1 Probabilistic Systems

In the literature, various formal underpinnings have been proposed to reason about the probability of specific events in a dynamically behaving system. In this document, such formal underpinnings are summarized under the term *probabilistic systems*. This chapter introduces two probabilistic systems, namely *generic Markov chains* and *choice-aware Markov decision processes*. These are later used for the probabilistic safety analysis of executable models.

Roughly speaking, a Markov chain (MC) contains for each state a probability distribution over potential successor states. MCs can be used for the analysis of purely probabilistic models, i.e., models containing no nondeterministic choice. Section 1.1 describes generic Markov chains, a slightly generalized version of MCs that have been developed to better suit to executable models than standard MCs.

Markov decision processes (MDPs) combine nondeterministic choice and probabilistic choice: for each state, a MDP contains a nondeterministic choice between different probability distributions over potential successor states. An intuitive way to look at a transition in a MDP is that *first* one probability distribution of the active state is selected *nondeterministically*, and *secondly*, this probability distribution is used to select a successor state *probabilistically*. Choice-aware Markov decision processes (CMDPs) are a major extension of the well-known MDPs: to define the transitions of a state, there may be multiple consecutive nondeterministic and probabilistic choices in any order, in contrast to MDPs, which are limited to exactly one nondeterministic choice and afterwards exactly one probabilistic choice per transition. In CMDPs, the choices are "saved" explicitly in the structure (hence "choice-aware"). CMDPs enable the probabilistic analysis of executable models that contain both probabilistic and nondeterministic choices, and are described in more detail in section 1.2.

Both section 1.1 (discussing generic MCs) and section 1.2 (discussing generic CMDPs) have the same outline. This approach is useful because the definitions and proofs of the generic CMDPs are based on those of the generic MCs. First, the probabilistic systems are introduced formally. Afterwards, paths and a probability measure based on that paths are defined for the respective system.

Generic MCs have been published in [LK+17]. Descriptions about standard Markov chains and standard Markov decision processes have been discussed by many authors before, e.g., in [BK08; Bai98]. The definitions of generic MCs and CMDPs are structurally close to their standard counterparts. This chapter is an excerpt from the thesis "Probabilistic Safety Analysis of Executable models" [Leu18]. More details can be found there.

1.1 Generic Markov Chains

As the first probabilistic system, generic Markov chains (generic MCs/GMCs), which are suited to model purely probabilistic systems, are introduced.

Definition 1.1 (Generic Markov Chain)**.** A generic Markov chain $\mathcal{M}$ is represented by the tuple (S, Θ, τ, R) consisting of

- a countable set S of *states*, and
- a countable set Θ of *targets* with a *target state* function $\tau : \Theta \to S$, and
- a *transition distribution* function $R : S \to \mathit{Dists}(\Theta)$

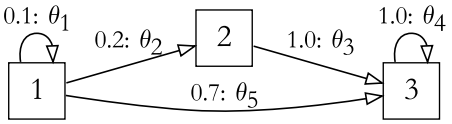
where $\mathit{Dists}(\Theta) = \{\mu : \Theta \to [0, 1] \mid \sum_{\theta \in \Theta} \mu(\theta) = 1\}$.

Let μ_s be a shorthand for $R(s)$. By convention $S^{\mathcal{M}}$ stands for $\mathcal{M}$'s states, $\Theta^{\mathcal{M}}$ for $\mathcal{M}$'s targets, and so on. This is used in the remainder, when the corresponding generic Markov chain is not clear from the context.

By choosing the states as targets, i.e., $\Theta = S$, and the identity function as τ, a probabilistic system is obtained that is commonly known as Markov chains. Such Markov chains are identified as *standard Markov chains* in the remainder.

