Markov Automata with Multiple Objectives

Tim Quatmann, Sebastian Junges, and Joost-Pieter Katoen

RWTH Aachen University, Aachen, Germany

Abstract. Markov automata combine non-determinism, probabilistic branching, and exponentially distributed delays. This compositional variant of continuous-time Markov decision processes is used in reliability engineering, performance evaluation and stochastic scheduling. Their verification so far focused on single objectives such as (timed) reachability, and expected costs. In practice, often the objectives are mutually dependent and the aim is to reveal trade-offs. We present algorithms to analyze several objectives simultaneously and approximate Pareto curves. This includes, e.g., several (timed) reachability objectives, or various expected cost objectives. We also consider combinations thereof, such as on-time-within-budget objectives—which policies guarantee reaching a goal state within a deadline with at least probability \( p \) while keeping the allowed average costs below a threshold? We adopt existing approaches for classical Markov decision processes. The main challenge is to treat policies exploiting state residence times, even for untimed objectives. Experimental results show the feasibility and scalability of our approach.

1 Introduction

Markov automata extend labeled transition systems with probabilistic branching and exponentially distributed delays. They are a compositional variant of continuous-time Markov decision processes (CTMDPs), in a similar vein as Segala’s probabilistic automata extend classical MDPs. Transitions of a Markov automaton (MA) lead from states to probability distributions over states, and are either labeled with actions (allowing for interaction) or real numbers (rates of exponential distributions). MAs are used in reliability engineering, hardware design, data-flow computation, dependability, and performance evaluation, as MAs are a natural semantic framework for modeling formalisms such as AADL, dynamic fault trees, stochastic Petri nets, stochastic activity networks, SADF etc. The verification of MAs so far focused on single objectives such as reachability, timed reachability, expected costs, and long-run averages. These analyses cannot treat objectives that are mutually influencing each other, like quickly reaching a target is more costly. The aim of this paper is to analyze multiple objectives on MAs at once and to facilitate trade-off analysis by approximating Pareto curves.

Consider the stochastic job scheduling problem of [13]: perform \( n \) jobs with exponential service times on \( k \) identical processors under a pre-emptive scheduling policy. Once a job finishes, all \( k \) processors can be assigned any of the \( m \) remaining jobs. When \( n-m \) jobs are finished, this yields \( \binom{m}{k} \) non-deterministic choices.
The largest-expected-service-time-first-policy is optimal to minimize the expected time to complete all jobs \cite{13}. It is unclear how to schedule when imposing extra constraints, e.g., requiring a high probability to finish a batch of $c$ jobs within a tight deadline (to accelerate their post-processing), or having a low average waiting time. These multiple objectives involve non-trivial trade-offs. Our algorithms analyze such trade-offs. Fig. 1 e.g., shows the obtained result for 12 jobs and 3 processors. It approximates the set of points ($p_1, p_2$) for schedules achieving that (1) the expected time to complete all jobs is at most $p_1$ and (2) the probability to finish half of the jobs within an hour is at least $p_2$.

This paper presents techniques to verify MAs with multiple objectives. We consider multiple (un)timed reachability and expected reward objectives as well as their combinations. Put shortly, we reduce all these problems to instances of multi-objective verification problems on classical MDPs. For multi-objective queries involving (combinations of) untimed reachability and expected reward objectives, corresponding algorithms on the underlying MDP can be used. In this case, the MDP is simply obtained by ignoring the timing information, see Fig. 2(b). The MDP is in relating MA schedulers—that can exploit state sojourn times to optimize their decisions—to MDP schedulers. For multiple timed reachability objectives, digitization \cite{8, 9} is employed to obtain an MDP, see Fig. 2(c). The key is to mimic sojourn times by self-loops with appropriate probabilities. This provides a sound arbitrary close approximation of the timed behavior and also allows to combine timed reachability objectives with other types of objectives. The main contribution is to show that digitization is sound for all possible MA schedulers. This requires a new proof strategy as the existing ones are tailored to optimizing a single objective. All proofs can be found in the appendix. Experiments on instances of four MA benchmarks show encouraging results. Multiple untimed reachability and expected reward objectives can be efficiently treated for models with millions of states. As for single objectives \cite{9}, timed reachability is more expensive. Our implementation is competitive to PRISM for multi-objective MDPs \cite{14, 15} and to IMCA \cite{9} for single-objective MAs.

Related work. Multi-objective decision making for MDPs with discounting and long-run objectives has been well investigated; for a recent survey, see \cite{16}. Etesami et al. \cite{17} consider verifying finite MDPs with multiple $\omega$-regular objectives. Other multiple objectives include expected rewards under worst-case reachability \cite{18, 19}, quantiles and conditional probabilities \cite{20}, mean pay-offs and stability \cite{21}, long-run objectives \cite{22, 24}, total average discounted rewards under PCTL \cite{24}, and stochastic shortest path objectives \cite{25}. This has been extended to MDPs with unknown cost function \cite{26}, infinite-state MDPs \cite{24} arising from two-player timed games in a stochastic environment, and stochastic two-player games \cite{28}. To the best of our knowledge, this is the first work on multi-objective MDPs extended with random timing.
Fig. 2. MA $\mathcal{M}$ with underlying MDP $\mathcal{M}_D$ and digitization $\mathcal{M}_S$.

2 Preliminaries

Notations. The set of real numbers is denoted by $\mathbb{R}$, and we write $\mathbb{R}_{>0} = \{ x \in \mathbb{R} \mid x > 0 \}$ and $\mathbb{R}_{\geq 0} = \mathbb{R}_{>0} \cup \{ 0 \}$. For a finite set $S$, $\text{Dist}(S)$ denotes the set of probability distributions over $S$. $\mu \in \text{Dist}(S)$ is Dirac if $\mu(s) = 1$ for some $s \in S$.

2.1 Models

Markov automata generalize both Markov decision processes (MDPs) and continuous time Markov chains (CTMCs). They are extended with rewards (or, equivalently, costs) to allow modelling, e.g., energy consumption.

Definition 1 (Markov automaton). A Markov automaton (MA) is a tuple $\mathcal{M} = (S, \text{Act}, \rightarrow, s_0, \{ \rho_1, \ldots, \rho_\ell \})$ where $S$ is a finite set of states with initial state $s_0 \in S$, Act is a finite set of actions with $\perp \in \text{Act}$ and $\text{Act} \cap \mathbb{R}_{\geq 0} = \emptyset$, $\rightarrow \subset S \times (\text{Act} \cup \mathbb{R}_{\geq 0}) \times \text{Dist}(S)$ is a set of transitions such that for all $s \in S$ there is at most one transition $(s, \lambda, \mu) \in \rightarrow$ with $\lambda \in \mathbb{R}_{\geq 0}$, and $\rho_1, \ldots, \rho_\ell$ with $\ell \geq 0$ are reward functions $\rho_i : S \cup (S \times \text{Act}) \rightarrow \mathbb{R}_{\geq 0}$.

In the remainder of the paper, let $\mathcal{M} = (S, \text{Act}, \rightarrow, s_0, \{ \rho_1, \ldots, \rho_\ell \})$ denote an MA. A transition $(s, \gamma, \mu) \in \rightarrow$, denoted by $s \xrightarrow{\gamma} \mu$, is called probabilistic if $\gamma \in \text{Act}$ and Markovian if $\gamma \in \mathbb{R}_{\geq 0}$. In the latter case, $\gamma$ is the rate of an exponential distribution, modeling a time-delayed transition. Probabilistic transitions fire instantaneously. The successor state is determined by $\mu$, i.e., we move to $s'$ with probability $\mu(s')$. Probabilistic (Markovian) states PS (MS) have an outgoing probabilistic (Markovian) transition, respectively: $\text{PS} = \{ s \in S \mid s \xrightarrow{\alpha} \mu, \alpha \in \text{Act} \}$ and $\text{MS} = \{ s \in S \mid s \xrightarrow{\lambda} \mu, \lambda \in \mathbb{R}_{\geq 0} \}$. The exit rate $E(s)$ of $s \in \text{MS}$ is uniquely given by $s \xrightarrow{E(s)} \mu$. The transition probabilities of $\mathcal{M}$ are given by the function $P : S \times \text{Act} \times S \rightarrow [0,1]$ satisfying $P(s, \alpha, s') = \mu(s')$ if either $s \xrightarrow{\alpha} \mu$ or ($\alpha = \perp$ and $s \xrightarrow{E(s)} \mu$) and $P(s, \alpha, s') = 0$ in all other cases. The value $P(s, \alpha, s')$ corresponds to the probability to move from $s$ with action $\alpha$ to $s'$. The enabled actions at state $s$ are given by $\text{Act}(s) = \{ \alpha \in \text{Act} \mid \exists s' \in S : P(s, \alpha, s') > 0 \}$.

Example 1. Fig. 2(a) shows an MA $\mathcal{M}$. We do not depict Dirac probability distributions. Markovian transitions are illustrated by dashed arrows.
We assume action-deterministic MAs: \(|\{\mu \in \text{Dist}(S) \mid s \xrightarrow{\mu} s\}| \leq 1\) holds for all \(s \in S\) and \(\alpha \in \text{Act}\). Terminal states \(s \notin PS \cup MS\) are excluded by adding a Markovian self-loop. As standard for MAs\cite{12}, we impose the maximal progress assumption, i.e., probabilistic transitions take precedence over Markovian ones. Thus, we remove transitions \(s \xrightarrow{\lambda} \mu\) for \(s \in PS\) and \(\lambda \in \mathbb{R}_{>0}\) which yields \(S = PS \cup MS\). MAs with Zeno behavior, where infinitely many actions can be taken within finite time with non-zero probability, are unrealistic and considered a modeling error.

A reward function \(\rho_i\) defines state rewards and action rewards. When sojourning in a state \(s\) for \(t\) time units, the state reward \(\rho_i(s) \cdot t\) is obtained. Upon taking a transition \(s \xrightarrow{\gamma} \mu\), we collect action reward \(\rho_i(s, \gamma)\) (if \(\gamma \in \text{Act}\)) or \(\rho(s, \perp)\) (if \(\gamma \in \mathbb{R}_{>0}\)). For presentation purposes, in the remainder of this section, rewards are omitted. Full definitions with rewards can be found in App.\(A.3\).

**Definition 2 (Markov decision process \cite{29}).** A Markov decision process (MDP) is a tuple \(\mathcal{D} = (S, \text{Act}, \mathbf{P}, s_0, \emptyset)\) with \(S, s_0, \text{Act}\) as in Def.\(7\) and \(\mathbf{P}\): \(S \times \text{Act} \times S \rightarrow [0, 1]\) are the transition probabilities satisfying \(\sum_{s' \in S} \mathbf{P}(s, \alpha, s') \in \{0, 1\}\) for all \(s \in S\) and \(\alpha \in \text{Act}\).

MDPs are MAs without Markovian states and thus without timing aspects, i.e., MDPs exhibit probabilistic branching and non-determinism. Zeno behavior is not a concern, as we do not consider timing aspects. The underlying MDP of an MA abstracts away from its timing:

**Definition 3 (Underlying MDP).** The MDP \(\mathcal{M}_D = (S, \text{Act}, \mathbf{P}, s_0, \emptyset)\) is the underlying MDP of MA \(\mathcal{M} = (S, \text{Act}, \rightarrow, s_0, \emptyset)\) with transition probabilities \(\mathbf{P}\).

The digitization \(\mathcal{M}_\delta\) of \(\mathcal{M}\) w.r.t. some digitization constant \(\delta \in \mathbb{R}_{>0}\) is an MDP which digitizes the time \(\delta\). The main difference between \(\mathcal{M}_D\) and \(\mathcal{M}_\delta\) is that the latter also introduces self-loops which describe the probability to stay in a Markovian state for \(\delta\) time units. More precisely, the outgoing transitions of states \(s \in MS\) in \(\mathcal{M}_\delta\) represent that either (1) a Markovian transition in \(\mathcal{M}\) was taken within \(\delta\) time units, or (2) no transition is taken within \(\delta\) time units – which is captured by taking the self-loop in \(\mathcal{M}_\delta\). Counting the taken self-loops at \(s \in MS\) allows to approximate the sojourn time in \(s\).

**Definition 4 (Digitization of an MA).** For MA \(\mathcal{M} = (S, \text{Act}, \rightarrow, s_0, \emptyset)\) with transition probabilities \(\mathbf{P}\) and digitization constant \(\delta \in \mathbb{R}_{>0}\), the digitization of \(\mathcal{M}\) w.r.t. \(\delta\) is the MDP \(\mathcal{M}_\delta = (S, \text{Act}, \mathbf{P}_\delta, s_0, \emptyset)\) where

\[
\mathbf{P}_\delta(s, \alpha, s') = \begin{cases} 
\mathbf{P}(s, \perp, s') \cdot (1 - e^{-E(s)\delta}) & \text{if } s \in MS, \alpha = \perp, s \neq s' \\
\mathbf{P}(s, \perp, s') \cdot (1 - e^{-E(s)\delta}) + e^{-E(s)\delta} & \text{if } s \in MS, \alpha = \perp, s = s' \\
\mathbf{P}(s, \alpha, s') & \text{otherwise.}
\end{cases}
\]

**Example 2.** Fig.\(2\) shows an MA \(\mathcal{M}\) with its underlying MDP \(\mathcal{M}_D\) and a digitization \(\mathcal{M}_\delta\) for unspecified \(\delta \in \mathbb{R}_{>0}\).
Paths and schedulers. Paths represent runs of $\mathcal{M}$ starting in the initial state. Let $t(\kappa) = 0$ and $\alpha(\kappa) = \kappa$, if $\kappa \in \text{Act}$, and $t(\kappa) = \kappa$ and $\alpha(\kappa) = \bot$, if $\kappa \in \mathbb{R}_{\geq 0}$.

**Definition 5 (Infinite path).** An infinite path of MA $\mathcal{M}$ with transition probabilities $P$ is an infinite sequence $\pi = s_0 \xrightarrow{\kappa_0} s_1 \xrightarrow{\kappa_1} \ldots$ of states $s_0, s_1, \ldots \in S$ and stamps $\kappa_0, \kappa_1, \ldots \in \text{Act} \cup \mathbb{R}_{\geq 0}$ such that (1) $\sum_{i=0}^{\infty} t(\kappa_i) = \infty$, and for any $i\geq 0$ it holds that (2) $P(s_i, \alpha(\kappa_i), s_{i+1}) > 0$, (3) $s_i \in \text{PS}$ implies $\kappa_i \in \text{Act}$, and (4) $s_i \in \text{MS}$ implies $\kappa_i \in \mathbb{R}_{\geq 0}$.

An infix $s_i \xrightarrow{\kappa_i} s_{i+1}$ of a path $\pi$ represents that we stay at $s_i$ for $t(\kappa_i)$ time units and then perform action $\alpha(\kappa_i)$ and move to state $s_{i+1}$. Condition (1) excludes Zeno paths, condition (2) ensures positive transition probabilities, and conditions (3) and (4) assert that stamps $\kappa_i$ match the transition type at $s_i$.

A **finite path** is a finite prefix $\pi' = s_0 \xrightarrow{\kappa_0} \ldots \xrightarrow{\kappa_{n-1}} s_n$ of an infinite path. The **length** of $\pi'$ is $|\pi'| = n$, its **last state** is $\last(\pi') = s_n$, and the **time duration** is $T(\pi') = \sum_{0 \leq i < |\pi'|} t(\kappa_i)$. We denote the sets of finite and infinite paths of $\mathcal{M}$ by $\text{FPaths}^\mathcal{M}$ and $\text{IPaths}^\mathcal{M}$, respectively. The superscript $\mathcal{M}$ is omitted if the model is clear from the context. For a finite or infinite path $\pi = s_0 \xrightarrow{\kappa_0} s_1 \xrightarrow{\kappa_1} \ldots$ the **prefix** of $\pi$ of length $n$ is denoted by $\prefix(\pi, n)$. The $i$th state visited by $\pi$ is given by $\pi[i] = s_i$. The time-abstraction $\text{ta}(\pi)$ of $\pi$ removes all sojourn times and is a path of the underlying MDP $\mathcal{M}_D$: $\text{ta}(\pi) = s_0 \xrightarrow{\alpha(\kappa_0)} s_1 \xrightarrow{\alpha(\kappa_1)} \ldots$. Paths of $\mathcal{M}_D$ are also referred to as the **time-abstract paths** of $\mathcal{M}$.

**Definition 6 (Generic scheduler).** A **scheduler** $\sigma$ for $\mathcal{M}$ is a measurable function $\sigma : \text{FPaths} \times \text{Act} \rightarrow [0, 1]$ such that $\sigma(\pi, \cdot) \in \text{Dist}(\text{Act}(\last(\pi)))$ for each $\pi \in \text{FPaths}$. A scheduler $\sigma$ for $\mathcal{M}$ resolves the non-determinism of $\mathcal{M}$: $\sigma(\pi, \alpha)$ is the probability to take transition $\last(\pi) \xrightarrow{\alpha} \mu$ after observing the run $\pi$. The set of such schedulers is denoted by $\text{GM}^\mathcal{M}$ (GM if $\mathcal{M}$ is clear from the context). $\sigma \in \text{GM}$ is **deterministic** if the distribution $\sigma(\pi, \cdot)$ is Dirac for any $\pi$. Time-abstract schedulers behave independently of the time-stamps of the given path, i.e., $\sigma(\pi, \alpha) = \sigma(\pi', \alpha)$ for all actions $\alpha$ and paths $\pi, \pi'$ with $\text{ta}(\pi) = \text{ta}(\pi')$. We write $\text{TA}^\mathcal{M}$ to denote the set of time-abstract schedulers of $\mathcal{M}$. GM is the most general scheduler class for MAs. For MDPs, the most general scheduler class is TA.

### 2.2 Objectives

An objective $\mathcal{O}_i$ is a representation of a **quantitative** property like the probability to reach an error state, or the expected energy consumption. To express **Boolean** properties (e.g., the probability to reach an error state is below $p_i$), $\mathcal{O}_i$ is combined with a **threshold** $\triangleright_i p_i$ where $\triangleright_i \in \{<, \leq, >, \geq\}$ is a **threshold relation** and $p_i \in \mathbb{R}$ is a **threshold value**. Let $\mathcal{M}, \sigma \models \mathcal{O}_i \triangleright_i p_i$ denote that the MA $\mathcal{M}$ under scheduler $\sigma \in \text{GM}$ satisfies the property $\mathcal{O}_i \triangleright_i p_i$. 5
Reachability objectives. $I \subseteq \mathbb{R}$ is a time interval if it is of the form $I = [a, b]$ or $I = [a, \infty)$, where $0 \leq a < b$. The set of paths reaching a set of goal states $G \subseteq S$ in time $I$ is defined as

$$\diamondsuit^I G = \{ \pi = s_0 \xrightarrow{\kappa_0} s_1 \xrightarrow{\kappa_1} \ldots \in \text{IPaths} \mid \exists n \geq 0: \pi[n] \in G \text{ and } I \cap [t, t + t(\kappa_n)] \neq \emptyset \text{ for } t = T(\text{pref}(\pi, n)) \}.$$ 

We write $\diamondsuit G$ instead of $\diamondsuit^{[0, \infty)} G$. A probability measure $\text{Pr}^M_\sigma$ on sets of infinite paths is defined, which generalizes both the standard probability measure on MDPs and on CTMCs. A formal definition is given in App. A.2.

