# On Probabilistic Monitorability[⋆]

Antonis Achilleos[1], Elli Anastasiadi[1], Adrian Francalanza[2], Karoliina Lehtinen[3], and Mathias Ruggaard Pedersen[1]

[1] Reykjavík University
[2] University of Malta
[3] University of Liverpool

**Abstract.** This paper investigates monitorability in the context of probabilistic systems. We specify how monitor verdicts, reached over finite (partial) traces can be given a probabilistic interpretation. For monitors that are used to runtime-verify properties, we also relate their probabilistic verdicts to the probability that the corresponding completed trace satisfies the property of interest. This leads us to define probabilistic monitor soundness and completeness, which are then used to formulate probabilistic monitorability. Surprisingly, we show that this coincides with classical monitorability from the literature. This allows us to carry over prior results from the classical setting to the probabilistic realm.

## 1 Introduction

Monitors are passive computational entities that observe the execution of a system, *i.e.*, a finite trace, to determine properties about it [7,10,11]. The systems observed are occasionally equipped with probabilistic information about their branching behaviour and, due to their passivity, monitors intrinsically inherit this probabilistic behaviour. It is then natural, and fairly straightforward to ascribe this probabilistic measurement to monitor verdicts. However, when relating monitors to (linear-time) specifications, it is unclear whether the resulting probabilistic verdicts, reached by the monitor over finite trace observations, are still in accordance with the probability that the completed trace (which may be infinite) satisfies the specification being monitored at runtime. This constitutes a monitorability problem that, to wit, has not been studied in the literature.

This paper investigates monitorability for probabilistic systems. Our result are modelled on the monitorability definition given in [2,11] which, opportunely, teases apart the monitor behaviour from the semantics of the properties being monitored, and relates them in terms of standard soundness and completeness criteria; it has also been formally related to other variants in the literature [3] and used for branching-time settings [1,12]. Our contributions are:

[⋆] This research was supported by the projects "TheoFoMon: Theoretical Foundations for Monitorability" (no. 163406-051) and "Open Problems in the Equational Logic of Processes (OPEL)" (no. 196050-051) of the Icelandic Research Fund, and project BehAPI, funded by the EU H2020 RISE programme under the Marie Skłodowska-Curie grant (no. 778233).

1. We define probabilistic versions of monitor soundness and completeness relating the probability of verdicts reached from finite trace prefixes to the probability that the complete trace satisfies the property, Definitions 8 and 9.
2. We show a surprising correspondence between probabilistic monitorability and its classical variant, Theorem 1, which allows us to inherit prior results such as syntactic characterisations of monitorable properties.
3. We show how this framework is general enough to be adapted to probabilistic settings that consider a margin of error, Definition 11 and Theorem 2.
4. Section 4 concludes with an application of these results to estimate probabilities in settings that allow for repeated monitored runs while still being treated as a black box.

## 2 Preliminaries

We introduce the core concepts of measure and probability theory. We refer the interested reader to [4,6,8] for a more in-depth presentation.

**Definition 1 ($\sigma$-algebra [6, p. 754]).** *For a set $X$, a* $\sigma$-algebra *on $X$ is a set $\Sigma \subseteq 2^X$ such that $X \in \Sigma$, if $A \in \Sigma$ then $X \setminus A \in \Sigma$, and if $A_1, A_2, \ldots \in \Sigma$ then $\bigcup_{n \geq 1} A_n \in \Sigma$ (closure under complement and countable union).*

A pair $(X, \Sigma)$ of a set $X$ together with a $\sigma$-algebra $\Sigma$ on $X$ is known as a measurable space. If $\Sigma$ is a $\sigma$-algebra and $A \in \Sigma$, we say that $A$ is measurable for $\Sigma$, and if $\Sigma$ is evident from the context, we simply say that $A$ is measurable. With a $\sigma$-algebra on $X$ in hand, we can define a probability measure on $X$.

**Definition 2 (Probability measure [6, p. 754]).** *Given a measurable space $(X, \Sigma)$, a* probability measure *is a function $\mathbb{P} : \Sigma \to [0, 1]$ such that $\mathbb{P}(X) = 1$ and $\mathbb{P}(\bigcup_{i \in I} A_i) = \sum_{i \in I} \mathbb{P}(A_i)$ for any countable, pairwise disjoint collection $\{A_i\}_{i \in I} \subseteq \Sigma$. We denote by $\mathcal{D}(X)$ the set of all probability measures on $X$.*

A probabilistic system is one in which the evolution of the system is governed by some probability distribution. We use here one of the simplest probabilistic systems, namely (generative) Markov chains. Assume a finite set of actions $\mathit{Act}$.