L-labeled MC

This work introduces another useful manifestation of generic Markov chains, the so called labeled Markov chains. An *L-labeled Markov chain* is a generic Markov chain where Θ is chosen to be $L \times S$ for some set of *labels* L with $\tau(\ell, s) = s$. In contrast to approaches where states are labeled, the labeling belongs to the transitions. Shifting the labeling on the transitions is one reason for the efficiency of the implemented algorithms.



target	label
θ_1	$e0$
θ_2	$e0$
θ_3	$e0, e1$
θ_4	
θ_5	$e0$

Figure 1.1: Labeled Markov chain with 3 states

Figure 1.1 depicts an example of a $2^{\{e0,e1\}}$-labeled MC. The squared nodes represent the states, e.g., node 1 represents s_1. The distribution function of a state is depicted by the white-headed outgoing arcs of its corresponding node. Each arc is associated with a target, e.g., the reflexive arc of state 1 is associated with θ_1. The target node of an arc corresponds to the target state of its target, e.g., $\tau(\theta_1) = s_2$. The labels of each target are given in the table. This labeled Markov chain can be used to calculate the probability that eventually a label like $e0$ is reached from a specific state. How this can be formally expressed and calculated is topic of the remainder of this subsection.

1.1.1 Paths and Probability Measure

Let $\mathcal{M} = (S, \Theta, \tau, R)$ be a generic MC.

π

A finite path $\pi = \theta_1 \dots \theta_n \in \Theta^*$ of $\mathcal{M}$ is a sequence of targets where $\mu_{\tau(\theta_i)}(\theta_{i+1}) > 0$

for all $1 \leq i < n$. The empty sequence is also a valid finite path; $\varnothing$ denotes the empty sequence. $\mathit{FinPaths}^{\mathcal{M}}$ is the set of all finite paths of $\mathcal{M}$. An anchored finite path $\pi_{\Lsh} = [s, \theta_1\,\theta_2 \ldots \theta_n] \in S \times \mathit{FinPaths}^{\mathcal{M}}$ of $\mathcal{M}$ is a pair of a state and a finite path where $\mu_s(\theta_1) > 0$. Let $|\pi_{\Lsh}| = n$ be the path length of $\pi_{\Lsh} = [s, \theta_1\,\theta_2 \ldots \theta_n]$. $\mathit{FinPaths}^{\mathcal{M}}_{\Lsh}$ is the set of all anchored finite paths of $\mathcal{M}$. $\mathit{FinPaths}^{\mathcal{M}}_{s} = (\{s\} \times \mathit{FinPaths}^{\mathcal{M}}) \cap \mathit{FinPaths}^{\mathcal{M}}_{\Lsh}$ is the set of all anchored finite paths starting from s. Let $\tau : \mathit{FinPaths}^{\mathcal{M}}_{\Lsh} \to S$ be a function that returns the last state of an anchored finite path, i.e., $\tau([s, \varnothing]) = s$, and $\tau([s, \theta_1 \ldots \theta_n]) = \tau(\theta_n)$ otherwise. Given an anchored finite path $\pi_{\Lsh} = [s, \theta_1 \ldots \theta_n]$ and a target θ, let $\pi_{\Lsh}\theta = [s, \theta_1 \ldots \theta_n\,\theta]$ be the concatenation of the finite path with the target. Sometimes, a subset $\Pi \subseteq \mathit{FinPaths}^{\mathcal{M}}_{\Lsh}$ is from interest; then, such a subset Π is called *paths of interest*.