**Definition 7 (Reachability objective).** A reachability objective has the form $\mathbb{P}(\diamondsuit^I G)$ for time interval $I$ and goal states $G$. The objective is timed if $I \neq [0, \infty)$ and untimed otherwise. For MA $M$ and scheduler $\sigma \in \text{GM}$, let $M, \sigma \models \mathbb{P}(\diamondsuit^I G) \triangleright_i p_i$ iff $\text{Pr}^M_\sigma(\diamondsuit^I G) \triangleright_i p_i$.

**Expected reward objectives.** Expected rewards $\text{ER}^M_\sigma(\rho_j, G)$ define the expected amount of reward collected (w.r.t. $\rho_j$) until a goal state in $G \subseteq S$ is reached. This is a straightforward generalization of the notion on CTMCs and MDPs. A formal definition is found in App. A.2.

**Definition 8 (Expected reward objective).** An expected reward objective has the form $\mathbb{E}(\#j, G)$ where $j$ is the index of reward function $\rho_j$ and $G \subseteq S$. For MA $M$ and scheduler $\sigma \in \text{GM}$, let $M, \sigma \models \mathbb{E}(\#j, G) \triangleright_i p_i$ iff $\text{ER}^M_\sigma(\rho_j, G) \triangleright_i p_i$.

Expected time objectives $\mathbb{E}(T, G)$ are expected reward objectives that consider the reward function $\rho_T$ with $\rho_T(s) = 1$ if $s \in \text{MS}$ and all other rewards are zero.

### 3 Multi-objective Model Checking

Standard model checking considers objectives individually. This approach is not feasible when we are interested in multiple objectives that should be fulfilled by the same scheduler, e.g., a scheduler that maximizes the expected profit might violate certain safety constraints. Multi-objective model checking aims to analyze multiple objectives at once and reveals possible trade-offs.

**Definition 9 (Satisfaction of multiple objectives).** Let $M$ be an MA and $\sigma \in \text{GM}$. For objectives $\mathbb{O} = (\mathbb{O}_1, \ldots, \mathbb{O}_d)$ with threshold relations $\triangleright = (\triangleright_1, \ldots, \triangleright_d) \in \{<, \leq, >, \geq\}^d$ and threshold values $p = (p_1, \ldots, p_d) \in \mathbb{R}^d$ let

$$M, \sigma \models \mathbb{O} \triangleright p \iff M, \sigma \models \mathbb{O}_i \triangleright_i p_i \text{ for all } 1 \leq i \leq d.$$ 

Furthermore, let $\text{achieve}^M(\mathbb{O} \triangleright p) \iff \exists \sigma \in \text{GM} \text{ such that } M, \sigma \models \mathbb{O} \triangleright p$.

If $M, \sigma \models \mathbb{O} \triangleright p$, the point $p \in \mathbb{R}^d$ is achievable in $M$ with scheduler $\sigma$. The set of achievable points of $M$ w.r.t. $\mathbb{O}$ and $p$ is $\{p \in \mathbb{R}^d \mid \text{achieve}^M(\mathbb{O} \triangleright p)\}$. This definition is compatible with the notions on MDPs as given in [15,17].
Example 3. Fig. 3(b) and Fig. 3(c) depict the set of achievable points of the MA $M$ from Fig. 3(a) w.r.t. relations $\triangleright = (\geq, \geq)$ and objectives $(P(\diamond \{s_2\}), P(\diamond \{s_4\}))$ and $(P(\diamond \{s_2\}), P(\diamond^{[0,2]} \{s_4\}))$, respectively. Using the set of achievable points, we can answer Pareto, numerical, and achievability queries as considered in [15], e.g., the Pareto front lies on the border of the set.

Schedulers. For single-objective model checking on MAs, it suffices to consider deterministic schedulers [30]. For untimed reachability and expected rewards even time-abstract deterministic schedulers suffice [30]. Multi-objective model checking on MDPs requires history-dependent, randomized schedulers [17]. On MAs, schedulers may also employ timing information to make optimal choices, even if only untimed objectives are considered.

Example 4. Consider the MA $M$ in Fig. 3(a) with untimed objectives $P(\diamond \{s_2\}) \geq 0.5$ and $P(\diamond \{s_4\}) \geq 0.5$. A simple graph argument yields that both properties are only satisfied if action $\alpha$ is taken with probability exactly a half. Thus, on the underlying MDP, no deterministic scheduler satisfies both objectives. On the MA however, paths can be distinguished by their sojourn time in $s_0$. As the probability mass to stay in $s_0$ for at most $\ln(2)$ is exactly 0.5, a timed scheduler $\sigma$ with $\sigma(s_0 \xrightarrow{t} s_1, \alpha) = 1$ if $t \leq \ln(2)$ and 0 otherwise does satisfy both objectives.

Theorem 1. For some MA $M$ with $\text{achieve}^M(\emptyset \triangleright p)$, no deterministic time-abstract scheduler $\sigma$ satisfies $M$, $\sigma \models \emptyset \triangleright p$.

The geometric shape of the achievable points. Like for MDPs [17], the set of achievable points of any combination of aforementioned objectives is convex.

Proposition 1. The set $\{p \in \mathbb{R}^d \mid \text{achieve}^M(\emptyset \triangleright p)\}$ is convex.

For MDPs, the set of achievable points is a convex polytope where the vertices can be realized by deterministic schedulers that use memory bounded by the number of objectives. As there are finitely many such schedulers, the polytope is finite [17], i.e., it can be represented by a finite number of vertices. This result does not carry over to MAs. For example, the achievable points of the MA from Fig. 3(a) together with the objectives $(P(\diamond \{s_2\}), P(\diamond^{[0,2]} \{s_4\}))$ form the infinite

Fig. 3. Markov automaton and achievable points.
polytope shown in Fig. 3(c). The insight here is that for any sojourn time \( t \leq 2 \) in \( s_0 \), the timing information is relevant for optimal schedulers: The shorter the sojourn time in \( s_0 \), the higher the probability to reach \( s_4 \) within the time bound.

**Theorem 2.** For some MA \( \mathcal{M} \) and objectives \( \mathcal{O} \), the polytope \( \{ p \in \mathbb{R}^d \mid \text{achieve}^\mathcal{M}(\mathcal{O} \triangleright p) \} \) is not finite.

As infinite convex polytopes cannot be represented by a finite number of vertices, any method extending the approach of [15] – which computes these vertices – can only approximate the set of achievable points.

**Problem statement.** For an MA and objectives with threshold relations, construct arbitrarily tight over- and under-approximations of the achievable points.

### 4 Analysis of Markov Automata with Multiple Objectives

The state-of-the-art in single-objective model checking of MA is to reduce the MA to an MDP, cf. [8,9,10], for which efficient algorithms exist. We aim to lift this approach to multi-objective model checking. Assume MA \( \mathcal{M} \) and objectives \( \mathcal{O} \) with threshold relations \( \triangleright \). We discuss how the set of achievable points of \( \mathcal{M} \) relates to the set of achievable points of an MDP. The key challenge is to deal with timing information—even for untimed objectives—and to consider schedulers beyond those optimizing single objectives. We obtain:

- For untimed reachability and expected reward objectives, the achievable points of \( \mathcal{M} \) equal those of its underlying MDP, cf. Theorems 3 and 4.
- For timed reachability objectives, the set of achievable points of a digitized MDP \( \mathcal{M}_\delta \) provides a sound approximation of the achievable points of \( \mathcal{M} \), cf. Theorem 5. Corollary 1 gives the precision of the approximation.

#### 4.1 Untimed Reachability Objectives

Although timing information is essential for deterministic schedulers, cf. Theorem 1, timing information does not strengthen randomized schedulers:

**Theorem 3.** For MA \( \mathcal{M} \) and untimed reachability objectives \( \mathcal{O} \) it holds that \( \text{achieve}^{\mathcal{M}}(\mathcal{O} \triangleright p) \iff \text{achieve}^{\mathcal{M}_\delta}(\mathcal{O} \triangleright p) \).

The main idea for proving Theorem 3 is to construct for scheduler \( \sigma \in \text{GM}^{\mathcal{M}} \) a time-abstract scheduler \( \text{ta}(\sigma) \in \text{TA}^{\mathcal{M}_\delta} \) such that they both induce the same untimed reachability probabilities. To this end, we discuss the connection between probabilities of paths of MA \( \mathcal{M} \) and paths of MDP \( \mathcal{M}_\delta \).

**Definition 10 (Induced paths of a time-abstract path).** The set of induced paths on MA \( \mathcal{M} \) of a path \( \hat{\pi} \) of \( \mathcal{M}_\delta \) is given by

\[
\langle \hat{\pi} \rangle = \text{ta}^{-1}(\hat{\pi}) = \{ \pi \in \text{FPaths}^{\mathcal{M}} \cup \text{IPaths}^{\mathcal{M}} \mid \text{ta}(\pi) = \hat{\pi} \}.
\]
The set $\langle \hat{\pi} \rangle$ contains all paths of $M$ where replacing sojourn times by $\perp$ yields $\hat{\pi}$.

For $\sigma \in GM$, the probability distribution $\sigma(\pi, \cdot) \in Dist(Act)$ might depend on the sojourn times of the path $\pi$. The time-abstract scheduler $ta(\sigma)$ weights the distribution $\sigma(\pi, \cdot)$ with the probability masses of the paths $\pi \in \langle \hat{\pi} \rangle$.

**Definition 11 (Time-abstraction of a scheduler).** The time-abstraction of $\sigma \in GM$ is defined as $ta(\sigma) \in TA_{MD}$ such that for any $\hat{\pi} \in FPaths^{MD}$

$$ta(\sigma)(\hat{\pi}, \alpha) = \int_{\pi \in \langle \hat{\pi} \rangle} \sigma(\pi, \alpha) \, dPr^{MD}_{\sigma}(\pi | \langle \hat{\pi} \rangle).$$

The term $Pr^{MD}_{\sigma}(\pi | \langle \hat{\pi} \rangle)$ represents the probability for a path in $\langle \hat{\pi} \rangle$ to have sojourn times as given by $\pi$. The value $ta(\sigma)(\hat{\pi}, \alpha)$ coincides with the probability that $\sigma$ picks action $\alpha$, given that the time-abstract path $\hat{\pi}$ was observed.

**Example 5.** Consider the MA $M$ in Fig. 2(a) and the scheduler $\sigma$ choosing $\alpha$ at state $s_3$ iff the sojourn time at $s_0$ is at most one. Then $ta(\sigma)(s_0 \perp \rightarrow s_3, \alpha) = 1 - e^{-E(s_0)}$, the probability that $s_0$ is left within one time unit. For $\bar{\pi} = s_0 \perp \alpha \rightarrow s_6$ we have

$$Pr^{MD}_{\sigma}(\Diamond \{s_6\}) = Pr^{MD}_{\sigma}(\langle \bar{\pi} \rangle) = 1 - e^{-E(s_0)} = Pr^{MD}_{ta(\sigma)}(\bar{\pi}) = Pr^{MD}_{ta(\sigma)}(\Diamond \{s_6\}).$$

In the example, the considered scheduler and its time-abstraction induce the same untimed reachability probabilities. We generalize this observation.

**Lemma 1.** For any $\bar{\pi} \in FPaths^{MD}$ we have $Pr^{MD}_{\sigma}(\langle \bar{\pi} \rangle) = Pr^{MD}_{ta(\sigma)}(\bar{\pi})$.

The result is lifted to untimed reachability probabilities.

**Proposition 2.** For any $G \subseteq S$ it holds that $Pr^{MD}_{\sigma}(\Diamond G) = Pr^{MD}_{ta(\sigma)}(\Diamond G)$.

As the definition of $ta(\sigma)$ is independent of the considered set of goal states $G \subseteq S$, Proposition 2 can be lifted to multiple untimed reachability objectives.

**Proof of Theorem 3 (sketch).** By applying Proposition 2 we can show that $M, \sigma \models \Diamond \triangleright p \iff M_{MD}, ta(\sigma) \models \Diamond \triangleright p$ for any scheduler $\sigma \in GM$ and untimed reachability objectives $\Diamond = (\Diamond G_1), \ldots, \Diamond (\Diamond G_d)$ with thresholds $\triangleright p$. Theorem 3 is a direct consequence of this.

### 4.2 Expected Reward Objectives

The results for expected reward objectives are similar to untimed reachability objectives: An analysis of the underlying MDP suffices. We show the following extension of Theorem 3 to expected reward objectives.

**Theorem 4.** For MA $M$ and untimed reachability and expected reward objectives $\Diamond$: achieve$^{MD}(\Diamond \triangleright p) \iff$ achieve$^{MD}(\Diamond \triangleright p)$.
To prove this, we show that a scheduler \( \sigma \in \text{GM}^M \) and its time-abstraction \( \text{ta}(\sigma) \in \text{TA} \) induce the same expected rewards on \( M \) and \( M_D \), respectively. Theorem 4 follows then analogously to Theorem 3.

**Proposition 3.** Let \( \rho \) be some reward function of \( M \) and let \( \rho^D \) be its counter-part for \( M_D \). For \( G \subseteq S \) we have \( \text{ER}_\sigma^M(\rho, G) = \text{ER}_{\text{ta}(\sigma)}^{M_D}(\rho^D, G) \).

Notice that \( \rho^D \) encodes the expected reward of \( M \) obtained in a state \( s \) by assuming the sojourn time to be the expected sojourn time \( 1/E(s) \). Although the claim is similar to Proposition 2 its proof cannot be adapted straightforwardly. In particular, the analogon to Lemma 1 does not hold: The expected reward collected along a time-abstract path \( \check{\pi} \in \text{FPaths}^{M_D} \) does in general not coincide for \( M \) and \( M_D \).

**Example 6.** We consider standard notations for rewards as detailed in App. A.2. Let \( M \) be the MA with underlying MDP \( M_D \) as shown in Fig. 2. Let \( \rho(s_0) = 1 \) and zero otherwise. Reconsider the scheduler \( \sigma \) from Example 5. Let \( \check{\pi}_\alpha = s_0 \xrightarrow{1} s_3 \xrightarrow{2} s_6 \). The probability \( \text{Pr}_{\pi}^M(\{s_0 \xrightarrow{t} s_3 \xrightarrow{t'} s_6 \mid t > 1\}) \) is zero since \( \sigma \) chooses \( \beta \) on such paths. For the remaining paths in \( \langle \check{\pi}_\alpha \rangle \), action \( \alpha \) is chosen with probability one. The expected reward in \( M \) along \( \check{\pi}_\alpha \) is:

\[
\int_{\pi \in \langle \check{\pi}_\alpha \rangle} \text{rew}^M(\rho, \pi) \ d\text{Pr}_\pi^M(\pi) = \int_0^1 \rho(s_0) \cdot t \cdot E(s_0) \cdot e^{-E(s_0)t} \ dt = 1 - 2e^{-1}.
\]

The expected reward in \( M_D \) along \( \check{\pi}_\alpha \) differs as

\[
\text{rew}^M_D(\rho^D, \check{\pi}_\alpha) \cdot \text{Pr}_{\text{ta}(\sigma)}^{M_D}(\check{\pi}_\alpha) = \rho^D(s_0, \perp) \cdot \text{ta}(\sigma)(s_0 \xrightarrow{1} s_3, \alpha) = 1 - e^{-1}.
\]

The intuition is as follows: If path \( s_0 \xrightarrow{t} s_3 \xrightarrow{t'} s_6 \) of \( M \) under \( \sigma \) occurs, we have \( t \leq 1 \) since \( \sigma \) chose \( \alpha \). Hence, the reward collected from paths in \( \langle \check{\pi}_\alpha \rangle \) is at most \( 1 \cdot \rho(s_0) = 1 \). There is thus a dependency between the choice of the scheduler at \( s_3 \) and the collected reward at \( s_0 \). This dependency is absent in \( M_D \) as the reward at a state is independent of the subsequent performed actions.

Let \( \check{\pi}_\beta = s_0 \xrightarrow{1} s_3 \xrightarrow{\beta} s_4 \). The expected reward along \( \check{\pi}_\beta \) is \( 2e^{-1} \) for \( M \) and \( e^{-1} \) for \( M_D \). As the rewards for \( \check{\pi}_\alpha \) and \( \check{\pi}_\beta \) sum up to one in both \( M \) and \( M_D \), the expected reward along all paths of length two coincides for \( M \) and \( M_D \).

This observation can be generalized to arbitrary MA and paths of arbitrary length.

**Proof of Proposition 3 (sketch).** For every \( n \geq 0 \), the expected reward collected along paths of length at most \( n \) coincides for \( M \) under \( \sigma \) and \( M_D \) under \( \text{ta}(\sigma) \). The proposition follows by letting \( n \) approach infinity.

Thus, queries on MA with mixtures of untimed reachability and expected reward objectives can be analyzed on the underlying MDP \( M_D \).
4.3 Timed Reachability Objectives

Timed reachability objectives cannot be analyzed on $\mathcal{M}_{\mathcal{D}}$ as it abstracts away from sojourn times. We lift the digitization approach for single-objective timed reachability \cite{DBLP:journals/tocl/ChatterjeeDG09} to multiple objectives. Instead of abstracting timing information, it is digitized. Let $\mathcal{M}_\delta$ denote the digitization of $\mathcal{M}$ for arbitrary digitization constant $\delta \in \mathbb{R}_{>0}$, see Def.\ref{df:digitization}. A time interval $I \subseteq \mathbb{R}_{\geq 0}$ of the form $[a, \infty)$ or $[a, b]$ with $a/\delta = d_a \in \mathbb{N}$ and $b/\delta = d_b \in \mathbb{N}$ is called well-formed. For the remainder, we only consider well-formed intervals, ensured by an appropriate digitization constant. An interval for time-bounds $I$ is transformed to digitization step bounds $\text{di}(I) \subseteq \mathbb{N}$. Let $a = \inf I$, we set $\text{di}(I) = \{ i/\delta \in \mathbb{N} \mid t \in I \} \setminus \{ 0 \mid a > 0 \}$.