**Definition 3 (Markov chain).** *A* Markov chain *is a tuple $M = (S, s_*, \Delta)$, where $S$ is a countable set of states, $s_* \in S$ is the start state, and $\Delta : S \to \mathcal{D}(\mathit{Act} \times S)$ is the transition function assigning to each state a distribution over actions and states.*

A Markov chain $M = (S, s_*, \Delta)$ currently in state $s \in S$ evolves by choosing action $a$ and state $s'$ with probability $\Delta(s)(a, s')$, moving to $s'$ while outputting the action $a$. In this paper we consider the trace-based behaviour of Markov chains. A trace is an infinite sequence of actions $a_1 a_2 \cdots \in \mathit{Act}^\omega$. We let $\pi, \pi'$ range over traces. A finite trace is a sequence of actions $a_1 a_2 \ldots a_n \in \mathit{Act}^*$ which we range over by $w, w'$, and sets of finite traces are ranged over by $F$. We denote by $\varepsilon$ the empty trace. Given two finite traces $w$ and $w'$, we write $w \preceq w'$ if $w$ is a prefix of $w'$, meaning that there exists a finite trace $w''$ such that $ww'' = w'$. For a trace $\pi = a_1a_2\dots$, we let $\pi\langle i\rangle = a_i$, $\pi|_i = a_1\dots a_i$ and $\pi|^i = a_{i+1},\dots$.

For a Markov chain $M = (S, s_*, \Delta)$ we obtain a measurable space of traces $(Act^\omega, \Sigma)$ using the cylinder construction (see e.g. [6, pp. 757–758]) as follows. Given a finite trace $a_1\dots a_n$, we define the cylinder of that trace as

$$\mathbb{C}(a_1\dots a_n) = \{\pi \in Act^\omega \mid \pi|_n = a_1\dots a_n\}.$$

Thus $\mathbb{C}(a_1\dots a_n)$ is the set of infinite traces that all agree on the finite prefix $a_1\dots a_n$. In the following, we fix the $\sigma$-algebra $\Sigma$ on $Act^\omega$, defined as the smallest $\sigma$-algebra containing all cylinders. For a given state $s$, we define a probability measure $\mathbb{P}^s_M$ on the measurable space $(Act^\omega, \Sigma)$ inductively as $\mathbb{P}^s_M(\mathbb{C}(\varepsilon)) = 1$ and

$$\mathbb{P}^s_M(\mathbb{C}(a_1a_2\dots a_n)) = \sum_{s'\in S} \Delta(s, a_1)(s') \cdot \mathbb{P}^{s'}_M(\mathbb{C}(a_2\dots a_n)).$$

Although we only define $\mathbb{P}^s_M$ on cylinders, the probability extends uniquely to the whole $\sigma$-algebra $\Sigma$ using the Hahn-Kolmogorov theorem [14, Theorem 1.7.8]. Thus for any measurable set $A \in \Sigma$, the probability $\mathbb{P}^s_M(A)$ is well-defined.

## 3 Monitoring

Runtime verification employs monitors to observe the behaviour of the system, typically as a black box; the system emits sequences of events/actions from some set *Act*. A monitor accepts if the (finite) observations lead it to conclude that the system satisfies a property of interest, and rejects if it observes enough events to conclude that the property is violated. Our objective is to give an account of monitoring in the case where the system being monitored is a probabilistic system. In this case, the monitor itself is still non-probabilistic, and can only observe the actions emitted by the probabilistic system. Thus the monitored system is still a black box, and the monitor has no way of knowing the internal state or the transition probabilities of the system.

**Definition 4 (Monitor).** *A* monitor $m = (F_{acc}, F_{rej})$ *is a pair of sets of finite traces* $F_{acc}, F_{rej} \subseteq Act^*$ *satisfying:* $(i)$ $F_{acc} \cap F_{rej} = \emptyset$*;* $(ii)$ *for* $i \in \{acc, rej\}$*:*

$$\textit{if } w \in F_i \textit{ then for any } w' \in Act^* \textit{ where } w \leq w' \textit{ we also have } w' \in F_i \qquad (1)$$

The traces in $F_{acc}$ denote the finite observations accepted by the monitor whereas those in $F_{rej}$ are the traces the monitor rejects. Condition (1) ensures that verdicts (i.e., acceptances and rejections) are irrevocable. For a set $F \subseteq Act^*$ we define $\mathbb{C}(F) = \bigcup_{w\in F} \mathbb{C}(w)$, so that $\mathbb{C}(F)$ is the union of the cylinders generated by each string in $F$. Since each cylinder $\mathbb{C}(w)$ is measurable by definition, $\mathbb{C}(F)$ is also measurable, being a countable union of measurable sets.