$\pi_{\Lsh}$ $|\pi_{\Lsh}|$ τ

An infinite path $\widehat{\pi} = \theta_1\,\theta_2\,\theta_3 \ldots \in \Theta^{\omega}$ of $\mathcal{M}$ is a sequence of targets where for all $i \geq 1$, $\mu_{\tau(\theta_i)}(\theta_{i+1}) > 0$. $\mathit{InfPaths}^{\mathcal{M}}$ is the set of all infinite paths of $\mathcal{M}$. An anchored infinite path $\widehat{\pi}_{\Lsh} = [s, \theta_1\,\theta_2\,\theta_3 \ldots] \in S \times \mathit{InfPaths}^{\mathcal{M}}$ of $\mathcal{M}$ is a pair of a state and an infinite path where $\mu_s(\theta_1) > 0$. $\mathit{InfPaths}^{\mathcal{M}}_{\Lsh}$ is the set of all infinite anchored infinite paths of $\mathcal{M}$. $\mathit{InfPaths}^{\mathcal{M}}_{s} = (\{s\} \times \mathit{InfPaths}^{\mathcal{M}}) \cap \mathit{InfPaths}^{\mathcal{M}}_{\Lsh}$ is the set of all anchored infinite paths starting from s. Let $\widehat{\pi}[..k] = \theta_1 \ldots \theta_k$ denote the k-th prefix of $\widehat{\pi} = \theta_1\,\theta_2\,\theta_3 \ldots$, and let $\mathit{Pref}(\widehat{\pi}) = \{\pi' \mid \pi' \text{ is prefix of } \widehat{\pi}\}$ denote the set of all prefixes of $\widehat{\pi}$. Note that $\varnothing$ is a prefix of all infinite paths. Also, let $\mathit{Pref}([s, \widehat{\pi}]) = \{[s, \pi] \mid \pi \in \mathit{Pref}(\widehat{\pi})\}$ denote the set of all anchored prefixes of $[s, \widehat{\pi}]$.

$\widehat{\pi}$ $\widehat{\pi}_{\Lsh}$ $\widehat{\pi}[..k]$

In the remainder, both finite and infinite paths are sometimes just called paths when it is clear from the context which one is meant.

The *cylinder set* $\pi_{\Lsh}{\uparrow^{\mathcal{M}}}$ of the anchored finite path $\pi_{\Lsh} \in \mathit{FinPaths}^{\mathcal{M}}_{\Lsh}$ contains all anchored infinite paths of $\mathcal{M}$ that start with $\pi_{\Lsh}$. More formally, $\pi_{\Lsh}{\uparrow^{\mathcal{M}}} = \{\widehat{\pi}'_{\Lsh} \in \mathit{InfPaths}^{\mathcal{M}}_{\Lsh} \mid \pi_{\Lsh} \in \mathit{Pref}(\widehat{\pi}'_{\Lsh})\}$. Let $\Pi \subseteq \mathit{FinPaths}^{\mathcal{M}}$, then $\Pi{\uparrow^{\mathcal{M}}} = \bigcup_{\pi_{\Lsh} \in \Pi} \pi_{\Lsh}{\uparrow^{\mathcal{M}}}$. If $\mathcal{M}$ is clear from the context, $\pi_{\Lsh}{\uparrow}$ abbreviates $\pi_{\Lsh}{\uparrow^{\mathcal{M}}}$, and $\Pi{\uparrow}$ abbreviates $\Pi{\uparrow^{\mathcal{M}}}$.

$\pi_{\Lsh}{\uparrow^{\mathcal{M}}}$ $\Pi{\uparrow^{\mathcal{M}}}$ $\pi_{\Lsh}{\uparrow}$, $\Pi{\uparrow}$

The cylinder sets of a generic Markov chain are the basic elements to define its probability measure.

Definition 1.2 (Probability Space of a Generic Markov Chain starting in a certain state)**.** The probability space $(\Omega^{\mathcal{M}}_s, \mathfrak{E}^{\mathcal{M}}_s, \mathit{Pr}^{\mathcal{M}}_s)$ of a generic Markov chain $\mathcal{M} = (S, \Theta, \tau, R)$ starting in state $s \in S^{\mathcal{M}}$ consists of