We first relate paths in $\mathcal{M}$ to paths in its digitization.

\begin{definition}[Digitization of a path] The digitization $\text{di}(\pi)$ of path $\pi = s_0 \xrightarrow{\kappa_0} s_1 \xrightarrow{\kappa_1} \ldots$ in $\mathcal{M}$ is the path in $\mathcal{M}_\delta$ given by

$$\text{di}(\pi) = (s_0 \xrightarrow{\alpha(\kappa_0)} s_0) \xrightarrow{\alpha(\kappa_1)} \ldots$$

where $m_i = \max\{m \in \mathbb{N} \mid m\delta \leq t(\kappa_i)\}$ for each $i \geq 0$.
\end{definition}

\begin{example}
For the path $\pi = s_0 \xrightarrow{1.1} s_3 \xrightarrow{0.3} s_4 \xrightarrow{0.3} s_5 \xrightarrow{0.3} s_4$ of the MA $\mathcal{M}$ in Fig. 2(a) and $\delta = 0.4$, we get $\text{di}(\pi) = s_0 \xrightarrow{1} s_0 \xrightarrow{1} s_0 \xrightarrow{1} s_0 \xrightarrow{1} s_3 \xrightarrow{1} s_4 \xrightarrow{1} s_5 \xrightarrow{1} s_4$.
\end{example}

The $m_i$ in the definition above represent a digitization of the sojourn times $t(\kappa_i)$ such that $m_i\delta \leq t(\kappa_i) < (m_i+1)\delta$. These digitized times are incorporated into the digitization of a path by taking the self-loop at state $s_i \in \text{MS} m_i$ times. We also refer to the paths of $\mathcal{M}_\delta$ as digital paths (of $\mathcal{M}$). The number $|\pi|_{\text{ds}}$ of digitization steps of a digital path $\bar{\pi}$ is the number of transitions emerging from Markovian states, i.e., $|\bar{\pi}|_{\text{ds}} = \{|i < |\pi| \mid \pi[i] \in \text{MS}\}$. One digitization step represents the elapse of at most $\delta$ time units—either by staying at some $s \in \text{MS}$ for $\delta$ time or by leaving $s$ within $\delta$ time. The number $|\text{di}(\pi)|_{\text{ds}}$ multiplied with $\delta$ yields an estimate for the duration $T(\bar{\pi})$. A digital path $\bar{\pi}$ can be interpreted as representation of the set of paths of $\mathcal{M}$ whose digitization is $\bar{\pi}$.

\begin{definition}[Induced paths of a digital path] The set of induced paths of a (finite or infinite) digital path $\bar{\pi}$ of $\mathcal{M}_\delta$ is

$$[\bar{\pi}] = \text{di}^{-1}(\bar{\pi}) = \{ \pi \in \text{FPaths}^\mathcal{M} \cup \text{IPaths}^\mathcal{M} \mid \text{di}(\pi) = \bar{\pi} \}.$$ 

For sets of digital paths $\Pi$ we define the induced paths $[\Pi] = \bigcup_{\bar{\pi} \in \Pi} [\bar{\pi}]$. To relate timed reachability probabilities for $\mathcal{M}$ under scheduler $\sigma \in \text{GM}^\mathcal{M}$ with $\text{ds}$-bounded reachability probabilities for $\mathcal{M}_\delta$, relating $\sigma$ to a scheduler for $\mathcal{M}_\delta$ is necessary.

\begin{definition}[Digitization of a scheduler] The digitization of $\sigma \in \text{GM}^\mathcal{M}$ is given by $\text{di}(\sigma) \in \text{TA}^\mathcal{M}_\delta$ such that for any $\bar{\pi} \in \text{FPaths}^\mathcal{M}_\delta$ with last($\bar{\pi}$) $\in \text{PS}$

$$\text{di}(\sigma)(\bar{\pi}, \alpha) = \int_{\pi \in [\bar{\pi}]} \sigma(\pi, \alpha) \text{Pr}^\mathcal{M}_\sigma(\pi \mid [\bar{\pi}]).$$

\end{definition}
The digitization $\text{di}(\sigma)$ is similar to the time-abstraction $\text{ta}(\sigma)$ as both schedulers get a path with restricted timing information as input and mimic the choice of $\sigma$. However, while $\text{ta}(\sigma)$ receives no information regarding sojourn times, $\text{di}(\sigma)$ receives the digital estimate. Intuitively, $\text{di}(\sigma)(\bar{\pi}, \alpha)$ considers $\sigma(\pi, \alpha)$ for each $\pi \in [\bar{\pi}]$, weighted with the probability that the sojourn times of a path in $[\bar{\pi}]$ are as given by $\pi$. The restriction $\text{last}(\bar{\pi}) \in \text{PS}$ asserts that $\bar{\pi}$ does not end with a self-loop on a Markovian state, implying $[\bar{\pi}] \neq \emptyset$.

**Example 8.** Let MA $\mathcal{M}$ in Fig. 2(a) and $\delta = 0.4$. Again, $\sigma \in \text{GM}^\mathcal{M}$ chooses $\alpha$ at state $s_3$ iff the sojourn time at $s_0$ is at most one. Consider the digital paths $\bar{\pi}_m = (s_0 \overset{t}{\rightarrow})^m s_0 \overset{1}{\rightarrow} s_3$. For $\pi \in [\bar{\pi}_1] = \{s_0 \overset{t}{\rightarrow} s_3 \mid 0.4 \leq t < 0.8\}$ we have $\sigma(\pi, \alpha) = 1$. It follows $\text{di}(\sigma)(\bar{\pi}_1, \alpha) = 1$. For $\pi \in [\bar{\pi}_2] = \{s_0 \overset{1}{\rightarrow} s_3 \mid 0.8 \leq t < 1.2\}$ it is unclear whether $\sigma$ chooses $\alpha$ or $\beta$. Hence, $\text{di}(\sigma)$ randomly guesses:

$$\text{di}(\sigma)(\bar{\pi}_2, \alpha) = \int_{\pi \in [\bar{\pi}_2]} \sigma(\pi, \alpha) \text{dPr}^M(\pi \mid [\bar{\pi}_2]) = \frac{\int_{0.8}^{1} E(s_0)e^{-E(s_0)t} \text{d}t}{\int_{0.8}^{1} E(s_0)e^{-E(s_0)t} \text{d}t} \approx 0.55.$$  

On $\mathcal{M}_\delta$ we consider ds-bounded reachability instead of timed reachability.

**Definition 15 (ds-bounded reachability).** The set of infinite digital paths that reach $G \subseteq S$ within the interval $J \subseteq \mathbb{N}$ of consecutive natural numbers is

$$\hat{\bigcirc}^J_{\text{ds}}G = \{\pi \in \text{IPaths}^\mathcal{M}_\delta \mid \exists n \geq 0: \bar{\pi}[n] \in G \text{ and } \text{pref}(\bar{\pi}, n)_{\text{ds}} \in J\}.$$  

The timed reachability probabilities for $\mathcal{M}$ are estimated by ds-bounded reachability probabilities for $\mathcal{M}_\delta$. The induced ds-bounded reachability probability for $\mathcal{M}$ (under $\sigma$) coincides with ds-bounded reachability probability on $\mathcal{M}_\delta$ (under $\text{di}(\sigma)$).

**Proposition 4.** Let $\mathcal{M}$ be an MA with $G \subseteq S$, $\sigma \in \text{GM}$, and digitization $\mathcal{M}_\delta$. Further, let $J \subseteq \mathbb{N}$ be a set of consecutive natural numbers. It holds that

$$\text{Pr}^M(\hat{\bigcirc}^J_{\text{ds}}G) = \text{Pr}^M_{\text{di}(\sigma)}(\hat{\bigcirc}^J_{\text{ds}}G).$$  

Thus, induced ds-bounded reachability on MAs can be computed on their digitization.

Next, we relate ds-bounded and timed reachability on MAs, i.e., we quantify the maximum difference between time-bounded and ds-bounded reachability probabilities. Let $\lambda = \max\{E(s) \mid s \in \text{MS}\}$ be the maximum exit rate. For $\alpha \neq 0$:

$$\varepsilon^\downarrow([a, b]) = 1 - (1 + \lambda \delta)^{\text{dis}} \cdot e^{-\lambda a}, \quad \varepsilon^\uparrow([a, b]) = 1 - (1 + \lambda \delta)^{\text{dis}} \cdot e^{-\lambda b} + 1 - e^{-\lambda \delta},$$

and $\varepsilon^\downarrow([0, \infty)) = \varepsilon^\uparrow([0, \infty)) = \varepsilon^\downarrow([0, \infty)) = 0$. $\varepsilon^\downarrow(I)$ and $\varepsilon^\uparrow(I)$ approach 0 for small digitization constants $\delta \in \mathbb{R}_{>0}$.

**Proposition 5.** For MA $\mathcal{M}$, scheduler $\sigma \in \text{GM}$, goal states $G \subseteq S$, digitization constant $\delta \in \mathbb{R}_{>0}$ and time interval $I$

$$\text{Pr}^M(\hat{\bigcirc}^I G) \in \text{Pr}^M(\hat{\bigcirc}^I_{\text{ds}}G) + \left[-\varepsilon^\downarrow(I), \varepsilon^\uparrow(I)\right]$$
This generalizes existing results \cite{8,9} that only consider schedulers which maximize (or minimize) the corresponding probabilities. More details are given in App. F.

Example 9. Let $\mathbb{O} = (\mathbb{P}(O^1 G_1), \mathbb{P}(O^2 G_2))$ be two timed reachability objectives for an MA $\mathcal{M}$ with digitization $\mathcal{M}_\delta$ such that $\varepsilon^{+}_1 = 0.13$, $\varepsilon^{+}_2 = 0.22$, $\varepsilon^{+}_2 = 0.07$, and $\varepsilon^{+}_2 = 0.15$. The blue rectangle in Fig. 5(a) illustrates the set $\varepsilon(\mathbb{O}, \mathbf{p})$ for the point $\mathbf{p} = (0.4, 0.3)$. Assume $\text{achieve}^{\mathcal{M}_\delta}(\mathbb{O} \triangleright \mathbf{p})$ holds for threshold relations $\triangleright = \{\geq, \geq\}$, i.e., $\mathbf{p}$ is achievable for the digitization $\mathcal{M}_\delta$. From Cor. 1 we infer that $\varepsilon(\mathbb{O}, \mathbf{p})$ contains at least one point $\mathbf{p}'$ that is achievable for $\mathcal{M}$. Hence, the bottom left corner point of the rectangle is achievable for $\mathcal{M}$. This holds for any rectangle $\varepsilon(\mathbb{O}, \mathbf{q})$ with $\mathbf{q} \in A$, where $A$ is the set of achievable points of $\mathcal{M}_\delta$ denoted by the gray area$^1$ in Fig. 5(b). It follows that any point in $A^-$ (depicted

\footnote{In the figure, $A^-$ partly overlaps $A$, i.e., the green area also belongs to $A$.}
by the green area) is achievable for $\mathcal{M}$. On the other hand, an achievable point of $\mathcal{M}$ has to be contained in a set $\varepsilon(\emptyset, \mathbf{q})$ for at least one $\mathbf{q} \in A$. The red area depicts the points $\mathbb{R}^d \setminus A^+$ for which this is not the case, i.e., points that are not achievable for $\mathcal{M}$. The digitization constant $\delta$ controls the accuracy of the resulting approximation. Fig. 5(c) depicts a possible result when a smaller digitization constant $\tilde{\delta} < \delta$ is considered.

The observations from the example above are formalized in the following theorem. The theorem also covers unbounded reachability objectives by considering the time interval $I = [0, \infty)$. For expected reward objectives of the form $E(\# j, G)$ it can be shown that $ER_{\mathcal{M}}(\rho_j, G) = ER_{\mathcal{M}_\delta}(\rho_j^\delta, G)$. This claim is similar to Proposition 3 and can be shown analogously. This enables multi-objective model checking of MAs with timed reachability objectives.

**Theorem 5.** Let $\mathcal{M}$ be an MA with digitization $\mathcal{M}_\delta$. Furthermore, let $\emptyset$ be (un)timed reachability or expected reward objectives with threshold relations $\triangleright$ and $|\emptyset| = d$. It holds that $A^- \subseteq \{ \mathbf{p} \in \mathbb{R}^d \mid \text{achieve}^{\mathcal{M}}(\emptyset \triangleright \mathbf{p}) \} \subseteq A^+$ with:

$$A^- = \{ \mathbf{p}' \in \mathbb{R}^d \mid \forall \mathbf{p} \in \mathbb{R}^d : \mathbf{p}' \in \varepsilon(\emptyset, \mathbf{p}) \text{ implies achieve}^{\mathcal{M}_\delta}(\emptyset \triangleright \mathbf{p}) \}$$

and

$$A^+ = \{ \mathbf{p}' \in \mathbb{R}^d \mid \exists \mathbf{p} \in \mathbb{R}^d : \mathbf{p}' \in \varepsilon(\emptyset, \mathbf{p}) \text{ and achieve}^{\mathcal{M}_\delta}(\emptyset \triangleright \mathbf{p}) \}.$$

### 5 Experimental Evaluation

**Implementation.** We implemented multi-objective model checking of MAs into Storm [31]. The input model is given in the PRISM language[2] and translated into a sparse representation. For MA $\mathcal{M}$, the implementation performs a multi-objective analysis on the underlying MDP $\mathcal{M}_D$ or a digitization $\mathcal{M}_\delta$ and infers (an approximation of) the achievable points of $\mathcal{M}$ by exploiting the results from Sect. 4. For computing the achievable points of $\mathcal{M}_D$ and $\mathcal{M}_\delta$, we apply the approach of [15]. It repeatedly checks weighted combinations of the objectives (by means of value iteration [29] – a standard technique in single-objective MDP model checking) to refine an approximation of the set of achievable points. This procedure is extended as follows. Full details can be found in [32].

---

[2] We slightly extend the PRISM language in order to describe MAs.
We support ds-bounded reachability objectives by combining the approach of [15] (which supports step-bounded reachability on MDPs) with techniques from single-objective MA analysis [8]. Roughly, we reduce ds-bounded reachability to untimed reachability by storing the digitized time-epoch (i.e., the current number of digitization steps) into the state space. A blow-up of the resulting model is avoided by considering each time-epoch separately.

In contrast to [15], we allow a simultaneous analysis of minimizing and maximizing expected reward objectives. This is achieved by performing additional preprocessing steps that comprise an analysis of end components.

**Setup.** Our implementation uses a single core (2GHz) of a 48-core HP BL685C G7 limited to 20GB RAM. The timeout (TO) is two hours. For a model, a set of objectives, and a precision \( \eta \in \mathbb{R} > 0 \), we measure the time to compute an \( \eta \)-approximation of the set of achievable points. This setup coincides with Pareto queries as discussed in [15]. The digitization constant \( \delta \) is chosen heuristically such that recalculations with smaller constants \( \delta' < \delta \) are avoided. We set the precision for value-iteration to \( \varepsilon = 10^{-6} \). We use classical value iteration; the use of improved algorithms [33] is left for future work.

The source code including all material to reproduce the experiments is available at [http://www.stormchecker.org/benchmarks.html](http://www.stormchecker.org/benchmarks.html).

**Results for MAs.** We consider four case studies: (i) a job scheduler [13], see Sect. 1; (ii) a polling system [34, 35] containing a server processing jobs that ar-

---

**Table 1.** Experimental results for multi-objective MAs.

| benchmark   | N(-K$_\eta$) | #states log$_{10}(n)$ | (\( \langle \cdot, \mathcal{A}, \phi \rangle \)) | (\( \langle \cdot, \mathcal{E}, \phi \rangle \)) | (\( \langle \cdot, \mathcal{E}, \phi \rangle \)) | (\( \langle \cdot, \mathcal{E}, \phi \rangle \)) |
|-------------|--------------|------------------------|-----------------------------------------------|-----------------------------------------------|-----------------------------------------------|-----------------------------------------------|
| job scheduling | 10-2 | 12554 | 9 | 1.8 | 9 | 41 | 15 | 435 | 16 | 132 |
| | 12-3 | 116814 | 2 | 11 | 42 | 9 | 798 | 21 | 2026 | TO |
| | 17-2 | 4.6 \cdot 10^6 | 3 | 53 | 323 | TO | TO | TO |
| polling | 3-2 | 1020 | 4 | 0.3 | 5 | 0.8 | 3 | 130 | 12 | 669 |
| | 3-3 | 9858 | 1 | 5 | 1.3 | 8 | 23 | 2530 | TO |
| | 4-4 | 827735 | 3 | 10 | 963 | 20 | 4349 | TO | TO |
| stream | 30 | 1426 | 2 | 31 | 50 | 15 | 5830 | 16 | 4050 | TO |
| | 250 | 94376 | 3 | 90 | 184 | TO | TO | TO |
| | 1000 | 1.5 \cdot 10^6 | 3 | 41 | 3765 | TO | TO | TO |
| mutex | 2 | 13476 | 2 | 16 | 391 | 13 | 1166 | TO |
| | 3 | 38453 | 2 | 13 | 2739 | TO |

---

3 An \( \eta \)-approximation of \( A \subseteq \mathbb{R}^d \) is given by \( A^{-}, A^{+} \subseteq \mathbb{R}^d \) with \( A^{-} \subseteq A \subseteq A^{+} \) and for all \( p \in A^{+} \) exists a \( q \in A^{-} \) such that the distance between \( p \) and \( q \) is at most \( \eta \).
We considered multi-objective verification of Markov automata, including in particular timed reachability objectives. The next step is to apply our algorithms to the manifold applications of MA, such as generalized stochastic Petri nets to enrich the analysis possibilities of such nets.
References