*Example 1.* Consider a monitor whose accepting set is

$$F_{acc} = \{\pi \in Act^* \mid (\pi\langle 1\rangle = a = \pi\langle 2\rangle) \text{ or } (\pi\langle 1\rangle = c)\},$$

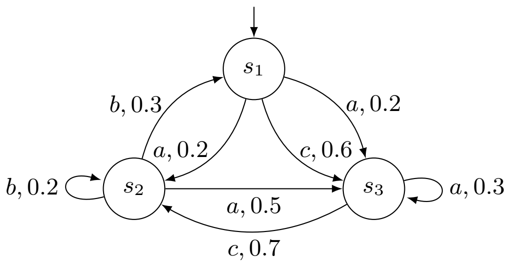

**Fig. 1.** A Markov chain with three states, the initial state being $s_1$. The symbol and number above each transition indicates which action is taken and with what probability.

and let $M = (S, s_1, \Delta)$ be the Markov chain describing the system depicted in Figure 1. In order to calculate the probability of the monitor accepting when monitoring this system, we first note that $\mathbb{C}(F_{acc}) = \mathbb{C}(aa) \cup \mathbb{C}(c)$. Since these are disjoint sets, we can calculate the probability as

$$\begin{aligned}\mathbb{P}^{s_1}_M(\mathbb{C}(F_{acc})) = \mathbb{P}^{s_1}_M(\mathbb{C}(aa)) + \mathbb{P}^{s_1}_M(\mathbb{C}(c)) &= (0.2 \cdot \mathbb{P}^{s_2}_M(\mathbb{C}(a)) + 0.2 \cdot \mathbb{P}^{s_3}_M(\mathbb{C}(a))) + 0.6\\ &= (0.2 \cdot 0.5 + 0.2 \cdot 0.3) + 0.6 = 0.76.\end{aligned}$$

Properties of the system will be described in the linear-time $\mu$-calculus [2,16].

$$\varphi, \psi ::= \texttt{tt} \mid \texttt{ff} \mid X \mid \varphi \wedge \psi \mid \varphi \vee \psi \mid [a]\varphi \mid \langle a \rangle \varphi \mid \mu X.\varphi \mid \nu X.\varphi$$

Formulas are interpreted over infinite traces using an interpretation $\rho : S \to 2^{Act^\omega}$ for variables. The semantics is standard; we present here the modal cases.

$$\begin{aligned}\llbracket [a]\varphi \rrbracket_\rho &= \{\pi \in Act^\omega \mid \pi|^1 \in \llbracket \varphi \rrbracket_\rho \text{ whenever } \pi\langle 1 \rangle = a\}\\ \llbracket \langle a \rangle\varphi \rrbracket_\rho &= \{\pi \in Act^\omega \mid \pi\langle 1 \rangle = a \text{ and } \pi|^1 \in \llbracket \varphi \rrbracket_\rho\}\end{aligned}$$

For closed formulas, we may omit the subscript and simply write $\llbracket \varphi \rrbracket$. Since the logic is closed under complement, we define negation as complement, meaning that $\llbracket \neg\varphi \rrbracket = Act^\omega \setminus \llbracket \varphi \rrbracket$. We next prove that each formula is measurable.

**Lemma 1.** *For each $\varphi$, $\llbracket \varphi \rrbracket$ is measurable.*

*Proof.* Since the linear-time $\mu$-calculus and Büchi automata are equivalent [9], [15, Proposition 2.3], which states that the set of traces recognisable by a given Büchi automaton is measurable, shows that $\llbracket \varphi \rrbracket$ is measurable. □

Lemma 1 means that the probability $\mathbb{P}^s_M(\llbracket \varphi \rrbracket)$ of a property is well-defined.

*Example 2.* The property $\varphi = [a]\langle a \rangle\texttt{tt} \wedge [b]\texttt{ff}$ states that a trace cannot start with $b$, and whenever it starts with $a$, it must be followed by another $a$. The probability that $M = (S, s_1, \Delta)$, from Figure 1, does not satisfy $\varphi$ is

$$\begin{aligned}\mathbb{P}^{s_1}_M(\llbracket \neg\varphi \rrbracket) &= \mathbb{P}^{s_1}_M(\mathbb{C}(b) \cup \mathbb{C}(ab) \cup \mathbb{C}(ac))\\ &= \mathbb{P}^{s_1}_M(\mathbb{C}(b)) + \mathbb{P}^{s_1}_M(\mathbb{C}(ab)) + \mathbb{P}^{s_1}_M(\mathbb{C}(ac))\\ &= 0 + (0.2 \cdot \mathbb{P}^{s_2}_M(\mathbb{C}(b)) + 0.2 \cdot \mathbb{P}^{s_3}_M(\mathbb{C}(b))) + (0.2 \cdot \mathbb{P}^{s_2}_M(\mathbb{C}(c)) + 0.2 \cdot \mathbb{P}^{s_3}_M(\mathbb{C}(c)))\\ &= 0 + (0.2 \cdot 0.5 + 0.2 \cdot 0) + (0.2 \cdot 0 + 0.2 \cdot 0.7) = 0.24.\end{aligned}$$

