdot |Q|^2$, so, by Lemma 22, $\rho_{pro}(K)$ coincides with $\rho_{pro}(\infty)$ until possibly $\rho_{pro}(K)$ encounters a pair $(s, q) \in I$. Define:

$$D \;:=\; \{w \mid \rho_{pro}(\infty) \text{ does not encounter any element of } I\}$$

For each $(s,q) \in I$ define:

$$E(s,q) \ \coloneqq \ \{w \mid (s,q) \text{ is the first element of } I \text{ that } \rho_{pro}(\infty) \text{ encounters on } w\}$$

So $D \cup \bigcup_{(s,q)\in I} E(s,q) = \Sigma^\omega$. We show $\mathrm{Ex}(C_{\rho_{pro}(K)}) \le \mathrm{Ex}(C_\rho)$ by conditioning separately on D and on each $E(s,q)$ that has positive probability.

There is, by Lemma 23, almost surely a time, n_{dec}, when $\rho_{pro}(K)$ encounters a deciding (s,q). In the event D, it follows $C_{\rho_{pro}(K)} = \ell_{pro}(n_{dec})$; i.e., we have almost surely

$$C_{\rho_{pro}(K)} \ = \ \ell_{pro}(n_{dec}) \ \overset{\text{by (14)}}{\le} \ \ell_\rho(n_{dec}) \ \le \ C_\rho \qquad \text{in the event } D. \tag{15}$$

Let $(s,q) \in I$ and consider the event $E(s,q)$. Let us write n for the time when $\rho_{pro}(\infty)$, and thus $\rho_{pro}(K)$, first encounters (s,q). Since (s,q) is not deciding, the belief $B_{pro}(n)$ is not deciding. Since $\rho_{pro}(K)$ observes a letter at time n, the belief $B_\rho(n) \succeq B_{pro}(n)$ is not deciding either. So we have almost surely

$$C_\rho - \ell_{pro}(n) \ \ge \ \ell_\rho(n) + 1 - \ell_{pro}(n) \ \overset{\text{by (14)}}{\ge} \ 1 \qquad \text{in the event } E(s,q). \tag{16}$$

1. Suppose $\mathrm{Ex}(C_\rho - \ell_{pro}(n) \mid E(s,q)) \le 1$. Then, by (16), we have $C_\rho = \ell_\rho(n)+1$ almost surely in the event $E(s,q)$. Thus, almost surely in $E(s,q)$, there exists $k \in \mathbb{N}$ such that $\Delta(B_\rho, \perp^k a) \succeq \Delta((s,q), \perp^k a)$ is deciding for all a. It follows that there exists $k \in \mathbb{N}$ such that $\Delta((s,q), \perp^k a)$ is deciding for all a. We will choose $K \ge k$, so $\Delta((s,q), \perp^K a)$ is deciding for all a. Hence, by (14), we have $C_{\rho_{pro}(K)} = \ell_{pro}(n) + 1 \le \ell_\rho(n) + 1 = C_\rho$ almost surely in the event $E(s,q)$.
2. Otherwise $\mathrm{Ex}(C_\rho - \ell_{pro}(n) \mid E(s,q)) > 1$. It follows from Lemma 25 that one can choose K large enough so that $\mathrm{Ex}(C_{\rho_{pro}(K)} - \ell_{pro}(n) \mid E(s,q)) < \mathrm{Ex}(C_\rho - \ell_{pro}(n) \mid E(s,q))$. We will choose K in this way, so that we have $\mathrm{Ex}(C_{\rho_{pro}(K)} \mid E(s,q)) < \mathrm{Ex}(C_\rho \mid E(s,q))$.

By choosing K large enough so that for each $(s,q) \in I$ the respective constraint in item 1 or 2 is satisfied, we obtain $\mathrm{Ex}(C_{\rho_{pro}(K)} \mid E(s,q)) \le \mathrm{Ex}(C_\rho \mid E(s,q))$ for each $(s,q) \in I$. Combining this with (15) yields the result. □