1. Eisentraut, C., Hermanns, H., Zhang, L.: On probabilistic automata in continuous time. In: Proc. of LICS, IEEE CS (2010) 342–351
2. Deng, Y., Hennessy, M.: On the semantics of Markov automata. Inf. Comput. 222 (2013) 139–168
3. Boudali, H., Crouzen, P., Stoelinga, M.: A rigorous, compositional, and extensible framework for dynamic fault tree analysis. IEEE Trans. Dependable Sec. Comput. 7(2) (2010) 128–143
4. Coste, N., Hermanns, H., Lantreibcq, E., Serwe, W.: Towards performance prediction of compositional models in industrial GALS designs. In: Proc. of CAV. Vol. 5643 LNCS, Springer (2009) 204–218
5. Katoen, J.P., Wu, H.: Probabilistic model checking for uncertain scenario-aware data flow. ACM Trans. Embedded Comput. Sys. 22(1) (2016) 15:1–15:27
6. Bozzano, M., Cimatti, A., Katoen, J.P., Nguyen, V.Y., Noll, T., Roveri, M.: Safety, dependability and performance analysis of extended AADL models. Comput. J. 54(5) (2011) 754–775
7. Eisentraut, C., Hermanns, H., Katoen, J.P., Zhang, L.: A semantics for every GSPN. In: Petri Nets. Vol. 7927 LNCS, Springer (2013) 90–109
8. Hatefi, H., Hermanns, H.: Model checking algorithms for Markov automata. ECEASST 53 (2012)
9. Guck, D., Hatefi, H., Hermanns, H., Katoen, J.P., Timmer, M.: Analysis of timed and long-run objectives for Markov automata. LMCS 10(3) (2014)
10. Guck, D., Timmer, M., Hatefi, H., Ruijters, E., Stoelinga, M.: Modelling and analysis of Markov reward automata. In: Proc. of ATVA. Vol. 8837 LNCS, Springer (2014) 168–184
11. Hatefi, H., Braitling, B., Wimmer, R., Fioriti, L.M.F., Hermanns, H., Becker, B.: Cost vs. time in stochastic games and Markov automata. In: Proc. of SETTA. Vol. 9409 LNCS, Springer (2015) 19–34
12. Butkova, Y., Wimmer, R., Hermanns, H.: Long-run rewards for Markov automata. In: Proc. of TACAS. LNCS, Springer (2017) To appear.
13. Bruno, J.L., Downey, P.J., Frederickson, G.N.: Sequencing tasks with exponential service times to minimize the expected flow time or makespan. J. ACM 28(1) (1981) 100–113
14. Kwiatkowska, M., Norman, G., Parker, D.: PRISM 4.0: Verification of probabilistic real-time systems. In: Proc. of CAV. Vol. 6806 LNCS, Springer (2011) 585–591
15. Foréjt, V., Kwiatkowska, M., Parker, D.: Pareto curves for probabilistic model checking. In: Proc. of ATVA. Vol. 7561 LNCS, Springer (2012) 317–332
16. Roijers, D.M., Vamplew, P., Whiteson, S., Dazeley, R.: A survey of multi-objective sequential decision-making. J. Artif. Intell. Res. 48 (2013) 67–113
17. Etessami, K., Kwiatkowska, M.Z., Vardi, M.Y., Yannakakis, M.: Multi-objective model checking of Markov decision processes. LMCS 4(4) (2008)
18. Foréjt, V., Kwiatkowska, M.Z., Norman, G., Parker, D., Qu, H.: Quantitative multi-objective verification for probabilistic systems. In: Proc. of TACAS. Vol. 6605 LNCS, Springer (2011) 112–127
19. Bruyère, V., Filiot, E., Randour, M., Raskin, J.F.: Meet your expectations with guarantees: Beyond worst-case synthesis in quantitative games. In: Proc. of STACS. Vol. 25 LIPIcs, Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik (2014) 199–213
20. Baier, C., Dubslaff, C., Klüppelholz, S.: Trade-off analysis meets probabilistic model checking. In: CSL-LICS, ACM (2014) 1:1–1:10
21. Brázil, T., Chatterjee, K., Forejt, V., Kucera, A.: Trading performance for stability in Markov decision processes. J. Comput. Syst. Sci. 84 (2017) 144–170
22. Brázil, T., Brozek, V., Chatterjee, K., Forejt, V., Kucera, A.: Markov decision processes with multiple long-run average objectives. LMCS 10(1) (2014)
23. Basset, N., Kwiatkowska, M.Z., Topcu, U., Wiltsche, C.: Strategy synthesis for stochastic games with multiple long-run objectives. In: Proc. of TACAS. Vol. 9035 LNCS, Springer (2015) 256–271
24. Teichteil-Königsbuch, F.: Path-constrained Markov decision processes: bridging the gap between probabilistic model-checking and decision-theoretic planning. In: Proc. of ECAL Vol. 242 Frontiers in AI and Applications, IOS Press (2012) 744–749
25. Randour, M., Raskin, J.F., Sankur, O.: Variations on the stochastic shortest path problem. In: Proc. of VMCAI. Vol. 8931 LNCS, Springer (2015) 1–18
26. Junges, S., Jansen, N., Dehnert, C., Topcu, U., Katoen, J.P.: Safety-constrained reinforcement learning for mdps. In: Proc. of TACAS. Vol. 9636 LNCS, Springer (2016) 130–146
27. David, A., Jensen, P.G., Larsen, K.G., Legay, A., Lime, D., Sørensen, M.G., Taankvist, J.H.: On time with minimal expected cost! In: Proc. of ATVA. Vol. 8837 LNCS, Springer (2014) 129–145
28. Chen, T., Forejt, V., Kwiatkowska, M.Z., Simaitis, A., Wiltsche, C.: On stochastic games with multiple objectives. In: Proc. of MFCS. Vol. 8087 LNCS, Springer (2013) 266–277
29. Puterman, M.L.: Markov Decision Processes: Discrete Stochastic Dynamic Programming. John Wiley and Sons (1994)
30. Neuhäußer, M.R., Stoelinga, M., Katoen, J.P.: Delayed nondeterminism in continuous-time Markov decision processes. In: Proc. of FOSSACS. Vol. 5504 LNCS, Springer (2009) 364–379
31. Dehnert, C., Junges, S., Katoen, J.P., Volk, M.: A Storm is coming: A modern probabilistic model checker. In: Proc. of CAV. (2017)
32. Tim Quatmann: Multi-objective model checking of Markov Automata. Master’s thesis, RWTH Aachen University (2016)
33. Haddad, S., Monmege, B.: Reachability in MDPs: Refining convergence of value iteration. In: RP. Vol. 8762 LNCS, Springer (2014) 125–137
34. Srinivasan, M.M.: Nondeterministic polling systems. Management Science 37(6) (1991) 667–681
35. Timmer, M., Katoen, J.P., van de Pol, J., Stoelinga, M.: Efficient modelling and generation of Markov automata. In: Proc. of CONCUR. Vol. 7454 LNCS, Springer (2012) 364–379
36. Pnueli, A., Zuck, L.: Verification of multiprocess probabilistic protocols. Distributed Computing 1(1) (1986) 53–72
37. Neuhäußer, M.R.: Model checking Nondeterministic and Randomly Timed Systems. PhD thesis, RWTH Aachen University (2010)
38. Ash, R.B., Doléans-Dade, C.: Probability and Measure Theory. Harcourt/Academic Press (2000)
A Additional Preliminaries

A.1 Models with Rewards

We extend the models with rewards.

Definition 16 (Markov decision process [29]). A Markov decision process (MDP) is a tuple $D = (S, Act, P, s_0, \{\rho_1, \ldots, \rho_\ell\})$, where $S, s_0, Act, \ell$ are as in Definition [3], $\rho_1, \ldots, \rho_\ell$ are action reward functions $\rho_i : S \times Act \rightarrow \mathbb{R}_{\geq 0}$, and $P : S \times Act \times S \rightarrow [0, 1]$ is a transition probability function satisfying $\sum_{s' \in S} P(s, \alpha, s') \in \{0, 1\}$ for all $s \in S$ and $\alpha \in Act$.

The reward $\rho(s, \alpha)$ is collected when choosing action $\alpha$ at state $s$. Note that we do not consider state rewards for MDPs.

Definition 17 (Underlying MDP). For MA $M = (S, Act, \rightarrow, s_0, \{\rho_1, \ldots, \rho_\ell\})$ with transition probabilities $P$ the underlying MDP of $M$ is given by $M_D = (S, Act, P, s_0, \{\rho_1^D, \ldots, \rho_\ell^D\})$, where for each $i \in \{1, \ldots, \ell\}$

$$
\rho_i^D(s, \alpha) = \begin{cases} 
\rho_i(s, \alpha) & \text{if } s \in PS \\
\rho_i(s, \bot) + \frac{1}{E(s)} \cdot \rho_i(s) & \text{if } s \in MS \text{ and } \alpha = \bot \\
0 & \text{otherwise.}
\end{cases}
$$

The reward functions $\rho_1^D, \ldots, \rho_\ell^D$ incorporate the action and state rewards of $M$ where the state rewards are multiplied with the expected sojourn times $\frac{1}{E(s)}$ of states $s \in MS$.

Definition 18 (Digitization of an MA). For an MA $M = (S, Act, \rightarrow, s_0, \{\rho_1, \ldots, \rho_\ell\})$ with transition probabilities $P$ and a digitization constant $\delta \in \mathbb{R}_{> 0}$, the digitization of $M$ w.r.t. $\delta$ is given by the MDP $M_\delta = (S, Act, P_\delta, s_0, \{\rho_1^\delta, \ldots, \rho_\ell^\delta\})$, where $P_\delta$ is as in Definition [3] and for each $i \in \{1, \ldots, \ell\}$

$$
\rho_i^\delta(s, \alpha) = \begin{cases} 
\rho_i(s, \alpha) & \text{if } s \in PS \\
\rho_i(s, \bot) + \frac{1}{E(s)} \cdot \rho_i(s) \cdot (1 - e^{-E(s)\delta}) & \text{if } s \in MS \text{ and } \alpha = \bot \\
0 & \text{otherwise.}
\end{cases}
$$

A.2 Measures

Probability measure. Given a scheduler $\sigma \in GM$, the probability measure $Pr^M_\sigma$ is defined for measurable sets of infinite paths of MA $M$. This is achieved by considering the probability measure $Pr^{Steps}_{\sigma, \pi}$ for transition steps. For a history $\pi \in FPaths$ with $s = last(\pi)$ and a measurable set of transition steps $T \subseteq \mathbb{R}_{\geq 0} \times Act \times S$ we have

$$
Pr^{Steps}_{\sigma, \pi}(T) = \begin{cases} 
\sum_{(0, s') \in T} \sigma(\pi, \alpha) \cdot P(s, \alpha, s') & \text{if } s \in PS \\
\int_{\{t \mid (t, \bot, s') \in T\}} E(s) \cdot e^{-E(s)t} \cdot \sum_{(t, \bot, s') \in T} P(s, \bot, s') \, dt & \text{if } s \in MS
\end{cases}
$$
\( \Pr_\sigma^M \) is obtained by lifting \( \Pr_{\sigma, \pi}^{Steps} \) to sequences of transition steps (i.e., paths). More information can be found in [37]. To simplify the notations, we write \( \Pr_\sigma^M (\pi) \) instead of \( \Pr_\sigma^M (\{\pi\}) \). For a set of finite paths \( \Pi \subseteq FPaths^M \) we set \( \Pr_\sigma^M (\Pi) = \Pr_\sigma^M (Cyl(\Pi)) \), where \( Cyl(\Pi) \) is the Cylinder of \( \Pi \) given by

\[
Cyl(\Pi) = \{ \pi \overset{\kappa_0}{\to} s_{n+1} \overset{\kappa_{n+1}}{\to} \cdots \in IPaths^M \mid \pi \in \Pi \}.
\]

**Expected reward.** We fix a reward function \( \rho \) of the MA \( M \). The reward of a finite path \( \pi' = s_0 \overset{\kappa_0}{\to} \cdots \overset{\kappa_{n-1}}{\to} s_n \in FPaths \) is given by

\[
rew^M(\rho, \pi') = \sum_{i=0}^{\lvert \pi' \rvert - 1} \rho(s_i) \cdot t(\kappa_i) + \rho(s_i, \alpha(\kappa_i)).
\]

Intuitively, \( rew^M(\rho, \pi') \) is the sum over the rewards obtained in every step \( s_i \overset{\kappa}{\to} \) depicted in the path \( \pi' \). The reward obtained in step \( i \) is composed of the state reward of \( s_i \) multiplied with the sojourn time \( t(\kappa_i) \) as well as the action reward given by \( s_i \) and \( \alpha(\kappa_i) \). State rewards assigned to probabilistic states do not affect the reward of a path as the sojourn time in such states is zero.

For an infinite path \( \pi = s_0 \overset{\kappa_0}{\to} s_1 \overset{\kappa_1}{\to} \cdots \in IPaths \), the reward of \( \pi \) up to a set of goal states \( G \subseteq S \) is given by

\[
rew^M(\rho, \pi, G) = \begin{cases} 
rew^M(\rho, \text{pref}(\pi, n)) & \text{if } n = \min \{ i \geq 0 \mid s_i \in G \} \\
\lim_{n \to \infty} rew^M(\rho, \text{pref}(\pi, n)) & \text{if } s_i \notin G \text{ for all } i \geq 0.
\end{cases}
\]

Intuitively, we stop collecting reward as soon as \( \pi \) reaches a state in \( G \). If no state in \( G \) is reached, reward is accumulated along the infinite path, which potentially yields an infinite reward. The expected reward \( ER^M_\sigma(\rho, G) \) of the function \( rew^M(\rho, \cdot, G) : IPaths^M \to \mathbb{R}_{\geq 0} \), i.e.,

\[
ER^M_\sigma(\rho, G) = \int_{\pi \in IPaths^M} rew^M(\rho, \pi, G) d\Pr_\sigma^M (\pi).
\]

**B Proofs About Sets of Achievable Points**

**B.1 Proof of Theorem [1]**

**Theorem 1.** For some MA \( M \) with achieve\(^M\)(\( \emptyset \triangleright p \)), no deterministic time-abstract scheduler \( \sigma \) satisfies \( M, \sigma \models \emptyset \triangleright p \).

**Proof.** Consider the MA \( M \) in Fig. [3(a)] with objectives \( \emptyset = (\Pr(\Diamond s_2), \Pr(\Diamond s_4)) \), relations \( \triangleright = (\geq, \geq) \), and point \( p = (0.5, 0.5) \). We have achieve\(^M\)(\( \emptyset \triangleright p \)) (A scheduler achieving both objectives is given in Example [2]). However, there are only two deterministic time abstract schedulers for \( M \):

\[
\sigma_\alpha: \text{ always choose } \alpha \quad \text{and} \quad \sigma_\beta: \text{ always choose } \beta
\]

and it holds that \( M, \sigma_\alpha \not\models \Pr(\Diamond s_2) \geq 0.5 \) and \( M, \sigma_\beta \not\models \Pr(\Diamond s_4) \geq 0.5 \). \( \Box \)

20
B.2 Proof of Proposition 1

Proposition 1. The set \( \{ p \in \mathbb{R}^d \mid \text{achieve}^M(\emptyset \triangleright p) \} \) is convex.

Proof. Let \( M \) be an MA and let \( \emptyset = (\emptyset_1, \ldots, \emptyset_d) \) be objectives with relations \( \triangleright = (\triangleright_1, \ldots, \triangleright_d) \) and points \( p_1, p_2 \in \mathbb{R}^d \) such that \( \text{achieve}^M(\emptyset \triangleright p_1) \) and \( \text{achieve}^M(\emptyset \triangleright p_2) \) holds. For \( i = 1, 2 \), let \( \sigma_i \in \text{GM} \) be a scheduler satisfying \( M, \sigma_i \models \emptyset \triangleright p_i \). Consider some \( w \in [0, 1] \). The point \( p = w \cdot p_1 + (1 - w) \cdot p_2 \) is achievable with the scheduler that makes an initial one-off random choice:

- with probability \( w \) mimic \( \sigma_1 \) and
- with probability \( 1 - w \) mimic \( \sigma_2 \).

Hence, \( \text{achieve}^M(\emptyset \triangleright p) \), implying that the set of achievable points is convex.

\( \square \)

B.3 Proof of Theorem 2

Theorem 2. For some MA \( M \) and objectives \( \emptyset \), the polytope \( \{ p \in \mathbb{R}^d \mid \text{achieve}^M(\emptyset \triangleright p) \} \) is not finite.

Proof. We show that the claim holds for the MA \( M \) in Fig. 3(a) with objectives \( \emptyset = (\{0, 1\}, \{0, 2\}, \{\leq, \leq\}) \) and relations \( \triangleright = (\geq, \geq) \).

For the sake of contradiction assume that the polytope \( A = \{ p \in \mathbb{R}^2 \mid \text{achieve}^M(\emptyset \triangleright p) \} \) is finite. Then, there must be two distinct vertices \( p_1, p_2 \) of \( A \) such that \( \{ w \cdot p_1 + (1 - w) \cdot p_2 \mid w \in [0, 1] \} \) is a face of \( A \). In particular, this means that \( p = 0.5 \cdot p_1 + 0.5 \cdot p_2 \) is achievable but \( p_\varepsilon = p + (0, \varepsilon) \) is not achievable for all \( \varepsilon > 0 \). We show that there is in fact an \( \varepsilon \) for which \( p_\varepsilon \) is achievable, contradicting our assumption that \( A \) is finite.

For \( i = 1, 2 \), let \( \sigma_i \in \text{GM} \) be a scheduler satisfying \( M, \sigma_i \models \emptyset \triangleright p_i \). \( \sigma_1 \neq \sigma_2 \) is reached earlier when \( \sigma_i \) is considered. This in-

\( \square \)

21
C Proofs for Untimed Reachability

C.1 Proof of Lemma 1

Lemma 1. For any \( \hat{\pi} \in \text{FPaths}_{\mathcal{M}_D} \) we have \( \Pr_{\mathcal{M}_\sigma}^D(\hat{\pi}) = \Pr_{\text{tail}(\sigma)}^M(\hat{\pi}) \).

Proof. The proof is by induction over the length of the considered path \(|\hat{\pi}| = n\). Let \( \mathcal{M} = (S, \text{Act}, \to, s_0, \{\rho_1, \ldots, \rho_k\}) \) and \( \mathcal{M}_D = (S, \text{Act}, \mathbf{p}, s_0, \{\rho_1^D, \ldots, \rho_k^D\}) \).

If \( n = 0 \), then \( \{\hat{\pi}\} = \{\hat{\pi}\} = \{s_0\} \). Hence, \( \Pr_{\mathcal{M}_\sigma}^D(\hat{\pi}) = 1 = \Pr_{\text{tail}(\sigma)}^M(\hat{\pi}) \). In the induction step, we assume that the lemma holds for a fixed path \( \hat{\pi} \in \text{FPaths}_{\mathcal{M}_D} \) with length \(|\hat{\pi}| = n\) and last(\( \hat{\pi} \)) = s. Consider the path \( \hat{\pi} \overset{\alpha}{\to} s' \in \text{FPaths}_{\mathcal{M}_D} \).

Case \( s \in \text{PS} \): It follows that

\[
\Pr_{\mathcal{M}_\sigma}^D(\hat{\pi} \overset{\alpha}{\to} s') = \int_{\pi \in (\hat{\pi})} \sigma(\pi, \alpha) \cdot \Pr_{\mathcal{M}_\sigma}^M(\pi) \, d\Pr_{\mathcal{M}_\sigma}^M(\pi) = \Pr_{\mathcal{M}_\sigma}^M(\hat{\pi}) \cdot \Pr_{\text{tail}(\sigma)}^M(s', \alpha) = \Pr_{\text{tail}(\sigma)}^M(\hat{\pi} \overset{\alpha}{\to} s').
\]

Case \( s \in \text{MS} \): As \( s \in \text{MS} \) we have \( \alpha = \bot \) and it follows

\[
\Pr_{\mathcal{M}_\sigma}^M(\hat{\pi} \overset{\bot}{\to} s') = \int_{\pi \in (\hat{\pi})} \int_0^\infty E(s) \cdot e^{-E(s)t} \cdot \Pr_{\mathcal{M}_\sigma}^M(\pi) \, dt \, d\Pr_{\mathcal{M}_\sigma}^M(\pi) = \Pr_{\mathcal{M}_\sigma}^M(\hat{\pi}) \cdot \Pr_{\text{tail}(\sigma)}^M(s', \bot) = \Pr_{\text{tail}(\sigma)}^M(\hat{\pi} \overset{\bot}{\to} s').
\]

\( \square \)

C.2 Proof of Proposition 2

Proposition 2. For any \( G \subseteq S \) it holds that \( \Pr_{\mathcal{M}_\sigma}(\hat{\gamma} G) = \Pr_{\text{tail}(\sigma)}^M(\hat{\gamma} G) \).
Proof. Let $\Pi$ be the set of finite time-abstract paths of $M_D$ that end at the first visit of a state in $G$, i.e.,

$$\Pi = \{ s_0 \xrightarrow{\alpha_0} \ldots \xrightarrow{\alpha_{n-1}} s_n \in FPaths^{M_D} \mid s_n \in G \text{ and } \forall i < n: s_i \notin G \}.$$ 

Every path $\pi \in \Diamond G \subseteq IPaths^M$ has a unique prefix $\pi'$ with $ta(\pi') \in \Pi$. We have

$$\Diamond G = \bigcup_{\pi \in \Pi} Cyl(\langle \hat{\pi} \rangle).$$

The claim follows with Lemma 1 since

$$\Pr^M(\Diamond G) = \sum_{\hat{\pi} \in \Pi} \Pr^M(\langle \hat{\pi} \rangle) = \sum_{\hat{\pi} \in \Pi} \Pr^M_{ta(\sigma)}(\hat{\pi}) = \Pr^M_{ta(\sigma)}(\Diamond G).$$

C.3 Proof of Theorem 3

Theorem 3. For MA $M$ and untimed reachability objectives $\Diamond$ it holds that

$$\text{achieve}^M(\Diamond \rhd p) \iff \text{achieve}^{M_D}(\Diamond \rhd p).$$

Proof. Let $\Diamond = (\Diamond G_1, \ldots, \Diamond G_d)$ be the considered list of objectives with threshold relations $\rhd = (\rhd_1, \ldots, \rhd_d)$. The following equivalences hold for any $\sigma \in GM^M$ and $p \in \mathbb{R}^d$.

$$M, \sigma \models \Diamond \rhd p \iff \forall i: M, \sigma \models \Diamond G_i \rhd p_i$$

$$\iff \forall i: \Pr^M_{\sigma}(\Diamond G_i) \rhd p_i$$

$$\iff \forall i: \Pr^M_{ta(\sigma)}(\Diamond G_i) \rhd p_i$$

$$\iff \forall i: M_{D, ta(\sigma)} \models \Diamond G_i \rhd p_i$$

$$\iff M_{D, ta(\sigma)} \models \Diamond \rhd p.$$ 

Assume that $\text{achieve}^M(\Diamond \rhd p)$ holds, i.e., there is a $\sigma \in GM^M$ such that $M, \sigma \models \Diamond \rhd p$. It follows that $M_{D, ta(\sigma)} \models \Diamond \rhd p$ which means that $\text{achieve}^{M_D}(\Diamond \rhd p)$ holds as well. For the other direction assume $\text{achieve}^{M_D}(\Diamond \rhd p)$, i.e., $M_{D, \sigma} \models \Diamond \rhd p$ for some time-abstract scheduler $\sigma \in TA$. We have $ta(\sigma) = \sigma$. It follows that $M_{D, ta(\sigma)} \models \Diamond \rhd p$. Applying the equivalences above yields $M, \sigma \models \Diamond \rhd p$ and thus $\text{achieve}^M(\Diamond \rhd p)$. 