### 3.1 Soundness, completeness, and monitorability

In the non-probabilistic setting [2], soundness ensures that any trace accepted by the monitor also satisfies the property of interest, and that any trace rejected by the monitor does not satisfy the property. In other words, soundness means that the monitor is an *underapproximation* of the property.

**Definition 5 (Soundness).** *A monitor $m = (F_{acc}, F_{rej})$ is* sound *for a formula $\varphi$ if $\mathbb{C}(F_{acc}) \subseteq [\![\varphi]\!]$ and $\mathbb{C}(F_{rej}) \subseteq [\![\neg\varphi]\!]$.*

Dually, completeness requires the monitor to *overapproximate* the property being monitored: if a trace satisfies the property, the monitor must accept that trace, and if a trace violates the property, the monitor should reject the trace.

**Definition 6 (Completeness).** *A monitor $m = (F_{acc}, F_{rej})$ is* complete *for a formula $\varphi$ if $[\![\varphi]\!] \subseteq \mathbb{C}(F_{acc})$ and $[\![\neg\varphi]\!] \subseteq \mathbb{C}(F_{rej})$.*

Together, Definitions 5 and 6 require a monitor to fully agree with the property being monitored, i.e. $\mathbb{C}(F_{acc}) = [\![\varphi]\!]$ and $\mathbb{C}(F_{rej}) = [\![\neg\varphi]\!]$. A property is said to be monitorable if there exists a monitor which fully agrees with it.

**Definition 7 (Monitorability).** *A formula $\varphi$ is* monitorable *if there exists a monitor that is sound and complete for $\varphi$.*

In the probabilistic setting, we do not change either the monitors or the properties, but we interpret them over probabilistic systems. Hence, whereas non-probabilistic soundness and completeness range over satisfaction of the property in *all* models, the probabilistic version will range over the probability of the property in *all probabilistic models*. In order to extend the notions of soundness and completeness to the probabilistic setting, we impose two criteria: (1) the extension should be conservative, so that if $m$ is sound and complete for $\varphi$, it is also probabilistically sound and complete for $\varphi$; (2) the extension should preserve the idea of soundness being an underapproximation and completeness being an overapproximation, but in a probabilistic setting.

**Definition 8 (Probabilistic soundness).** *A monitor $m = (F_{acc}, F_{rej})$ is* probabilistically sound *for $\varphi$ if $\mathbb{P}_M^{s_*}(\mathbb{C}(F_{acc})) \leq \mathbb{P}_M^{s_*}([\![\varphi]\!])$ and $\mathbb{P}_M^{s_*}(\mathbb{C}(F_{rej})) \leq \mathbb{P}_M^{s_*}([\![\neg\varphi]\!])$ for all Markov chains $M = (S, s_*, \Delta)$.*

Definition 8 fulfills criterion (1), since the monotonicity property of probability measures, which states that if $A \subseteq B$, then $\mathbb{P}(A) \leq \mathbb{P}(B)$, gives us that if $\mathbb{C}(F_{acc}) \subseteq [\![\varphi]\!]$, then $\mathbb{P}_M^{s_*}(\mathbb{C}(F_{acc})) \leq \mathbb{P}_M^{s_*}([\![\varphi]\!])$, and likewise for rejection. It also fulfills criterion (2), since probabilistic soundness ensures that the probability of the monitor accepting is an underapproximation of the probability of the property being satisfied, and likewise for rejection.

*Example 3.* Assume $Act = \{a, b, c\}$. Let $\varphi = [a]\langle a\rangle\mathtt{tt} \wedge [b]\mathtt{ff}$, $F_{acc} = \{\pi \in Act^* \mid (\pi\langle 1\rangle = a = \pi\langle 2\rangle)\}$ or $(\pi\langle 1\rangle = c)$ and $F_{rej} = \emptyset$. For any $M = (S, s_*, \Delta)$, we have

$$\mathbb{P}_M^{s_*}(\mathbb{C}(F_{acc})) = \mathbb{P}_M^{s_*}(\{\pi \in Act^\omega \mid (\pi\langle 1\rangle = a = \pi\langle 2\rangle) \text{ or } (\pi\langle 1\rangle = c)\}) = \mathbb{P}([\![\varphi]\!])$$

and $0 = \mathbb{P}_M^{s_*}(\emptyset) = \mathbb{P}_M^{s_*}(F_{rej}) \leq \mathbb{P}_M^{s_*}([\![\neg\varphi]\!])$, so $m = (F_{acc}, F_{rej})$ is sound for $\varphi$.