- the sample space $\Omega^{\mathcal{M}}_s = \mathit{InfPaths}^{\mathcal{M}}_s$, and
- the events $\mathfrak{E}^{\mathcal{M}}_s$ as the smallest σ-algebra on $\Omega^{\mathcal{M}}_s$ that contains

$$\{\pi_{\Lsh}{\uparrow} \mid \pi_{\Lsh} \in \mathit{FinPaths}^{\mathcal{M}}_s\}\ , \text{ and}$$

- the probability measure $\mathit{Pr}^{\mathcal{M}}_s$ with

$$\mathit{Pr}^{\mathcal{M}}_s([s, \theta_1 \ldots \theta_n]{\uparrow}) = \mu_s(\theta_1) \cdot \prod_{1 \leq i < n} \mu_{\tau(\theta_i)}(\theta_{i+1})\ .$$

Using this probability measure, the probability of a countable set of anchored finite paths Π starting from state s which are non-overlapping, i.e., $\pi_{\Lsh}{\uparrow} \cap \pi'_{\Lsh}{\uparrow} = \emptyset$ for all

$\pi_{\text{⚓}} \neq \pi'_{\text{⚓}} \in \Pi$, can be calculated. This can be achieved by summing up the probabilities of each anchored finite path in the set, i.e.

$$Pr_s^{\mathcal{M}}(\Pi\uparrow) = Pr_s^{\mathcal{M}}(\bigcup_{\pi_{\text{⚓}} \in \Pi} \pi_{\text{⚓}}\uparrow) = \sum_{\pi_{\text{⚓}} \in \Pi} Pr_s^{\mathcal{M}}(\pi_{\text{⚓}}\uparrow) \ .$$

The non-overlapping property ensures that each path is counted exactly once. To allow this simple summation, Π needs to be a subset of $\mathit{FinPaths}_s^{\mathcal{M}}$. Otherwise, this set may contain paths starting at different states for which the probabilities are defined in other probability spaces. In general, summing up probabilities from different probability spaces is not well defined. Such sums may even have values greater than 1. For that reason, given an arbitrary $\Pi \subseteq \mathit{FinPaths}_{\text{⚓}}^{\mathcal{M}}$, the probability of that paths cannot be calculated. But the probability of those paths in Π that start from state s can be
$\Pi\restriction_s$ calculated. Therefore, the *restriction* to those paths is defined as $\Pi\restriction_s = \Pi \cap \mathit{FinPaths}_s^{\mathcal{M}}$.

1.2 Choice-Aware Markov Decision Processes

After the explanations of the generic Markov chains, choice-aware Markov decision process (CMDPs) are introduced as the second probabilistic system. CMDPs are well-suited for models that comprise both probabilistic and nondeterministic choice. Before CMDPs are defined, its choices and its choice transition function are introduced, which enable CMDPs to have multiple consecutive nondeterministic and probabilistic choices in any order.

Let Θ be a finite set of targets, and $\mathcal{C}$ a finite set of choices, and $\mathit{Dists}(\mathcal{C}) = \{\mu_{\mathcal{C}} : \mathcal{C} \to [0,1] \mid \sum_{c \in \mathcal{C}} \mu_{\mathcal{C}}(c) = 1\}$ be the probability distributions for the choices $\mathcal{C}$. Furthermore, let $\mathit{succ} : \mathcal{C} \to \Theta + \mathit{Dists}(\mathcal{C}) + 2^{\mathcal{C}}$ be the choice transition function that maps each choice to either a target, a probability distribution, or a non-empty set of choices. A set of choices is used to model nondeterminism. The sequence of choices $\varrho = c_0\, c_1 \ldots c_n \in \mathcal{C}^*$ is a choice path of the choice transition function *succ* if for all non-final choices, *succ* returns a probability distribution with a probability greater 0 to its successor (probabilism), or *succ* returns a set of choices that includes the successor (nondeterminism); more formally, for all $0 \leq i < n$ either $\mu_{\mathcal{C}} = \mathit{succ}(c_i)$ with $\mu_{\mathcal{C}}(c_{i+1}) > 0$ or $c_{i+1} \in \mathit{succ}(c_i)$. A choice path $c_0\, c_1 \ldots c_n$ with $n \geq 1$ forms a cycle if the $c_0 = c_n$. A choice transition function *succ* is acyclic, if there exists no choice path of *succ* that forms a cycle. A choice path $c_0\, c_1 \ldots c_n$ is terminal if $\mathit{succ}(c_n) \in \Theta$. Note that it makes sense to call an acyclic choice transition function also terminal or finite, because applying the function iteratively on its result finally terminates.