D Proofs for Expected Reward

D.1 Proof of Proposition 3

Let $n \geq 0$ and $G \subseteq S$. The set of time-abstract paths that end after $n$ steps or at the first visit of a state in $G$ is denoted by

$$\Pi^n_G = \{ s_0 \xrightarrow{\alpha_0} \ldots \xrightarrow{\alpha_{m-1}} s_m \in FPaths^{M_D} \mid (m = n \text{ or } s_m \in G) \text{ and } s_i \notin G \text{ for all } 0 \leq i < m \}.$$
For \( \mathcal{M} \) under \( \sigma \in \text{GM}^\mathcal{M} \) and \( \mathcal{M}_\mathcal{D} \) under \( \text{ta}(\sigma) \in \text{TA} \), we define the expected reward collected along the paths of \( \Pi_n^\mathcal{G} \) as

\[
\text{ER}_\sigma^\mathcal{M}(\rho, \Pi_n^\mathcal{G}) = \sum_{\pi \in \Pi_n^\mathcal{G}} \int_{\pi \in (\hat{\pi})} \text{rew}^\mathcal{M}(\rho, \pi) \, d\Pr^\mathcal{M}_\sigma(\pi)
\]

and

\[
\text{ER}_{\text{ta}(\sigma)}^\mathcal{M}(\rho^\mathcal{D}, \Pi_n^\mathcal{G}) = \sum_{\pi \in \Pi_n^\mathcal{G}} \text{rew}^\mathcal{M}(\rho^\mathcal{D}, \hat{\pi}) \cdot \Pr^\mathcal{M}_{\text{ta}(\sigma)}(\hat{\pi}),
\]

respectively. Intuitively, \( \text{ER}_\sigma^\mathcal{M}(\rho, \Pi_n^\mathcal{G}) \) corresponds to \( \text{ER}_\sigma^\mathcal{M}(\rho, G) \) assuming that no more reward is collected after the \( n \)-th transition. It follows that the value \( \text{ER}_\sigma^\mathcal{M}(\rho, \Pi_n^\mathcal{G}) \) approaches \( \text{ER}_\sigma^\mathcal{M}(\rho, G) \) for large \( n \). Similarly, \( \text{ER}_{\text{ta}(\sigma)}^\mathcal{M}(\rho^\mathcal{D}, \Pi_n^\mathcal{G}) \) approaches \( \text{ER}_{\text{ta}(\sigma)}^\mathcal{M}(\rho^\mathcal{D}, G) \) for large \( n \). This observation is formalized by the following lemma.

**Lemma 2.** For MA \( \mathcal{M} = (S, \text{Act}, \rightarrow, s_0, \{\rho_1, \ldots, \rho_k\}) \) with \( G \subseteq S \), \( \sigma \in \text{GM} \), and reward function \( \rho \) it holds that

\[
\lim_{n \to \infty} \text{ER}_\sigma^\mathcal{M}(\rho, \Pi_n^\mathcal{G}) = \text{ER}_\sigma^\mathcal{M}(\rho, G).
\]

Furthermore, any reward function \( \rho^\mathcal{D} \) for \( \mathcal{M}_\mathcal{D} \) satisfies

\[
\lim_{n \to \infty} \text{ER}_{\text{ta}(\sigma)}^\mathcal{M}(\rho^\mathcal{D}, \Pi_n^\mathcal{G}) = \text{ER}_{\text{ta}(\sigma)}^\mathcal{M}(\rho^\mathcal{D}, G).
\]

**Proof.** We show the first claim. The second claim follows analogously. For each \( n \geq 0 \), consider the function \( f_n : \text{Paths}^\mathcal{M} \to \mathbb{R}_{\geq 0} \) given by

\[
f_n(\pi) = \begin{cases} 
\text{rew}^\mathcal{M}(\rho, \text{pref}(\pi, m)) & \text{if } m = \min \{i \in \{0, \ldots, n\} \mid s_i \in G\} \\
\text{rew}^\mathcal{M}(\rho, \text{pref}(\pi, n)) & \text{if } s_i \notin G \text{ for all } i \leq n
\end{cases}
\]

for every path \( \pi = s_0 \xrightarrow{\kappa_0} s_1 \xrightarrow{\kappa_1} \cdots \in \text{Paths}^\mathcal{M} \). Intuitively, \( f_n(\pi) \) is the reward collected on \( \pi \) within the first \( n \) steps and only up to the first visit of \( G \). This allows us to express the expected reward collected along the paths of \( \Pi_n^\mathcal{G} \) as

\[
\text{ER}_\sigma^\mathcal{M}(\Pi_n^\mathcal{G}) = \sum_{\pi \in \Pi_n^\mathcal{G}} \int_{\pi \in (\hat{\pi})} \text{rew}^\mathcal{M}(\rho, \pi) \, d\Pr^\mathcal{M}_\sigma(\pi) = \int_{\pi \in \text{Paths}^\mathcal{M}} f_n(\pi) \, d\Pr^\mathcal{M}_\sigma(\pi).
\]

It holds that \( \lim_{n \to \infty} f_n(\pi) = \text{rew}^\mathcal{M}(\rho, \pi, G) \) which is a direct consequence from the definition of the reward of \( \pi \) up to \( G \) (cf. App. A.2). Furthermore, note that the sequence of functions \( f_0, f_1, \ldots \) is non-decreasing, i.e., we have \( f_n(\pi) \leq f_{n+1}(\pi) \) for all \( n \geq 0 \) and \( \pi \in \text{Paths}^\mathcal{M} \). By applying the monotone convergence theorem [38] we obtain

\[
\lim_{n \to \infty} \text{ER}_\sigma^\mathcal{M}(\Pi_n^\mathcal{G}) = \lim_{n \to \infty} \int_{\pi \in \text{Paths}^\mathcal{M}} f_n(\pi) \, d\Pr^\mathcal{M}_\sigma(\pi)
\]

\[
\int_{\pi \in \text{Paths}^\mathcal{M}} \lim_{n \to \infty} f_n(\pi) \, d\Pr^\mathcal{M}_\sigma(\pi)
\]

\[
\int_{\pi \in \text{Paths}^\mathcal{M}} \text{rew}^\mathcal{M}(\rho, \pi, G) \, d\Pr^\mathcal{M}_\sigma(\pi) = \text{ER}_\sigma^\mathcal{M}(\rho, G).
\]

\( \square \)
The next step is to show that the expected reward collected along the paths of $\Pi_G^n$ coincides for $\mathcal{M}$ under $\sigma$ and $\mathcal{M}_D$ under $\operatorname{ta}(\sigma)$.

**Lemma 3.** Let $\rho$ be some reward function of $\mathcal{M}$ and let $\rho^D$ be its counterpart for $\mathcal{M}_D$. Let $\mathcal{M} = (S, \text{Act}, \rightarrow, s_0, \{\rho_1, \ldots, \rho_l\})$ be an MA with $G \subseteq S$ and $\sigma \in \mathcal{GM}$. For all $G \subseteq S$ and $n \geq 0$ it holds that

$$\operatorname{ER}_{\sigma}^\mathcal{M}(\rho, \Pi_G^n) = \operatorname{ER}_{\operatorname{ta}(\sigma)}^{\mathcal{M}_D}(\rho^D, \Pi_G^n).$$

**Proof.** The proof is by induction over the path length $n$. To simplify the notation, we often omit the reward functions $\rho$ and $\rho^D$ and write, e.g., $\operatorname{rew}^\mathcal{M}(\pi)$ instead of $\operatorname{rew}^\mathcal{M}(\rho^D, \pi)$ or $\operatorname{ER}^\mathcal{M}(\Pi_G^n)$ instead of $\operatorname{ER}^\mathcal{M}(\rho, \Pi_G^n)$.

If $n = 0$, then $\Pi_G^n = \{s_0\}$. The claim holds since $\operatorname{rew}^\mathcal{M}(s_0) = \operatorname{rew}^\mathcal{M}(s_0) = 0$.

In the induction step, we assume that the lemma is true for some fixed $n \geq 0$. We split the term $\operatorname{ER}^\mathcal{M}(\Pi_G^{n+1})$ into the reward that is obtained by paths which reach $G$ within $n$ steps and the reward obtained by paths of length $n + 1$. In a second step, we consider the sum of the reward collected within the first $n$ steps and the reward obtained in the $(n + 1)$-th step:

$$\begin{align*}
\operatorname{ER}^\mathcal{M}(\Pi_G^{n+1}) &= \sum_{\pi \in \Pi_G^{n+1}} \int_{|\pi| \leq n} \operatorname{rew}^\mathcal{M}(\pi) \operatorname{dPr}_\sigma^\mathcal{M}(\pi) \\
&+ \sum_{\pi \in \Pi_G^{n+1}} \int_{|\pi| = n+1} \operatorname{rew}^\mathcal{M}(\pi') + \rho(s) \cdot t(\kappa) + \rho(s, \alpha(\kappa)) \operatorname{dPr}_\sigma^\mathcal{M}(\pi) \\
&= \sum_{\pi \in \Pi_G^{n+1}} \int_{|\pi| \leq n} \operatorname{rew}^\mathcal{M}(\pi) \operatorname{dPr}_\sigma^\mathcal{M}(\pi) + \sum_{\pi \in \Pi_G^{n+1}} \int_{|\pi| = n+1} \rho(s) \cdot t(\kappa) + \rho(s, \alpha(\kappa)) \operatorname{dPr}_\sigma^\mathcal{M}(\pi),
\end{align*}$$

where we define $\operatorname{pref}(\pi, n)$ for paths with $|\pi| \leq n$ such that $\operatorname{pref}(\pi, n) = \pi$. The two terms (1) and (2) are treated separately.

**Term (1):** Let $A_G^{\leq n} = \{\hat{\pi} \in \Pi_G^{n+1} | |\hat{\pi}| \leq n\}$ be the paths in $\Pi_G^{n+1}$ of length at most $n$. We have $A_G^{\leq n} \subseteq \Pi_G^{n+1}$ and every path in $A_G^{\leq n}$ visits a state in $G$. Correspondingly, $A_G^{\geq n} = \Pi_G^n \setminus A_G^{\leq n}$ is the set of time-abstract paths of length $n$ that do not visit a state in $G$. Hence, the paths in $\Pi_G^n$ with length $n + 1$ have a prefix in $A_G^{\geq n}$. The set $\Pi_G^{n+1}$ is partitioned such that

$$\begin{align*}
\Pi_G^{n+1} &= A_G^{\leq n} \cup \{\hat{\pi} \in \Pi_G^{n+1} | |\hat{\pi}| = n + 1\} \\
&= A_G^{\leq n} \cup \{\hat{\pi} = \hat{\pi}' \overset{\alpha}{\rightarrow} s' \in \text{FPaths}^\mathcal{M}_D | \hat{\pi}' \in A_G^{\geq n}\}.
\end{align*}$$
The reward obtained within the first $n$ steps is independent of the $(n+1)$-th transition. To show this formally, we fix a path $\hat{\pi'} \in A_{\pi}^{\leq n}$ with last($\hat{\pi'}$) = $s$ and derive

$$
\sum_{\pi' \xrightarrow{\alpha} s' \in FPaths^{M_D}} \int_{\pi \in (\hat{\pi'} \xrightarrow{\alpha} s')} rew^M(pref(\pi, n)) dPr^M(\pi)
$$

$$
= \left\{ \begin{array}{ll}
\int_{\pi' \in (\hat{\pi'})} rew^M(\pi') \cdot \sum_{(\pi', \alpha) \in A \times S} \sigma(\pi', \alpha) \cdot P(s, \alpha, s') dPr^M(\pi') & \text{if } s \in PS \\
\int_{\pi' \in (\hat{\pi'})} rew^M(\pi') \cdot \sum_{s' \in S} P(s, \bot, s') dPr^M(\pi') & \text{if } s \in MS
\end{array} \right.
$$

$$
= \int_{\pi' \in (\hat{\pi'})} rew^M(\pi') dPr^M(\pi'). \quad (3)
$$

With the above-mentioned partition of the set $P_{\pi_G}^{n+1}$, it follows that the expected reward obtained within the first $n$ steps is given by

$$
\sum_{\hat{\pi} \in P_{\pi_G}^{n+1}} \int_{\pi \in (\hat{\pi})} rew^M(pref(\pi, n)) dPr^M(\pi)
$$

$$
= \sum_{\hat{\pi} \in A_{\pi}^{\leq n}} \int_{\pi \in (\hat{\pi})} rew^M(\pi) dPr^M(\pi)
$$

$$
+ \sum_{\hat{\pi} \in A_{\pi}^{\geq n}} \sum_{\pi' \in FPaths^{M_D}} \int_{\pi \in (\hat{\pi} \xrightarrow{\alpha} s')} rew^M(pref(\pi, n)) dPr^M(\pi)
$$

$$
= \sum_{\hat{\pi} \in A_{\pi}^{\leq n}} \int_{\pi \in (\hat{\pi})} rew^M(\pi) dPr^M(\pi) + \sum_{\hat{\pi} \in A_{\pi}^{\geq n}} \int_{\pi \in (\hat{\pi})} rew^M(\pi) dPr^M(\pi)
$$

$$
= ER^M_{\pi_G}(P_{\pi_G}^{n})
$$

$$
\stackrel{H}{=} ER^M_{\pi_G}(P_{\pi_G}^{n+1})
$$

$$
= \sum_{\hat{\pi} \in A_{\pi}^{\leq n}} rew^M^D(\hat{\pi}) \cdot Pr^M^D(\hat{\pi}) + \sum_{\hat{\pi} \in A_{\pi}^{\geq n}} rew^M^D(\hat{\pi}) \cdot Pr^M^D(\hat{\pi})
$$

$$
= \sum_{\hat{\pi} \in A_{\pi}^{\leq n}} rew^M^D(\hat{\pi}) \cdot Pr^M^D(\hat{\pi})
$$

$$
+ \sum_{\hat{\pi} \in A_{\pi}^{\geq n}} \sum_{\pi' \in FPaths^{M_D}} rew^M^D(pref(\hat{\pi}, n)) \cdot Pr^M^D(\hat{\pi})
$$

$$
= \sum_{\hat{\pi} \in P_{\pi_G}^{n+1}} rew^M^D(pref(\hat{\pi}, n)) \cdot Pr^M^D(\hat{\pi}) \quad (4)
$$

**Term (2):** For the expected reward obtained in step $n + 1$, consider a path $\hat{\pi} = \hat{\pi'} \xrightarrow{\alpha} s' \in P_{\pi_G}^{n+1}$ such that $|\hat{\pi'}| = n$ and last($\hat{\pi'}$) = $s$. 

26
Proposition 3. Let $\rho$ be some reward function of $\mathcal{M}$ and let $\rho^D$ be its counterpart for $\mathcal{M}_D$. For $G \subseteq S$ we have $\text{ER}^M(\rho, G) = \text{ER}^D(\rho^D, G)$.

Proof. The proposition is a direct consequence of Lemma 2 and Lemma 3 as

$$\text{ER}^M(\rho, G) = \lim_{n \to \infty} \text{ER}^M(\rho, \Pi^n_G) = \lim_{n \to \infty} \text{ER}^D(\rho^D, \Pi^n_G) = \text{ER}^D(\rho^D, G).$$
D.2 Proof of Theorem 4

Theorem 4. For MA $\mathcal{M}$ and untimed reachability and expected reward objectives $\mathcal{O}$: achieve$^\mathcal{M}(\mathcal{O} \triangleright p) \iff$ achieve$^\mathcal{MD}(\mathcal{O} \triangleright p)$.

Proof. Let $\mathcal{O} = (\mathcal{O}_1, \ldots, \mathcal{O}_d)$ be the considered list of untimed reachability and expected reward objectives with threshold relations $\triangleright = (\triangleright_1, \ldots, \triangleright_d)$. The following equivalences hold for any $\sigma \in \text{GM}_\mathcal{M}$ and $p \in \mathbb{R}^d$.

$$\mathcal{M}, \sigma \models \mathcal{O} \triangleright p \iff \forall i: \mathcal{M}_i, \sigma \models \mathcal{O}_i \triangleright p_i \iff \mathcal{M}_\text{D}, \text{ta}(\sigma) \models \mathcal{O} \triangleright p,$$

where for the equivalence marked with $\ast$ we consider two cases: If $\mathcal{O}_i$ is of the form $P(\Diamond G)$, Proposition 2 yields

$$\mathcal{M}, \sigma \models \mathcal{O}_i \triangleright p_i \iff \text{Pr}_{\mathcal{M}, \sigma}(\Diamond G) \triangleright p_i \iff \text{Pr}_{\mathcal{M}_\text{D}, \text{ta}(\sigma)}(\Diamond G) \triangleright p_i \iff \mathcal{M}_\text{D}, \text{ta}(\sigma) \models \mathcal{O}_i \triangleright p_i,$$

Otherwise, $\mathcal{O}_i$ is of the form $E(\# j, G)$ and with Proposition 3 it follows that

$$\mathcal{M}, \sigma \models \mathcal{O}_i \triangleright p_i \iff \text{ER}_{\mathcal{M}, \sigma}(\# j, G) \triangleright p_i \iff \text{ER}_{\mathcal{M}_\text{D}, \text{ta}(\sigma)}(\# j, G) \triangleright p_i \iff \mathcal{M}_\text{D}, \text{ta}(\sigma) \models \mathcal{O}_i \triangleright p_i.$$

The remaining steps of the proof are completely analogous to the proof of Theorem 3 conducted on page 23. $\square$

E Proofs for Timed Reachability

E.1 Proof of Proposition 4

Let $\mathcal{M} = (S, \mathcal{A}, \rightarrow, s_0, \{\rho_1, \ldots, \rho_k\})$ be an MA and let $\mathcal{M}_\delta$ be the digitization of $\mathcal{M}$ with respect to some $\delta \in \mathbb{R}_{>0}$. We consider the infinite paths of $\mathcal{M}$ that are represented by a finite digital path.

Definition 19 (Induced cylinder of a digital path). Given a digital path $\bar{\pi} \in \text{FPaths}^{\mathcal{M}_\delta}$ of MA $\mathcal{M}$, the induced cylinder of $\bar{\pi}$ is given by

$$[\bar{\pi}]_{\text{cyl}} = \{\pi \in \text{IPaths}^\mathcal{M} \mid \bar{\pi} \text{ is a prefix of } \text{di}(\pi)\}.$$

Recall the definition of the cylinder of a set of finite paths (cf. App. A.2). If $\bar{\pi} \in \text{FPaths}^\mathcal{M}_\delta$ does not end with a self-loop at a Markovian state, then $[\bar{\pi}]_{\text{cyl}} = \text{Cyl}([\bar{\pi}])$ holds.