**Definition 9 (Probabilistic completeness).** *A monitor $m = (F_{acc}, F_{rej})$ is* probabilistically complete *for a formula $\varphi$ if $\mathbb{P}^{s_*}_M(\mathbb{C}(F_{acc})) \geq \mathbb{P}^{s_*}_M(\llbracket\varphi\rrbracket)$ and $\mathbb{P}^{s_*}_M(\mathbb{C}(F_{rej})) \geq \mathbb{P}^{s_*}_M(\llbracket\neg\varphi\rrbracket)$ for all Markov chains $M = (S, s_*, \Delta)$.*

This definition also fulfills both of the stated criteria. Criterion (1) is satisfied for the same reason as for probabilistic soundness, and criterion (2) is satisfied because the probability that the monitor accepts is an overapproximation of the probability that the property is satisfied, and likewise for rejection.

*Example 4.* Recall $Act = \{a, b, c\}$ and $\varphi$ from Example 3 with

$$F_{acc} = \{\pi \in Act^* \mid (\pi\langle 1\rangle = a = \pi\langle 2\rangle) \text{ or } (\pi\langle 1\rangle = c)\}, \text{ and}$$
$$F_{rej} = \{\pi \in Act^* \mid (\pi\langle 1\rangle = b) \text{ or } (\pi\langle 1\rangle = a \text{ and } (\pi\langle 2\rangle = b \text{ or } \pi\langle 2\rangle = c))\}.$$

Then, for any system described by a Markov chain $M = (S, s_*, \Delta)$, we get

$$\begin{aligned}\mathbb{P}^{s_*}_M(\mathbb{C}(F_{acc})) &= \mathbb{P}(\{\pi \in Act^\omega \mid (\pi\langle 1\rangle = a = \pi\langle 2\rangle) \text{ or } (\pi\langle 1\rangle = c)\}) = \mathbb{P}^{s_*}_M(\llbracket\varphi\rrbracket), \text{ and}\\ \mathbb{P}^{s_*}_M(\mathbb{C}(F_{rej})) &= \mathbb{P}^{s_*}_M(\{\pi \in Act^\omega \mid (\pi\langle 1\rangle = b) \text{ or } (\pi\langle 1\rangle = a \text{ and } (\pi\langle 2\rangle = b \text{ or } \pi\langle 2\rangle = c))\})\\ &= \mathbb{P}^{s_*}_M(\{\pi \in Act^\omega \mid (\pi\langle 1\rangle \neq a \text{ or } \pi\langle 2\rangle \neq a) \text{ and } (\pi\langle 1\rangle \neq c)\}) = \mathbb{P}^{s_*}_M(\llbracket\neg\varphi\rrbracket),\end{aligned}$$

so the monitor $m = (F_{acc}, F_{rej})$ is both sound and complete for $\varphi$.

Soundness and completeness together would then imply $\mathbb{P}^{s_*}_M(\mathbb{C}(F_{acc})) = \mathbb{P}^{s_*}_M(\llbracket\varphi\rrbracket)$ and $\mathbb{P}^{s_*}_M(\mathbb{C}(F_{rej})) = \mathbb{P}^{s_*}_M(\llbracket\neg\varphi\rrbracket)$ for all Markov chains $M = (S, s_*, \Delta)$. This describes the probabilistic monitorability of a formula.

**Definition 10 (Probabilistic monitorability).** *A formula $\varphi$ is* probabilistically monitorable *if there exists a monitor $m$ that is probabilistically sound and probabilistically complete for $\varphi$.*

It is interesting to consider the connections between the probabilistic and non-probabilistic version of soundness and completeness. Because probabilistic soundness and completeness are conservative extensions of their non-probabilistic counterparts, if $m$ monitors soundly for $\varphi$ in the non-probabilistic setting, then $m$ should also monitor soundly for $\varphi$ in the probabilistic setting. Likewise for completeness. Surprisingly, it turns out that the reverse implication also holds.