Example 10. Let $\mathcal{M}$ and $\mathcal{M}_\delta$ be as in Fig. 2. We consider the path $\bar{\pi}_1 = s_0 \downarrow s_0 \downarrow s_3 \downarrow s_4$ and digitization constant $\delta = 0.4$. The set $[\bar{\pi}_1]_{\text{cyl}}$ contains each infinite path whose digitization has the prefix $\bar{\pi}_1$, i.e.,

$$[\bar{\pi}_1]_{\text{cyl}} = \{s_0 \downarrow s_3 \downarrow s_4 \downarrow \cdots \in \text{IPaths}^\mathcal{M} \mid 0.8 \leq t < 1.2\}.$$
We observe that these are exactly the paths that have a prefix in \([\bar{\pi}_1]\). Put differently, we have \([\bar{\pi}_1]_{cyl} = Cyl([\bar{\pi}_1])\).

Next, consider the digital path \(\bar{\pi}_2 = s_0 \xrightarrow{1} s_0 \xrightarrow{1} s_0\). Note that there is no path \(\pi \in \text{FPaths}^M\) with \(\text{di}(\pi) = \bar{\pi}_2\), implying \([\bar{\pi}_2] = \emptyset\). Intuitively, \(\bar{\pi}_2\) depicts a sojourn time at \(\text{last}(\bar{\pi}_2)\) but finite paths of MAs do not depict sojourn times at their last state. On the other hand, the induced cylinder of \(\bar{\pi}_2\) contains all paths that sojourn at least 2\(\delta\) time units at \(s_0\), i.e.,

\[
[\bar{\pi}_2]_{cyl} = \{s_0 \xrightarrow{t} s_1 \xrightarrow{\kappa} \cdots \in \text{IPaths}^M \mid t \geq 0.8\}.
\]

The schedulers \(\sigma\) and \(\text{di}(\sigma)\) induce the same probabilities for a given digital path. This is formalized by the following lemma. Note that a similar statement for \(\text{ta}(\sigma)\) and time-abstract paths was shown in Lemma [I]

Lemma 4. Let \(M\) be an MA with scheduler \(\sigma \in \text{GM}\), digitization \(M_\delta\), and digital path \(\bar{\pi} \in \text{FPaths}^{M_\delta}\). It holds that

\[
\text{Pr}_{\text{M}}([\bar{\pi}]_{\text{cyl}}) = \text{Pr}_{\text{M}_\delta}([\bar{\pi}]_{\text{cyl}}).
\]

Proof. The proof is by induction over the length \(n\) of \(\bar{\pi}\). Let \(M = (S, \text{Act}, \rightarrow, s_0, \{\rho_1, \ldots, \rho_t\})\) and \(M_\delta = (S, \text{Act}, M_\delta, s_0, \{\rho_1^\delta, \ldots, \rho_t^\delta\})\). If \(n = 0\), then \(\bar{\pi} = s_0\) and \([\bar{\pi}]_{\text{cyl}} = \text{IPaths}^M\). Hence, \(\text{Pr}_{\text{M}}([s_0]_{\text{cyl}}) = 1 = \text{Pr}_{\text{M}_\delta}(s_0)\). In the induction step it is assumed that the lemma holds for a fixed path \(\bar{\pi} \in \text{FPaths}^{M_\delta}\) with \([\bar{\pi}] = n\) and \(\text{last}(\bar{\pi}) = s\). Consider a path \(\bar{\pi} \xrightarrow{[\bar{\pi}]} s' \in \text{FPaths}^{M_\delta}\). We distinguish the following cases.

Case \(s \in \text{PS}\): It follows that \([\bar{\pi} \xrightarrow{[\bar{\pi}]} s']_{\text{cyl}} = Cyl([\bar{\pi} \xrightarrow{[\bar{\pi}]} s'])\) since \(\bar{\pi} \xrightarrow{[\bar{\pi}]} s'\) ends with a probabilistic transition. Hence,

\[
\text{Pr}_{\text{M}}([\bar{\pi} \xrightarrow{[\bar{\pi}]} s']_{\text{cyl}}) = \text{Pr}_{\text{M}}([\bar{\pi} \xrightarrow{[\bar{\pi}]} s'])
\]

\[
= \int_{\pi \in [\bar{\pi}]} \sigma(\pi, \alpha) \cdot \text{P}(s, \alpha, s') \text{dPr}_{\text{M}}^M(\pi)
\]

\[
= \int_{\pi \in [\bar{\pi}]} \sigma(\pi, \alpha) \cdot \text{P}(s, \alpha, s') \text{dPr}_{\text{M}}^M([\pi] \cap [\bar{\pi}])
\]

\[
= \int_{\pi \in [\bar{\pi}]} \sigma(\pi, \alpha) \cdot \text{P}(s, \alpha, s') \text{d}[\text{Pr}_{\text{M}}^M(\pi \mid [\bar{\pi}]) \cdot \text{Pr}_{\text{M}}^M([\bar{\pi}])]
\]

\[
= \text{Pr}_{\text{M}}([\bar{\pi}]) \cdot \text{P}(s, \alpha, s') \cdot \int_{\pi \in [\bar{\pi}]} \sigma(\pi, \alpha) \text{dPr}_{\text{M}}^M(\pi \mid [\bar{\pi}])
\]

\[
= \text{Pr}_{\text{M}}([\bar{\pi}]) \cdot \text{P}(s, \alpha, s') \cdot \text{di}(\sigma)(\bar{\pi}, \alpha)
\]

\[
\text{III} \text{ } \text{Pr}_{\text{M}_\delta}(\bar{\pi}) \cdot \text{P}(s, \alpha, s') \cdot \text{di}(\sigma)(\bar{\pi}, \alpha)
\]

\[
= \text{Pr}_{\text{M}_\delta}([\bar{\pi} \xrightarrow{[\bar{\pi}]} s']).
\]
Case $s \in \mathcal{M}$: As $s \in \mathcal{M}$ we have $\alpha = \bot$ and it follows
\[
\Pr^M(\bar{\pi} \xrightarrow{cyl} s') = \Pr^M(\bar{\pi} \cap \bar{\pi} \xrightarrow{cyl} s') = \Pr^M(\bar{\pi} \xrightarrow{cyl}) \cdot \Pr^M(\bar{\pi} \xrightarrow{cyl}).
\] (6)

Assume that a path $\pi \in [\bar{\pi}]_{cyl}$ has been observed, i.e., $\text{pref}(\text{di}(\pi), m) = \bar{\pi}$ holds for some $m \geq 0$. The term $\Pr^M(\bar{\pi} \xrightarrow{cyl} s' | [\bar{\pi}]_{cyl})$ coincides with the probability that also $\text{pref}(\text{di}(\pi), m+1) = \bar{\pi} \xrightarrow{cyl} s'$ holds. We have either
- $s \neq s'$ which means that the transition from $s$ to $s'$ has to be taken during a period of $\delta$ time units or
- $s = s'$ where we additionally have to consider the case that no transition is taken at $s$ for $\delta$ time units.

It follows that
\[
\Pr^M(\bar{\pi} \xrightarrow{cyl} s' | [\bar{\pi}]_{cyl}) = \begin{cases} 
\mathbf{P}(s, \bot, s') \cdot (1 - e^{-E(s)\delta}) & \text{if } s \neq s' \\
\mathbf{P}(s, \bot, s') \cdot (1 - e^{-E(s)\delta}) + e^{-E(s)\delta} & \text{if } s = s' 
\end{cases}.
\] (7)

We conclude that
\[
\Pr^M(\bar{\pi} \xrightarrow{cyl} s' | [\bar{\pi}]_{cyl}) = \frac{0}{\frac{1}{\left[ \begin{array}{c} \gamma \delta \end{array} \right]}} \cdot \mathbf{P}(s, \bot, s') = \mathbf{P}(s, \bot, s') \cdot \mathbf{P}(\ldots).
\]

We apply Lemma 4 to show Proposition 4. The idea of the proof is similar to the proof of Proposition 2 conducted on page 23.

**Proposition 4.** Let $\mathcal{M}$ be an MA with $G \subseteq S$, $\sigma \in \Gamma M$, and digitization $\mathcal{M}_{\delta}$. Further, let $J \subseteq \mathbb{N}$ be a set of consecutive natural numbers. It holds that
\[
\Pr^M(\hat{\Phi}_{\text{ds}}G) = \Pr^M(\hat{\Phi}_{\text{di}(\sigma)}\hat{\Phi}_{\text{ds}}G).
\]

**Proof.** Consider the set $\Pi^J_G \subseteq \mathcal{FPaths}^{\mathcal{M}_{\delta}}$ of paths that (i) visit $G$ within $J$ digitization steps and (ii) do not have a proper prefix that satisfies (i). Every path in $\hat{\Phi}_{\text{ds}}G$ has a unique prefix in $\Pi^J_G$, yielding
\[
\hat{\Phi}_{\text{ds}}G = \bigcup_{\tilde{\pi} \in \Pi^J_G} Cyl(\{\tilde{\pi}\})
\]

For the corresponding paths of $\mathcal{M}$ we obtain
\[
[\hat{\Phi}_{\text{ds}}G] = \{\pi \in \mathcal{IPaths}^M \mid \text{di}(\pi) \in \hat{\Phi}_{\text{ds}}G\}
= \{\pi \in \mathcal{IPaths}^M \mid \text{di}(\pi) \text{ has a unique prefix in } \Pi^J_G\}
= \bigcup_{\tilde{\pi} \in \Pi^J_G} [\tilde{\pi}]_{cyl}.
\]
The proposition follows with Lemma 4 since
\[
\Pr_{\text{di}(\sigma)}(\check{\sigma}_G) = \sum_{\pi \in \Pi_G} \Pr_{\text{di}(\sigma)}(\check{\sigma}) = \sum_{\pi \in \Pi_G} \Pr_{\text{di}(\sigma)}(\check{\sigma}_G) = \Pr_{\text{di}(\sigma)}(\check{\sigma}_G).
\]

\[\Box\]

E.2 Proof of Proposition 5

The notation \(|\bar{\pi}|_{ds}\) for paths \(\bar{\pi}\) of \(M_\delta\) is also applied to paths of \(M\), where \(|\pi|_{ds} = |\text{di}(\pi)|_{ds}\) for any \(\pi \in FPaths^M\). Intuitively, one digitization step represents the elapse of at most \(\delta\) time units. Consequently, the duration of a path with \(k \in \mathbb{N}\) digitization steps is at most \(k\delta\).

Lemma 5. For a path \(\pi \in FPaths^M\) and digitization constant \(\delta\) it holds that
\[
T(\pi) \leq |\pi|_{ds} \cdot \delta .
\]

Proof. Let \(\pi = s_0 \xrightarrow{\kappa_0} \cdots \xrightarrow{\kappa_{n-1}} s_n\) and let \(m_i = \max\{m \in \mathbb{N} \mid m\delta \leq t(\kappa_i)\}\) for each \(i \in \{0, \ldots, n-1\}\) (as in Definition 12). The number \(|\pi|_{ds}\) is given by \(\sum_{0 \leq i < n, s_i \in MS}(m_i + 1)\). With \(t(\kappa_i) \leq (m_i + 1)\delta\) it follows that
\[
T(\pi) = \sum_{0 \leq i < n, s_i \in MS} t(\kappa_i) \leq \sum_{0 \leq i < n} (m_i + 1)\delta = |\pi|_{ds} \cdot \delta .
\]

\[\Box\]

For a path \(\pi\) and \(t \in \mathbb{R}_{\geq 0}\), the prefix of \(\pi\) up to time point \(t\) is given by \(\text{pref}_T(\pi, t) = \text{pref}(\pi, \max\{n \mid T(\text{pref}(\pi, n)) \leq t\})\). For the proof of Proposition 5 we focus on the probability that (under a given scheduler \(\sigma\)) the digitization approach yields an inaccurate estimate of the actual time. This is the probability that more than \(k \in \mathbb{N}\) digitization steps have been performed within \(k\delta\) time units. We denote this value by \(\Pr_{\sigma}(\#[k\delta]^{> k})\).

Definition 20 (Digitization step bounded paths). Assume an MA \(M\) and a digitization constant \(\delta \in \mathbb{R}_{>0}\). For some \(t \in \mathbb{R}_{\geq 0}\), \(k \in \mathbb{N}\), and \(\triangleright \in \{<, \leq, >, \geq\}\) the set of paths whose prefix up to time point \(t\) has \(\triangleright \) digitization steps is defined as
\[
\#[t]^{\triangleright k} = \{\pi \in IPaths^M \mid |\text{pref}_T(\pi, t)|_{ds} \triangleright k\}.
\]

Example 11. Let \(M\) be the MA given in Fig. 7(a). We consider the set \(\#[5\delta]^{\leq 5}\). The digitization constant \(\delta\) remains unspecified in this example. Fig. 7(b) illustrates paths \(\pi_1, \pi_2,\) and \(\pi_3\) of \(M\). We depict sojourn times by arrow length. For instance, the path \(\pi_1\) corresponds to \(s_0 \xrightarrow{2.5\delta} s_0 \xrightarrow{1.8\delta} s_1 \xrightarrow{1.7\delta} \cdots \in IPaths^M\). Digitization steps that are “earned” by sojourning at some state for a multiple
of $\delta$ time units are indicated by black dots. Transitions of $\pi_i$ (where $i \in \{1, 2, 3\}$) that do not belong to $\text{pref}_T(\pi_i, 5\delta)$ are depicted in gray. We obtain

\begin{align*}
\text{pref}_T(\pi_1, 5\delta) &= 5 \quad \implies \quad \pi_1 \in \#[5\delta]\leq 5 \\
\text{pref}_T(\pi_2, 5\delta) &= 4 \quad \implies \quad \pi_2 \in \#[5\delta]\leq 5 \\
\text{pref}_T(\pi_3, 5\delta) &= 7 \quad \implies \quad \pi_3 \notin \#[5\delta]\leq 5.
\end{align*}

Note that only the digitization steps of the prefix up to time point $5\delta$ are considered. For example, the step of $\pi_2$ at time point $4.5\delta$ is not considered since the corresponding transition is not part of $\text{pref}_T(\pi_2, 5\delta)$. However, we have $|\text{pref}_T(\pi_2, 5.5\delta)|_{ds} = 6$, implying $\pi_2 \notin \#[5.5\delta]\leq 5$.

All considered paths reach $G = \{s_1\}$ within $5\delta$ time units but $\pi_3 \notin \#[5\delta]\leq 5$ requires more than 5 digitization steps.

The following lemma gives an upper bound for the probability $\Pr_\sigma^\mathcal{M}(\#[k\delta]>^k)$.

**Lemma 6.** Let $\mathcal{M}$ be an MA with $\sigma \in \mathcal{G}M$ and maximum rate $\lambda = \max\{\mathbb{E}(s) \mid s \in MS\}$. Further, let $\delta \in \mathbb{R}_{>0}$ and $k \in \mathbb{N}$. It holds that

$$
\Pr_\sigma^\mathcal{M}(\#[k\delta]>^k) \leq 1 - (1 + \lambda\delta)^k \cdot e^{-\lambda\delta k}
$$

For the proof of Lemma 6 we employ the following auxiliary lemma.

**Lemma 7.** Let $\mathcal{M}$ be an MA with $\sigma \in \mathcal{G}M$ and maximum rate $\lambda = \max\{\mathbb{E}(s) \mid s \in MS\}$. For each $\delta \in \mathbb{R}_{>0}$, $k \in \mathbb{N}$, and $t \in \mathbb{R}_{\geq 0}$ it holds that

$$
\Pr_\sigma^\mathcal{M}(\#[k\delta + t]\leq^k) \geq \Pr_\sigma^\mathcal{M}(\#[k\delta]\leq^k) \cdot e^{-\lambda t}.
$$

**Proof.** First, we show that the set $\#[k\delta + t]\leq^k$ corresponds to the paths of $\#[k\delta]\leq^k$ with the additional requirement that no transition is taken between the time points $k\delta$ and $k\delta + t$, i.e.,

$$
\#[k\delta + t]\leq^k = \{\pi \in \#[k\delta]\leq^k \mid \text{there is no prefix } \pi' \text{ of } \pi \text{ with } k\delta < T(\pi') \leq k\delta + t\}.
$$

32
"\(\subseteq\)" If \(\pi \in \#[k\delta + t]^{\leq k}\), then \(\pi \in \#[k\delta]^{\leq k}\) follows immediately. Furthermore, assume towards a contradiction that there is a prefix \(\pi'\) of \(\pi\) with \(k\delta < T(\pi') \leq k\delta + t\). Then, \(k < T(\pi')/\delta \leq |\pi'|_{ds}\) (cf. Lemma 5). As \(T(\pi') \leq k\delta + t\), this means that \(|\text{pref}_T(\pi, k\delta + t)|_{ds} \geq |\pi'|_{ds} > k\) which contradicts \(\pi \in \#[k\delta + t]^{\leq k}\).

"\(\supseteq\)" For \(\pi \in \#[k\delta]^{\leq k}\) with no prefix \(\pi'\) such that \(k\delta < T(\pi') \leq k\delta + t\), it holds that \(\text{pref}_T(\pi, k\delta + t) = \text{pref}_T(\pi, k\delta)\). Hence, \(|\text{pref}_T(\pi, k\delta + t)|_{ds} = |\text{pref}_T(\pi, k\delta)|_{ds} \leq k\) and it follows that \(\pi \in \#[k\delta + t]^{\leq k}\).

The probability for no transition to be taken between \(k\delta\) and \(k\delta + t\) only depends on the current state at time point \(k\delta\). More precisely, for some state \(s \in \text{MS}\) assume the set of paths \(#[k\delta]^{\leq k}\) on the current state at time point zero. As this happens with probability one, it follows that \(\pi, k\delta\). With \(\lambda \geq E(s)\) for all \(s \in \text{MS}\) it follows that

\[
\Pr^M_\sigma(\#[k\delta + t]^{\leq k}) = \Pr^M_\sigma(\{\pi \in \#[k\delta]^{\leq k} \mid \text{there is no prefix } \pi' \text{ of } \pi \text{ with } k\delta < T(\pi') \leq k\delta + t\})
\]

\[
= \sum_{s \in \text{MS}} \Pr^M_\sigma(\{\pi \in \#[k\delta]^{\leq k} \mid \text{last}(\text{pref}_T(\pi, k\delta)) = s\}) \cdot e^{-E(s)t}
\]

\[
\geq \sum_{s \in \text{MS}} \Pr^M_\sigma(\{\pi \in \#[k\delta]^{\leq k} \mid \text{last}(\text{pref}_T(\pi, k\delta)) = s\}) \cdot e^{-\lambda t}
\]

\[
= \Pr^M_\sigma(\#[k\delta]^{\leq k}) \cdot e^{-\lambda t}.
\]

\(\square\)

**Proof (of Lemma 7).** Let \(\mathcal{M} = (S, \text{Act}, \rightarrow, s_0, \emptyset)\). By induction over \(k\), we show that

\[
\Pr^M_\sigma(\#[k\delta]^{\leq k}) \geq (1 + \lambda\delta)^k \cdot e^{-\lambda\delta k}.
\]

The claim follows as \(#[k\delta]^{\geq k} = \text{IPaths}^M \setminus \#[k\delta]^{\leq k}\).

For \(k = 0\), we have \(\pi \in \#[0 \cdot \delta]^{\leq 0}\) iff \(\pi\) takes no Markovian transition at time point zero. As this happens with probability one, it follows that

\[
\Pr^M_\sigma(\#[0 \cdot \delta]^{\leq 0}) = 1 = (1 + \lambda\delta)^0 \cdot e^{-\lambda\delta \cdot 0}.
\]

We assume in the induction step that the proposition holds for some fixed \(k\). We distinguish between two cases for the initial state \(s_0\) of \(\mathcal{M}\).

**Case** \(s_0 \in \text{MS}\): We partition the set \(\#[k\delta + \delta]^{\leq k+1} = A^\geq \delta \cup A^{<\delta}\) with

\[
A^\geq \delta = \{s_0 \xrightarrow{\delta} s_1 \xrightarrow{\delta} \cdots \in \#[k\delta + \delta]^{\leq k+1} \mid t \geq \delta\}
\]

\[
A^{<\delta} = \{s_0 \xrightarrow{\delta} s_1 \xrightarrow{\delta} \cdots \in \#[k\delta + \delta]^{\leq k+1} \mid t < \delta\}.
\]

Hence, \(A^\geq \delta\) contains the paths where we wait at least \(\delta\) time units at \(s_0\) and \(A^{<\delta}\) contains the paths where the first transition is taken within \(t < \delta\) time units. It follows that \(\Pr^M_\sigma(\#[k\delta + \delta]^{\leq k+1}) = \Pr^M_\sigma(A^\geq \delta) + \Pr^M_\sigma(A^{<\delta})\). We consider the probabilities for \(A^\geq \delta\) and \(A^{<\delta}\) separately.
\[ \text{Pr}_\pi^M(A^{\geq \delta}) : \text{A path } s_0 \stackrel{t}{\longrightarrow}s_1 \stackrel{\kappa_1}{\longrightarrow} \ldots \in A^{\geq \delta}, \text{ after the first } \delta \text{ time units there are at most } k \text{ digitization steps within the next } k\delta \text{ time units, i.e.,} \]

\[ s_0 \stackrel{t+\delta}{\longrightarrow}s_1 \stackrel{\kappa_1}{\longrightarrow} \ldots \in A^{\geq \delta} \iff s_0 \rightarrow s_1 \stackrel{\kappa_1}{\longrightarrow} \ldots \in \#([k\delta]^{\leq k}). \]

The probability for \( A^{\geq \delta} \) can therefore be derived from the probability to wait at \( s_0 \) for at least \( \delta \) time units and the probability for \( \#([k\delta]^{\leq k}) \). In order to apply this, we need to modify the considered scheduler as it might depend on the sojourn time in \( s_0 \). Let \( \sigma_\delta \) be the scheduler for \( M \) that mimics \( \sigma \) on paths where the first transition is delayed by \( \delta \), i.e., \( \sigma_\delta \) satisfies

\[ \sigma_\delta(s_0 \rightarrow \ldots \rightarrow s_{n-1} \rightarrow s_n, \alpha) = \sigma(s_0 \stackrel{t+\delta}{\longrightarrow} \ldots \rightarrow s_n, \alpha). \]

for all \( s_0 \rightarrow \ldots \rightarrow s_{n-1} \rightarrow s_n \in FPaths^M \) and \( \alpha \in \text{Act} \). It holds that

\[
\text{Pr}_\sigma^M(A^{\geq \delta}) = e^{-E(s_0)\delta} \cdot \text{Pr}_{\sigma_\delta}^M(\#([k\delta]^{\leq k}) \geq E(s_0)\delta) \cdot (1 + \lambda \delta)^k \cdot e^{-\lambda \delta k} \\
= e^{-E(s_0)\delta} \cdot (1 + \lambda \delta)^{k-1} \cdot e^{-\lambda \delta (k+1)} \cdot e^{\lambda \delta} \\
= (1 + \lambda \delta)^k \cdot e^{-\lambda \delta (k+1)} \cdot e^{\lambda \delta}. \tag{8}
\]

\[ \text{Pr}_\pi^M(A^{< \delta}) : \text{A path } s_0 \stackrel{t}{\longrightarrow}s_1 \stackrel{\kappa_1}{\longrightarrow} \ldots \in A^{< \delta}, \text{ the first digitization step happens at less than } \delta \text{ time units, i.e., } 0 \leq t < \delta. \text{ It follows that there are at most } k \text{ digitization steps in the remaining } k\delta + \delta - t \text{ time units, i.e.,} \]

\[ s_0 \rightarrow s_1 \stackrel{\kappa_1}{\longrightarrow} s_2 \stackrel{\kappa_2}{\longrightarrow} \ldots \in A^{< \delta} \iff s_1 \rightarrow s_2 \stackrel{\kappa_2}{\longrightarrow} \ldots \in \#^{s_i}[k\delta + \delta - t]^{\leq k}, \]

where \( \#^{s_i}[k\delta + \delta - t]^{\leq k} \) refers to the paths \( \#([k\delta + \delta - t]^{\leq k}) \) of \( M^{s_i} = (S, \text{Act}, \rightarrow, s_1, \rho_1, \ldots, \rho_t) \), the MA obtained from \( M \) by changing the initial state to \( s_1 \). Hence, the probability for \( A^{< \delta} \) can be derived from the probability to take a transition from \( s_0 \) to some state \( s \) within \( t < \delta \) time units and the probability for \( \#^{s}[k\delta + \delta - t]^{\leq k} \). Again, we need to adapt the considered scheduler. Let \( \pi \in FPaths^M \) with \( \text{last}(\pi) = s \). The scheduler \( \sigma[\pi] \) for \( M^s \) mimics the scheduler \( \sigma \) for \( M \), where \( \pi \) is prepended to the given path, i.e., we set

\[ \sigma[\pi](s \stackrel{\kappa_1}{\longrightarrow} \ldots \rightarrow s_{n-1} \rightarrow s_n, \alpha) = \sigma(s \stackrel{\kappa_1}{\longrightarrow} \ldots \rightarrow s_n, \alpha) \]
for all $s \overset{\kappa_1}{\longrightarrow} \ldots \overset{\kappa_{n-1}}{\longrightarrow} s_n \in \textsc{FPaths}^{M^*}$ and $\alpha \in \text{Act}$. With Lemma 7 it follows that

\[
\Pr_\sigma^M(A^{<\delta}) = \int_0^\delta \Pr_\sigma^M(\#[k\delta + \delta - t] \leq k) \cdot e^{-\int_0^\delta \Pr_\sigma^M(\#[s] \leq k) \cdot e^{-\lambda \delta - t}) dt \geq (1 + \lambda \delta)^k \cdot e^{-\lambda \delta} \cdot e^{-\lambda \delta - t}) dt = (1 + \lambda \delta)^k \cdot e^{-\lambda \delta} \cdot E(s_0) \cdot \int_0^\delta e^{-\int_0^\delta \Pr_\sigma^M(\#[s] \leq k) \cdot e^{-\lambda \delta - t}) dt = (1 + \lambda \delta)^k \cdot e^{-\lambda \delta(k+1)} \cdot E(s_0) \cdot \int_0^\delta e^{(\lambda - E(s_0))t} dt .
\]  

(9)

Combining the results for $A^{\geq\delta}$ and $A^{<\delta}$ (i.e., Equations 8 and 9), we obtain

\[
\Pr_\sigma^M(\#[k\delta + \delta] \leq k+1) = \Pr_\sigma^M(A^{\geq\delta}) + \Pr_\sigma^M(A^{<\delta}) 
\]

\[
\geq (1 + \lambda \delta)^k \cdot e^{-\lambda \delta(k+1)} \cdot \left( E(s_0) \cdot \int_0^\delta e^{(\lambda - E(s_0))t} dt \right) \]

\[
\geq (1 + \lambda \delta)^k \cdot e^{-\lambda \delta(k+1)} \cdot (1 + \lambda \delta) = (1 + \lambda \delta)^{k+1} \cdot e^{-\lambda \delta(k+1)} ,
\]

where the inequality marked with * is due to

\[
e^{(\lambda - E(s_0))\delta} + E(s_0) \cdot \int_0^\delta e^{(\lambda - E(s_0))t} dt = e^{(\lambda - E(s_0))\delta} + (E(s_0) - \lambda - \delta) \cdot \int_0^\delta e^{(\lambda - E(s_0))t} dt = e^{(\lambda - E(s_0))\delta} - (\lambda - E(s_0)) \cdot \int_0^\delta e^{(\lambda - E(s_0))t} dt + \lambda \cdot \int_0^\delta e^{(\lambda - E(s_0))t} dt \]

\[
= \begin{cases} 
1 - 0 + \lambda \cdot \int_0^\delta e^{(\lambda - E(s_0))t} dt & \text{if } E(s_0) = \lambda \\
\lambda \cdot \int_0^\delta e^{(\lambda - E(s_0))t} dt & \text{if } E(s_0) < \lambda 
\end{cases} \]

\[
= 1 + \lambda \cdot \int_0^\delta e^{(\lambda - E(s_0))t} dt \geq 1 + \lambda \cdot \int_0^\delta 1 dt = 1 + \lambda \delta .
\]

35
Since \( M \) is non-zeno, a state \( s \in MS \) is reached from \( s_0 \) within zero time almost surely (i.e., with probability one). From the previous case, it already follows that the Proposition holds for \( M^* \) with \( s \in MS \) and the set \( \#^*[k\delta + \delta] \leq k+1 \). With \( \Pi_{MS} = \{ s_0 \to s_1 \to s_n \in FPaths^M \mid s_n \in MS \text{ and } \forall i < n: s_i \in PS \} \) we obtain

\[
\Pr_{\sigma}^{M}(\#^*[k\delta + \delta] \leq k+1) = \int_{\pi \in \Pi_{MS}} \Pr_{\sigma}[\pi](\#^*[k\delta + \delta] \leq k+1) d\Pr_{\sigma}^{M}(\pi)
\]

\[
\geq \int_{\pi \in \Pi_{MS}} (1 + \lambda \delta)^{k+1} \cdot e^{-\lambda \delta(k+1)} d\Pr_{\sigma}^{M}(\pi)
\]

\[
= (1 + \lambda \delta)^{k+1} \cdot e^{-\lambda \delta(k+1)} \cdot \Pr_{\sigma}^{M}(\Pi_{MS})
\]

\[
= (1 + \lambda \delta)^{k+1} \cdot e^{-\lambda \delta(k+1)} .
\]

\( \square \)

We now present the proof of Proposition 5.

**Proposition 5.** For \( MA \), scheduler \( \sigma \in GM \), goal states \( G \subseteq S \), digitization constant \( \delta \in \mathbb{R}_{>0} \) and time interval \( I \)

\[
\Pr_{\sigma}^{M}(\diamond I \ G) \in \Pr_{\sigma}^{M}([\diamond^{\downarrow} \ G]) + \left[-\varepsilon^\downarrow(I), \varepsilon^\uparrow(I)\right]
\]

**Proof.** In Section 4.3 we already discussed that

\[
\Pr_{\sigma}(\diamond I \ G) = \Pr_{\sigma}([\diamond^{\downarrow} \ G]) + \Pr_{\sigma}(\diamond I \ G \setminus [\diamond^{\downarrow} \ G]) - \Pr_{\sigma}([\diamond^{\downarrow} \ G] \setminus \diamond I \ G).
\]

The main part of the proof is to show that

\[
\Pr_{\sigma}^{M}([\diamond^{\downarrow} \ G] \setminus \diamond I \ G) \leq \varepsilon^\downarrow(I) \text{ and } \Pr_{\sigma}^{M}(\diamond I \ G \setminus [\diamond^{\downarrow} \ G]) \leq \varepsilon^\uparrow(I). \quad (10)
\]

Then, the proposition follows directly. We show Equation (10) for the different forms of the time interval \( I \).

**Case I = \([0, \infty)\):** In this case we have \( \text{di}(I) = \mathbb{N} \). It follows that

\[
[\diamond^{\downarrow} \ G] = \diamond I \ G = \{ s_0 \xrightarrow{\sigma_0} s_1 \xrightarrow{\sigma_1} \cdots \in IPaths^M \mid s_i \in G \text{ for some } i \geq 0 \}.
\]

Hence,

\[
\Pr_{\sigma}^{M}([\diamond^{\downarrow} \ G] \setminus \diamond I \ G) = \Pr_{\sigma}^{M}(\diamond I \ G \setminus [\diamond^{\downarrow} \ G]) = \Pr_{\sigma}^{M}(\emptyset) = 0 = \varepsilon^\downarrow(I) = \varepsilon^\uparrow(I).
\]

**Case I = \([0, b] \text{ for } b = \text{di}(\delta)\):** We have \( \text{di}(I) = \{0, 1, \ldots, \text{di}(b)\} \).

- We show that \( [\diamond^{\downarrow} \ G] \subseteq \diamond I \ G \) which implies

\[
\Pr_{\sigma}^{M}([\diamond^{\downarrow} \ G] \setminus \diamond I \ G) = \Pr_{\sigma}^{M}(\emptyset) = 0 = \varepsilon^\downarrow(I).
\]

36
Let \( \pi \in [\hat{0}]_{\text{ds}}^\text{di(I)} G \) and let \( \pi' \) be the smallest prefix of \( \pi \) with \( \text{last}(\pi') \in G \). It follows that \( \text{di}(\pi') \) is also the smallest prefix of \( \text{di}(\pi) \) with \( \text{last}(\text{di}(\pi')) \in G \).

Since \( \text{di}(\pi) \in [\hat{0}]_{\text{ds}}^\text{di(I)} G \), it follows that \( |\pi'|_{\text{ds}} = |\text{di}(\pi')|_{\text{ds}} \leq \text{di}_b \). From Lemma 5 we obtain

\[
T(\pi') \leq |\pi'|_{\text{ds}} \cdot \delta = |\text{di}(\pi')|_{\text{ds}} \cdot \delta \leq \text{di}_b \delta = b .
\]

Hence, the prefix \( \pi' \) reaches \( G \) within \( b \) time units, implying \( \pi \in \hat{0}^I G \).

- Next, we show \( \hat{0}^I G \setminus [\hat{0}]_{\text{ds}}^\text{di(I)} G \subseteq \#[b]^{>\text{di}_a} \). With Lemma 6 we obtain

\[
\Pr^M_{\sigma}(\hat{0}^I G \setminus [\hat{0}]_{\text{ds}}^\text{di(I)} G) \leq \Pr^M_{\sigma}(\#[b]^{>\text{di}_a}) \leq 1 - (1 + \lambda \delta)^{\text{di}_a} \cdot e^{-\lambda b} = \varepsilon^I (I)
\]

Consider a path \( \pi \in \hat{0}^I G \setminus [\hat{0}]_{\text{ds}}^\text{di(I)} G \). Note that \( \pi \) reaches \( G \) within \( b \) time units but with more than \( \text{di}_b \) digitization steps. Hence, the prefix of \( \pi \) up to time point \( b \) certainly has more than \( \text{di}_b \) digitization steps, i.e., \( \pi \) satisfies \( |\text{pref}^\pi(\pi, a)|_{\text{ds}} > \text{di}_a \) which means \( \pi \in \#[b]^{>\text{di}_a} \).

Case I = \([a, \infty)\) for \( a = \text{di}_a \delta \): We have \( \text{di}(I) = \{\text{di}_a + 1, \text{di}_a + 2, \ldots\} \).

- We show that \([\hat{0}]_{\text{ds}}^\text{di(I)} G \setminus \hat{0}^I G \subseteq \#[a]^{>\text{di}_a} \). With Lemma 6 we obtain

\[
\Pr^M_{\sigma}(\#[\text{ds}]^\text{di(I)} G \setminus \hat{0}^I G) \leq \Pr^M_{\sigma}(\#[a]^{>\text{di}_a}) \leq 1 - (1 + \lambda \delta)^{\text{di}_a} \cdot e^{-\lambda a} = \varepsilon^I (I)
\]

Consider a path \( \pi \in [\hat{0}]_{\text{ds}}^\text{di(I)} G \setminus \hat{0}^I G \). As \( \pi \notin \hat{0}^I G \), it follows that \( \pi \) has to reach (and leave) \( G \) within less than \( a \) time units. Let \( \bar{\pi} \) be the largest prefix of \( \text{di}(\pi) \) that satisfies \( \text{last}(\bar{\pi}) \in G \). Our observations yield that \( \pi \) leaves \( \text{last}(\bar{\pi}) \) before time point \( a \). Hence, \( \bar{\pi} \) is a prefix of \( \text{di}(\text{pref}^\pi(\pi, a)) \). Moreover, \( |\bar{\pi}|_{\text{ds}} \in \text{di}(I) \) as \( \text{di}(\pi) \in [\hat{0}]_{\text{ds}}^\text{di(I)} G \). It follows that \( |\text{pref}^\pi(\pi, a)|_{\text{ds}} \geq |\bar{\pi}|_{\text{ds}} > \text{di}_a \) which implies \( \pi \in \#[a]^{>\text{di}_a} \).

- Now consider a path \( \pi \in \hat{0}^I G \setminus [\hat{0}]_{\text{ds}}^\text{di(I)} G \). \( \pi \) visits \( G \) only once since \( \pi \in \hat{0}^I G \). Moreover, \( \text{di}(\pi) \) does not visit \( G \) after \( \text{di}_a \) digitization steps due to \( \pi \notin [\hat{0}]_{\text{ds}}^\text{di(I)} G \). This means \( \pi \) visits \( G \) only finitely often. Let \( \pi' = s_0 \xrightarrow{s_1} \cdots \xrightarrow{s_{n-1}} s_n \) be the largest prefix of \( \pi \) such that \( s_n \in G \). Notice that \( |\pi'|_{\text{ds}} \leq \text{di}_a \) holds. Let \( \pi' \xrightarrow{s} s \) be the prefix of \( \pi \) of length \( |\pi'| + 1 \). We show by contradiction that \( a \leq T(\pi' \xrightarrow{s} s) < a + \delta \) holds:

- If \( T(\pi' \xrightarrow{s} s) < a \), then \( \text{last}(\pi') \in G \) is left before time point \( a \) which contradicts \( \pi \in \hat{0}^I G \).

- Further, assume that \( T(\pi' \xrightarrow{s} s) \geq a + \delta \). With Lemma 6 we obtain

\[
T(\pi') \geq a + \delta - |\pi'|_{\text{ds}} \cdot \delta \\
\geq \left(\text{di}_a + 1 - |\pi'|_{\text{ds}}\right) \cdot \delta > 0 .
\]

Hence, \( \pi \) stays at \( \text{last}(\pi') \) for at least \( (j + 1 - |\pi'|_{\text{ds}}) \cdot \delta \) time units which means that \( \text{di}(\pi')^{(1 \xrightarrow{s} \text{last}(\pi'))_{j+1-|\pi'|_{\text{ds}}}} = \bar{\pi} \) is a prefix of \( \text{di}(\pi) \). Since \( |\bar{\pi}|_{\text{ds}} = j + 1 \), this contradicts \( \pi \notin [\hat{0}]_{\text{ds}}^\text{di(I)} G \).
We infer that \( \pi \) takes at least one transition in the time interval \([a, a + \delta]\).

The probability for this can be upper bounded by \(1 - e^{-\lambda \delta} \), i.e.,

\[
\Pr^M_{\sigma}(\Diamond I \ G \setminus [\Diamond_{ds} I \ G]) \\
\leq \Pr^M_{\sigma}(\{ \pi \in \text{IPaths}^M | \pi \text{ takes a transition in time interval } [a, a + \delta]\}) \\
\leq 1 - e^{-\lambda \delta} = \varepsilon^\uparrow(I).
\]

**Case I** \([a, b]\) for \( a = di_a \delta \) and \( b = di_b \delta \): We have \( di(I) = \{di_a + 1, di_a + 2, \ldots, di_b\} \).