**Theorem 1.** *Monitor $m$ is sound for $\varphi$ if and only if $m$ is probabilistically sound for $\varphi$; $m$ is complete for $\varphi$ if and only if $m$ is probabilistically complete for $\varphi$.*

*Proof.* Soundness and completeness imply their probabilistic counterparts by monotonicity of probability measures. For the other direction, we prove the contrapositive, so assume that $m$ is not sound for $\varphi$. Assume without loss of generality that $\mathbb{C}(m_{acc}) \not\subseteq \llbracket\varphi\rrbracket$. This means that there exists a trace $\pi \in \mathbb{C}(m_{acc})$ such that $\pi \notin \llbracket\varphi\rrbracket$. Since $\varphi$ describes an $\omega$-regular property, there must exist a trace $\pi' \in \mathbb{C}(m_{acc})$ and a Markov chain $M$ such that $\mathbb{P}^{s_*}_M(\mathbb{C}(m_{acc})) = 1$ but $\mathbb{P}^{s_*}_M(\llbracket\varphi\rrbracket) = 0$ by constructing $M$ such that it generates only the trace $\pi'$. Then $1 = \mathbb{P}^{s_*}_M(\mathbb{C}(m_{acc})) \not\leq \mathbb{P}^{s_*}_M(\llbracket\varphi\rrbracket) = 0$, so $m$ is not probabilistically sound for $\varphi$. A similar argument works for the case of completeness. □

A corollary of Theorem 1 is that the probabilistically monitorable formulas are exactly those that are also non-probabilistically monitorable. In [2] it was shown that the largest fragment of the linear-time $\mu$-calculus for which all formulas are monitorable is the Hennessy-Milner logic [13].

**Corollary 1.** *The logical fragment* $\varphi, \psi ::= \mathtt{tt} \mid \mathtt{ff} \mid \varphi \wedge \psi \mid \varphi \vee \psi \mid [a]\varphi \mid \langle a \rangle \varphi$ *is probabilistically monitorable and maximally expressive.*

### 3.2 Other Monitor Requirements

Theorem 1 may seem to imply that Definitions 8 and 9 are very restrictive. However, the theorem holds for other, more relaxed interpretations of soundness and completeness in a probabilistic setting. Fix two parameters $c, d > 0$.

**Definition 11 (Probabilistic soundness and completeness with a margin of error).** *A monitor* $m = (F_{acc}, F_{rej})$ *is probabilistically sound for* $\varphi$ *with* margin of error $c$ *if* $\mathbb{P}_M^{s_*}(\mathbb{C}(F_{acc})) \leq c \cdot \mathbb{P}_M^{s_*}(\llbracket \varphi \rrbracket)$ *and* $\mathbb{P}_M^{s_*}(\mathbb{C}(F_{rej})) \leq c \cdot \mathbb{P}_M^{s_*}(\llbracket \neg\varphi \rrbracket)$ *for all Markov chains* $M = (S, s_*, \Delta)$. *Likewise,* $m$ *is probabilistically complete with* margin of error $d$ *for* $\varphi$ *if* $\mathbb{P}_M^{s_*}(\mathbb{C}(F_{acc})) \geq d \cdot \mathbb{P}_M^{s_*}(\llbracket \varphi \rrbracket)$ *and* $\mathbb{P}_M^{s_*}(\mathbb{C}(F_{rej})) \geq d \cdot \mathbb{P}_M^{s_*}(\llbracket \neg\varphi \rrbracket)$ *for all Markov chains* $M = (S, s_*, \Delta)$.

The two parameters, when $c > 1$ and $d < 1$, allow the monitor to occasionally give more or fewer verdicts than it should, but always within a set margin of error. Another candidate for soundness and satisfaction-completeness, parameterized with respect to $c$ and $d$, is conditional soundness and completeness.

**Definition 12 (Conditional soundness and completeness).** *A monitor* $m = (F_{acc}, F_{rej})$ *is conditionally sound for* $\varphi$ *with* margin of error $c$ *if it holds that* $\mathbb{P}_M^{s_*}(\llbracket \varphi \rrbracket \mid \mathbb{C}(F_{acc})) \geq c$ *and* $\mathbb{P}_M^{s_*}(\llbracket \neg\varphi \rrbracket \mid \mathbb{C}(F_{rej})) \leq c$ *for all Markov chains* $M = (S, s_*, \Delta)$. *A monitor* $(F_{acc}, F_{rej})$ *is conditionally complete for* $\varphi$ *with* margin of error $d$ *if* $\mathbb{P}_M^{s_*}(\mathbb{C}(F_{acc}) \mid \llbracket \varphi \rrbracket) \geq d$ *and* $\mathbb{P}_M^{s_*}(\mathbb{C}(F_{rej}) \mid \llbracket \neg\varphi \rrbracket) \geq d$ *for all Markov chains* $M = (S, s_*, \Delta)$.

We observe that for these variations of probabilistic soundness and completeness as well, the arguments used in the proof of Theorem 1 can also be applied.

**Theorem 2.** *All the variants of soundness and completeness are equivalent. This means that Definitions 5, 8, 11, and 12 are equivalent, and that Definitions 6, 9, 11, and 12 are also equivalent.*

*Proof.* The first two items, both for soundness and completeness are equivalent, by Theorem 1. To show that each other item is equivalent to the first, we follow the proof of Theorem 1. □

Theorem 2 allows us to treat monitorability uniformly for all the approaches described by Definitions 5, 6, 8, 9 and 11 to 12. For instance, the monitor synthesis defined in [12,2] and implemented in [5] applies directly to the probabilistic setting (with margins of error). We also remark that the approach of [2] allows more fine-grained notions of completeness in terms of satisfaction- and violation-completeness, which leads to more properties being monitorable [3]. Our results straightforwardly extend to these notions.

## 4 An application: estimating probabilities

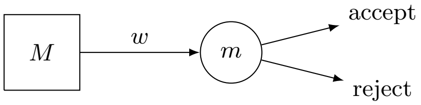

**Fig. 2.** A setup for estimating probabilities. $M$ is a probabilistic system being monitored by the monitor $m$, which reads the trace $w$ emitted by $S$ to provide a verdict.

The theory we have described in Section 3 allows us to estimate the probabilities of properties over infinite traces, even if the system itself is a black box. To see this, consider the setup depicted in Figure 2. Here we have a probabilistic system $M = (S, s_*, \Delta)$, of which we do not know the internal workings, and hence should be viewed as a black box. Using the synthesis from [2], we can generate a monitor $m = (F_{acc}, F_{rej})$ which is both sound and complete for a monitorable property $\varphi$, whose probability in $M$ we are interested in estimating. As $m$ observes the behaviour of $M$ given by a sequence of outputs $w = a_1 \ldots a_n$, $m$ will eventually, in finite time, produce either an accept or a reject verdict. This is guaranteed because $m$ is both sound and complete.

In a setting where a system is executed repeatedly (e.g. once every morning), we can estimate the probability $\mathbb{P}_M^{s_*}(\llbracket\varphi\rrbracket)$. Concretely, every time the system $M$ is run (with passive monitor $m$), the verdict reached for an exhibited trace is recorded (here we assume that we can reset the system to its initial state). After some number of iterations, say $n$ iterations, we will have observed some number $n_{acc}$ of accept verdicts and some number $n_{rej}$ of reject verdicts. We can then estimate the probabilities $\mathbb{P}_M^{s_*}(\mathbb{C}(F_{acc}))$ and $\mathbb{P}_M^{s_*}(\mathbb{C}(F_{rej}))$ by $\frac{n_{acc}}{n}$ and $\frac{n_{rej}}{n}$, respectively. By Theorem 1, the probability of satisfying the property is equal to the probability of the monitor accepting, and likewise for not satisfying the property and rejecting. This means that $\frac{n_{acc}}{n}$ and $\frac{n_{rej}}{n}$ are also estimates of $\mathbb{P}_M^{s_*}(\llbracket\varphi\rrbracket)$ and $\mathbb{P}_M^{s_*}(\llbracket\neg\varphi\rrbracket)$, respectively, so we can use these to estimate the probability that $\varphi$ is satisfied in $M$.

This approach to estimating only works for the monitorable fragment of the logic (see Corollary 1). However, even for non-monitorable properties, we can use the approach to give estimates of the probability in terms of lower and upper bounds. For some non-monitorable property $\varphi$ one could construct a sound monitor $m_1 = (F_{acc}^1, F_{rej}^1)$ and a complete monitor $m_2 = (F_{acc}^2, F_{rej}^2)$. Then $\mathbb{P}_M^{s_*}(\mathbb{C}(F_{acc}^1)) \leq \mathbb{P}_M^{s_*}(\llbracket\varphi\rrbracket) \leq \mathbb{P}_M^{s_*}(\mathbb{C}(F_{acc}^2))$, and similarly for $\llbracket\neg\varphi\rrbracket$ and the rejection parts of the monitors. Hence $m_1$ gives a lower bound on the probability of $\varphi$, and $m_2$ gives an upper bound. Now we can use the approach from before to estimate the probabilities of $m_1$ accepting and rejecting and of $m_2$ accepting and rejecting, thus giving us estimates on lower and upper bounds on $\varphi$. The downside is that in this case we have no guarantee that $m_1$ will give a verdict in finite time.