- As in the case \( "I = [a, \infty)" \), we show that \([\Diamond_{ds} I \ G] \setminus \Diamond I \ G \subseteq \#[a]^{\geq di_a}\). With Lemma 6 we obtain
  \[
  \Pr^M_{\sigma}(\{\Diamond_{ds} I \ G \setminus \Diamond I \ G \} \leq \Pr^M_{\sigma}(\{[a]^{\geq di_a}\}) \\
  \leq 1 - (1 + \lambda \delta)^{di_a \cdot e^{-\lambda a}} = \varepsilon^\uparrow(I).
  \]

Let \( \pi \in [\Diamond_{ds} I \ G] \setminus \Diamond I \ G \) and let \( \overline{\pi} \) be the largest prefix of \( di(\pi) \) with \( \text{last}(\overline{\pi}) \in G \) and \( |\overline{\pi}|_{ds} \in di(I) \). Such a prefix exists due to \( \pi \in [\Diamond_{ds} I \ G] \). \( \pi \) reaches \( \text{last}(\overline{\pi}) \) with at most \( di_b \) digitization steps and therefore within at most \( b \) time units (cf. Lemma 5). As \( \pi \not\in \Diamond I \ G \), we conclude that \( \pi \) has to reach (and leave) \( \text{last}(\overline{\pi}) \) within less than \( a \) time units. It follows that \( |\text{pref}_T(\pi, a)|_{ds} \geq |\overline{\pi}|_{ds} > di_a \) which implies \( \pi \in [a]^{\geq di_a} \).

- Next, let \( \pi \in [\Diamond_{ds} I \ G] \setminus \Diamond I \ G \) and let \( \pi' = s_0 \xrightarrow{n_0} s_1 \xrightarrow{n_1} \ldots \xrightarrow{n_{n-1}} s_n \) be the largest prefix of \( \pi \) such that \( s_n \in G \) and \( T(\pi') \leq b \). Such a prefix exists due to \( \pi \in [\Diamond I \ G] \). We distinguish two cases.
  - If \( |\pi'|_{ds} > di_b \), then \( \pi \in [b]^{\geq di_b} \) since \( |\text{pref}_T(\pi, b)|_{ds} \geq |\pi'|_{ds} > di_b \).
  - If \( |\pi'|_{ds} \leq di_b \), then \( |\pi'|_{ds} \leq di_a \) holds due to \( \pi \not\in [\Diamond_{ds} I \ G] \). Similar to the case \( "I = [a, \infty)" \) we can show that \( \pi \) takes at least one transition in time interval \([a, a + \delta]\).

It follows that

\[
[\Diamond_{ds} I \ G] \setminus [\Diamond I \ G] \\
\subseteq [b]^{\geq di_b} \cup \{ \pi \in \text{IPaths}^M | \pi \text{ takes a transition in time interval } [a, a + \delta]\}
\]

Hence,

\[
\Pr^M_{\sigma}(\Diamond I \ G \setminus [\Diamond_{ds} I \ G]) \leq 1 - (1 + \lambda \delta)^{di_a \cdot e^{-\lambda a}} + 1 - e^{-\lambda \delta} = \varepsilon^\uparrow(I).
\]

\( \square \)

**E.3 Proof of Theorem 5**

**Theorem 5.** Let \( \mathcal{M} \) be an MA with digitization \( \mathcal{M}_d \). Furthermore, let \( \Diamond \) be (un)timed reachability or expected reward objectives with threshold relations \( \triangleright \) and \( |\Diamond| = d \). It holds that \( A^- \subseteq \{p \in \mathbb{R}^d | \text{achieve}^\mathcal{M}(\Diamond \triangleright p)\} \subseteq A^+ \) with:

\[
A^- = \{p' \in \mathbb{R}^d | \forall p \in \mathbb{R}^d: p' \in \varepsilon(\Diamond, p) \text{ implies } \text{achieve}^\mathcal{M}_d(\Diamond \triangleright p)\}
\]

and

\[
A^+ = \{p' \in \mathbb{R}^d | \exists p \in \mathbb{R}^d: p' \in \varepsilon(\Diamond, p) \text{ and } \text{achieve}^\mathcal{M}_d(\Diamond \triangleright p)\}.
\]

38
Proof. For simplicity, we assume that only the threshold relation ≥ is considered, i.e., ⊳ = (≥, . . . , ≥). Furthermore, we restrict ourselves to (un)timed reachability objectives. The remaining cases are treated analogously.

First assume a point \( p' = (p'_1, \ldots, p'_d) \in A' \). Consider the point \( p = (p_1, \ldots, p_d) \) satisfying \( p'_i = p_i - \varepsilon_i^+ \) for each index \( i \). It follows that \( p' \in \varepsilon(\mathcal{O}, p) \) and thus \( \mathcal{M}_\delta, \bar{\sigma} \models \bar{\sigma} \circ (\mathcal{O} \triangleright p) \) for some scheduler \( \bar{\sigma} \in \text{TA}^{M_\delta} \). Consider the scheduler \( \sigma \in GM^M \) given by \( \sigma(\pi, \alpha) = \bar{\sigma}(\text{di}(\pi), \alpha) \) for each path \( \pi \in F\text{Paths}^M \) and action \( \alpha \in \text{Act} \). Notice that \( \bar{\sigma} = \text{di}(\sigma) \). For an index \( i \) let \( \mathcal{O}_i \) be the objective \( \mathcal{P}(\mathcal{O}^G) \).

It follows that

\[
\mathcal{M}_\delta, \sigma \models \mathcal{O}_i \geq p_i \iff \mathcal{M}_\delta, \text{di}(\sigma) \models \mathcal{O}_i \geq p_i \iff \Pr_{\text{di}(\sigma)}^M(\mathcal{O}_i^G) \geq p_i ,
\]

With Corollary 1 it follows that

\[
p'_i = p_i - \varepsilon_i^+ \leq \Pr_{\text{di}(\sigma)}^M(\mathcal{O}_i^G) - \varepsilon_i^+ \leq \Pr_{\sigma}^M(\mathcal{O}_i^G).
\]

As this observation holds for all objectives in \( \mathcal{O} \), it follows that \( \mathcal{M}, \sigma \models \mathcal{O} \triangleright p' \), implying achieve\(^M(\mathcal{O} \triangleright p') \).

The proof of the second inclusion is similar. Assume that \( \mathcal{M}, \sigma \models \mathcal{O} \triangleright p' \) holds for a point \( p' = (p'_1, \ldots, p'_d) \in \mathbb{R}^d \) and a scheduler \( \sigma \in GM^M \). For some index \( i \), consider \( \mathcal{O}_i = \mathcal{P}(\mathcal{O}_i^G) \). It follows that \( \Pr_{\sigma}^M(\mathcal{O}_i^G) \geq p'_i \). With Corollary 1 we obtain

\[
p'_i - \varepsilon_i^- \leq \Pr_{\sigma}^M(\mathcal{O}_i^G) - \varepsilon_i^- \leq \Pr_{\text{di}(\sigma)}^M(\mathcal{O}_i^G).
\]

Applying this for all objectives in \( \mathcal{O} \) yields \( \mathcal{M}_\delta, \text{di}(\sigma) \models \mathcal{O} \triangleright p \), where the point \( p = (p_1, \ldots, p_d) \in \mathbb{R}^d \) satisfies \( p_i = p'_i + \varepsilon_i^- \) or, equivalently, \( p'_i = p_i + \varepsilon_i^- \) for each index \( i \). Note that \( p' \in \varepsilon(\mathcal{O}, p) \) which implies \( \mathcal{P}(\mathcal{O}^G) \).

\[ \square \]

F Comparison to Single-objective Analysis

Corollary 1 generalizes existing results from single-objective timed reachability analysis: For MA \( \mathcal{M} \), goal states \( G \), time bound \( b \in \mathbb{R}_{>0} \), and digitization constant \( \delta \in \mathbb{R}_{>0} \) with \( b/\delta = \text{di}_b \in \mathbb{N} \), [9, Theorem 5.3] states that

\[
\sup_{\sigma \in GM^M} \Pr_{\sigma}^M(\mathcal{O}^{[0,b]}_\delta G) \leq \sup_{\sigma \in \text{TA}^{M_\delta}} \Pr_{\sigma}^M(\mathcal{O}^{[0,\text{di}_b]}_\delta G) + \left[ -\varepsilon^-([0,b]), \varepsilon^+([0,b]) \right].
\]

Corollary 1 generalizes this result by explicitly referring to the schedulers \( \sigma \in GM^M \) and \( \text{di}(\sigma) \in \text{TA}^{M_\delta} \) under which the claim holds. This extension is necessary as a multi-objective analysis can not be restricted to schedulers that only optimize a single objective.

We remark that the proof in [9, Theorem 5.3] can not be adapted to show our result. The main reason is that the proof relies on an auxiliary lemma which claims that

\[ \Pr_{\sigma}^M(\mathcal{O}^{[0,b]}_\delta G \mid |[\delta]|^2 < 2) \leq \Pr_{\sigma}^M(\mathcal{O}^{[0,b]}_\delta G) \] \[ (11) \]

4 We adapt [9, Lemma G.2] to our notations from Appendix 12.
holds for all schedulers $\sigma \in GM^M$. We show that this claim does not hold. The intuition is as follows. Assume we observe that at most one Markovian transition is taken in $\mathcal{M}$ within the first $\delta$ time units (i.e., we observe a path in $\#[\delta]<2$). The lemma claims that under this observation the probability to reach $G$ within $b$ time units does not increase. We give a counterexample to illustrate that there are schedulers for which this is not true. Consider the MA $\mathcal{M}$ from Figure 8 and let $\sigma$ be the scheduler for $\mathcal{M}$ satisfying

$$
\sigma(s_0 \xrightarrow{t_1} s_1 \xrightarrow{t_2} s_2, \alpha) = \begin{cases} 1 & \text{if } t_1 + t_2 > \delta \\ 0 & \text{otherwise.} \end{cases}
$$

Hence, $\sigma$ chooses $\alpha$ iff there are less than two digitization steps within the first $\delta$ time units. It follows that the probability to reach $G = \{s_3\}$ on a path in $\#[\delta] \geq 2$ is zero. We conclude that

$$
\Pr_{\sigma}^{\mathcal{M}}(\diamond[0,b]\{s_3\}) = \Pr_{\sigma}^{\mathcal{M}}(\diamond[0,b]\{s_3\} \cap \#[\delta] < 2) + \Pr_{\sigma}^{\mathcal{M}}(\diamond[0,b]\{s_3\} \cap \#[\delta] \geq 2) = 0
$$

which contradicts Equation 11.

G Further Details for the Experiments

G.1 Benchmark Details

We depict additional information regarding our experiments on multi-objective MAs.

Job scheduling. The job scheduling case study originates from [13] and was already discussed in Section 1. We consider $N$ jobs that are executed on $K$ identical processors. Each of the $N$ jobs gets a different rate between 1 and 3. We consider the following objectives.

$E_1$: Minimize the expected time until all jobs are completed.
$E_2$: Minimize the expected time until $\lceil N/2 \rceil$ jobs are completed.
$E_3$: Minimize the expected waiting time of the jobs.

$P$: Minimize the probability that the job with the lowest rate is completed before the job with the highest rate.

$P_{1\leq 1}^\leq$: Maximize the probability that all jobs are completed within $N/2K$ time units.

$P_{2\leq 1}^\leq$: Maximize the probability that $\lceil N/2 \rceil$ jobs are completed within $N/4K$ time units.

The objectives have been combined as follows: ($O^i$ refers to the objectives considered in Column $i$ of Table I):

$$O^1 = (E_1, E_2, E_3), \quad O^2 = (E_1, P_{2}^\leq), \quad O^3 = (P, E_1, E_2, E_3), \quad O^4 = (P, E_3, P_{1}^\leq, P_{2}^\leq)$$

**Polling.** The polling system is based on [34,35]. It considers two stations, each having a separate queue storing up to $K$ jobs of $N$ different types. The jobs arrive at Station $i$ (for $i \in \{1,2\}$) with some rate $\lambda_i$ as long as the queue of the station is not full. A server polls the two stations and processes the jobs by (non-deterministically) taking a job from a non-empty queue. The time for processing a job is given by a rate which depends on the type of the job. Erasing a job from a queue is unreliable, i.e., there is a 10% chance that an already processed job stays in the queue. For $i \in \{1,2\}$ we assume the following objectives:

$E_i$: Maximize the expected number of processed jobs of Station $i$ until its queue is full.

$E_{2+i}$: Minimize the expected sum of all waiting times of the jobs arriving at Station $i$ until the queue of Station $i$ is full.

$P_{i\leq 1}^\leq$: Minimize the probability that the queue of Station $i$ is full within two time units.

The objectives have been combined as follows: ($O^i$ refers to the objectives considered in Column $i$ of Table I):

$$O^1 = (E_1, E_2), \quad O^2 = (E_1, E_2, E_3, E_4), \quad O^3 = (P_{1}^\leq, P_{2}^\leq), \quad O^4 = (E_1, E_2, P_{1}^\leq, P_{2}^\leq)$$

**Stream.** This case study considers a client of a video streaming platform. The client consecutively receives $N$ data packages and stores them into a buffer. The buffered packages are processed during the playback of the video. The time it takes to receive (or to process) a single package is modeled by an exponentially distributed delay. Whenever a package is received and the video is not playing, the client nondeterministically chooses whether it starts the playback or whether it keeps on buffering. The latter choice is not reliable, i.e., there is a 1% chance that the playback is started anyway. In case of a buffer underrun, the playback is paused and the client waits for new packages to arrive. We analyzed the following objectives:

$E_1$: Minimize the expected buffering time until the playback is finished.

---

$^5$ A buffer underrun occurs when the next package needs to be processed while the buffer is empty.
Table 2. Additional model details.

| N(-K) | #states | #choices | #transitions | #MS | λmax |
|-------|---------|----------|--------------|-----|------|
| jobs  |         |          |              |     |      |
| 10-2  | 12,554  | 23,061   | 34,581       | 11,531 | 5.7  |
| 12-3  | 116,814 | 225,437  | 450,783      | 112,719 | 8.5  |
| 17-2  | 4,587,537 | 8,912,931 | 13,369,379 | 4,456,466 | 5.9  |
| polling | 3-2     | 1,820    | 1,852        | 2,477 | 508  | 14   |
|       | 3-3     | 9,408    | 18,295       | 24,536 | 4,801 | 14   |
|       | 4-4     | 827,735  | 1,682,325    | 2,146,086 | 465,125 | 16   |
| stream | 30      | 1,426    | 1,861        | 2,731 | 931  | 8    |
|       | 250     | 9,4376   | 125,501      | 187,751 | 62,751 | 8    |
|       | 1000    | 1,502,501| 2,002,001    | 3,001,001 | 1,001,001 | 8    |
| mutex | 2       | 13,476   | 31,752       | 36,120 | 216  | 2    |
|       | 3       | 38,453   | 99,132       | 111,687 | 8,487 | 3    |

\( E_2 \): Minimize the expected number of buffer underruns during the playback.
\( E_3 \): Minimize the expected time to start the playback.
\( P^\leq_1 \): Minimize the probability for a buffer underrun within 2 time units.
\( P^\leq_2 \): Maximize the probability that the playback starts within 0.5 time units.

The objectives have been combined as follows: (\( O^i \) refers to the objectives considered in Column \( i \) of Table II):

\[
O^1 = (E_1, E_2) \quad O^2 = (E_3, P^\leq_1) \quad O^3 = (P^\leq_1, P^\leq_2) \quad O^4 = (E_1, E_3, P^\leq_1)
\]

Mutex. This case study regards a randomized mutual exclusion protocol based on [36,35]. Three processes nondeterministically choose a job for which they need to enter the critical section. The amount of time a process spends in its critical section is given by a rate which depends on the chosen job. There are \( N \) different types of jobs. For each \( i \in \{1,2,3\} \) the following objective are considered:

\( P^\leq_i \): Maximize the probability that Process \( i \) enters its critical section within 0.5 time units.
\( P^\leq_{3+i} \): Maximize the probability that Process \( i \) enters its critical section within 1 time unit.

The objectives have been combined as follows: (\( O^i \) refers to the objectives considered in Column \( i \) of Table II):

\[
O^1 = (P^\leq_1, P^\leq_2, P^\leq_3) \quad O^2 = (P^\leq_4, P^\leq_5, P^\leq_6)
\]

G.2 Comparison with PRISM

We considered PRISM 4.3.1 obtained from its website [www.prismmodelchecker.org](http://www.prismmodelchecker.org).

We conducted our experiments on PRISM with both variants of the value iteration-based implementation (standard and Gauss-Seidel) and chose the faster variant.
For each benchmark instance. For all experiments the approximation precision $\eta = 0.001$ was considered.

The detailed results are given in Table 3. We depict the different benchmark instances with the number of states of the MDP (Column \#states) and the considered combination of objectives (P represents an (untimed) probabilistic objective, E an expected reward objective, and C$\leq$ a step-bounded reward objective). Column iter lists the time required for the iterative exploration of the set of achievable points as described in [15]. In Column verif we depict the verification time – including the time for the iterations as well as the conducted preprocessing steps. Column total indicates the total runtime of the tool which includes model building time and verification time. For our implementation, we also list the number of vertices of the obtained under-approximation (Column pts).

During our experiments we observed some issues concerning the implementation in PRISM. For example PRISM does not detect that both objectives considered for the sched.-instances yield infinite rewards under every possible resolution of non-determinism. Instead of that, PRISM gives an incorrect answer.
Table 4. Results for our implementation (Storm) and IMCA for single-objective MAs. All run-times are in seconds.

| benchmark instance | #states | IMCA verif. time | Storm (multi) verif. time | Storm (single) verif. time |
|--------------------|---------|------------------|---------------------------|---------------------------|
| jobs               | 10,2    | 0.009            | 0.047                     | 0.021                     |
|                    | 10,2    | 1.054            | 2.977                     | 1.702                     |
|                   | 12,3    | 0.136            | 0.556                     | 0.279                     |
|                   | 12,3    | 19.938           | 56.242                    | 31.682                    |
| jobs               | 3,3     | 6.254            | 0.102                     | 0.095                     |
|                    | 3,3     | 21.948           | 54.350                    | 14.163                    |
|                   | 4,4     | 3.630.283        | 52.162                    | 47.746                    |
|                   | 4,4     | 3.424.730        | 8.615.390                 | 1597.095                  |
| polling            | 30      | 0.005            | 0.009                     | 0.004                     |
|                    | 30      | 0.481            | 1.578                     | 0.509                     |
|                   | 250     | 2.972            | 1.462                     | 1.261                     |
|                   | 250     | 36.663           | 111.450                   | 33.527                    |
| mutex              | 2       | 1.785            | 1.217                     | 0.4                       |
|                    | 2       | 6.922            | 4.118                     | 1.008                     |

G.3 Comparison with IMCA

We consider IMCA 1.6 obtained from [https://github.com/buschko/imca](https://github.com/buschko/imca). The experiments on IMCA have been conducted with and without enabling value-iteration and we chose the faster variant for each benchmark instance. For timed reachability objectives, the precision $\eta = 0.01$ was considered in all experiments.

The resulting verification times are given in Table 4. We depict the different benchmark instances with the number of states of the MA (Column #states) and the considered objective (as discussed in App. G.1). Besides the run-times of IMCA, we depict the run-times of our implementation (effectively performing multi-objective model checking with only one objective) in Column Storm (multi). Column Storm (single) shows the run-times obtained when Storm is invoked with standard (single-objective) model checking methods.