## References

1. Luca Aceto, Antonis Achilleos, Adrian Francalanza, and Anna Ingólfsdóttir. A framework for parameterized monitorability. In Christel Baier and Ugo Dal Lago, editors, *Foundations of Software Science and Computation Structures - 21st International Conference, FOSSACS 2018, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2018, Thessaloniki, Greece, April 14-20, 2018, Proceedings*, volume 10803 of *Lecture Notes in Computer Science*, pages 203–220. Springer, 2018.
2. Luca Aceto, Antonis Achilleos, Adrian Francalanza, Anna Ingólfsdóttir, and Karoliina Lehtinen. Adventures in monitorability: from branching to linear time and back again. *Proc. ACM Program. Lang.*, 3(POPL):52:1–52:29, 2019.
3. Luca Aceto, Antonis Achilleos, Adrian Francalanza, Anna Ingólfsdóttir, and Karoliina Lehtinen. An operational guide to monitorability. In Peter Csaba Ölveczky and Gwen Salaün, editors, *Software Engineering and Formal Methods - 17th International Conference, SEFM 2019, Oslo, Norway, September 18-20, 2019, Proceedings*, volume 11724 of *Lecture Notes in Computer Science*, pages 433–453. Springer, 2019.
4. Robert B. Ash and Catherine A. Doléans-Dade. *Probability & Measure Theory.* Harcourt/Academic Press, 2nd edition, 1999.
5. Duncan Paul Attard and Adrian Francalanza. Trace partitioning and local monitoring for asynchronous components. In Alessandro Cimatti and Marjan Sirjani, editors, *Software Engineering and Formal Methods - 15th International Conference, SEFM 2017, Trento, Italy, September 4-8, 2017, Proceedings*, volume 10469 of *Lecture Notes in Computer Science*, pages 219–235. Springer, 2017.
6. Christel Baier and Joost-Pieter Katoen. *Principles of model checking.* MIT Press, 2008.
7. Ezio Bartocci, Yliès Falcone, Adrian Francalanza, and Giles Reger. Introduction to runtime verification. In Ezio Bartocci and Yliès Falcone, editors, *Lectures on Runtime Verification - Introductory and Advanced Topics*, volume 10457 of *Lecture Notes in Computer Science*, pages 1–33. Springer, 2018.
8. Patrick Billingsley. *Probability And Measure.* Wiley-Interscience, 3rd edition, 1995.
9. Mads Dam. Fixed points of Büchi automata. In R. K. Shyamasundar, editor, *Foundations of Software Technology and Theoretical Computer Science, 12th Conference, New Delhi, India, December 18-20, 1992, Proceedings*, volume 652 of *Lecture Notes in Computer Science*, pages 39–50. Springer, 1992.
10. Adrian Francalanza. A theory of monitors (extended abstract). In Bart Jacobs and Christof Löding, editors, *Foundations of Software Science and Computation Structures - 19th International Conference, FOSSACS 2016, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2016, Eindhoven, The Netherlands, April 2-8, 2016, Proceedings*, volume 9634 of *Lecture Notes in Computer Science*, pages 145–161. Springer, 2016.
11. Adrian Francalanza, Luca Aceto, Antonis Achilleos, Duncan Paul Attard, Ian Cassar, Dario Della Monica, and Anna Ingólfsdóttir. A foundation for runtime monitoring. In Shuvendu K. Lahiri and Giles Reger, editors, *Runtime Verification - 17th International Conference, RV 2017, Seattle, WA, USA, September 13-16, 2017, Proceedings*, volume 10548 of *Lecture Notes in Computer Science*, pages 8–29. Springer, 2017.
12. Adrian Francalanza, Luca Aceto, and Anna Ingólfsdóttir. Monitorability for the Hennessy-Milner logic with recursion. *Formal Methods Syst. Des.*, 51(1):87–116, 2017.

13. Matthew Hennessy and Robin Milner. Algebraic laws for nondeterminism and concurrency. *J. ACM*, 32(1):137–161, 1985.
14. Terence Tao. *An Introduction to Measure Theory*. Graduate studies in mathematics. American Mathematical Society, 2013.
15. Moshe Y. Vardi. Automatic verification of probabilistic concurrent finite-state programs. In *26th Annual Symposium on Foundations of Computer Science, Portland, Oregon, USA, 21-23 October 1985*, pages 327–338. IEEE Computer Society, 1985.
16. Moshe Y. Vardi. A temporal fixpoint calculus. In Jeanne Ferrante and P. Mager, editors, *Conference Record of the Fifteenth Annual ACM Symposium on Principles of Programming Languages, San Diego, California, USA, January 10-13, 1988*, pages 250–259. ACM Press, 1988.