ϱ

Definition 1.3 (Choice-aware Markov Decision Process)**.** A choice-aware Markov decision process $\mathcal{M}$ is represented by the tuple $(S, \Theta, \tau, \mathcal{C}, \mathit{succ}, C)$ consisting of

- a finite set S of *states*, and
- a finite set Θ of *targets* with a *target state* function $\tau : \Theta \to S$, and
- a finite set $\mathcal{C}$ of *choices* with an acyclic *choice transition* function $\mathit{succ} : \mathcal{C} \to \Theta + \mathit{Dists}(\mathcal{C}) + 2^{\mathcal{C}}$, and
- a function $C : S \to \mathcal{C}$ that determines the root choice of each state,

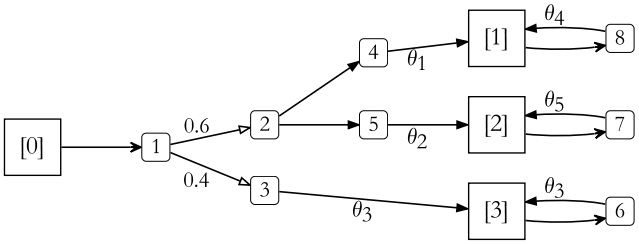
where $\mathit{Dists}(\mathcal{C}) = \{\mu_{\mathcal{C}} : \mathcal{C} \to [0,1] \mid \sum_{c \in \mathcal{C}} \mu_{\mathcal{C}}(c) = 1\}$.

By convention $S^{\mathcal{M}}$ stands for $\mathcal{M}$'s states, $\Theta^{\mathcal{M}}$ for $\mathcal{M}$'s targets, and so on. This is used in the remainder, when the corresponding choice-aware Markov decision process is not clear from the context.

This work introduces another useful manifestation of choice-aware Markov decision processes, the so called labeled choice-aware Markov decision processes. An *L-labeled choice-aware Markov decision processes* is a choice-aware Markov decision process where Θ is chosen to be $L \times S$ for some set of *labels* L with $\tau(\ell, s) = s$.

L-labeled CMDP

Figure 1.2 depicts an example of a $2^{\{e0,e1\}}$-labeled CMDP. The round-bordered smaller squared nodes represent choices, and the larger squared nodes with a number in the brackets represent the states, e.g., state node [1] represents s_1. The brackets in state nodes make it easier to distinguish them from choice nodes. The root choice of a state is depicted by a sole arc from the corresponding state node to a choice node. If the choice



target	label
θ_1	$e0$
θ_2	$e0$
θ_3	$e0, e1$
θ_4	
θ_5	$e0$

Figure 1.2: Example of labeled choice-aware Markov decision process

transition function returns a probabilistic distribution for a choice, the outgoing, white-headed arcs from the choice depict the distribution (with the probabilities as labels), e.g., the outgoing arcs from choice node 1 to choice nodes 2 and 3. Black-headed arcs without labels are used for nondeterministic choices, e.g., 2 to choice nodes 4 and 5. Black-headed arcs with targets as labels are used for target choices; the destination node of such an arc is the corresponding state node of the target's target state, e.g., choice node 4 to state node [1]. The labels of each target are given in the table. This labeled CMDP can be used to calculate the worst case and the best case probability that eventually a label like $e0$ is reached from a specific state. How this can be formally expressed and calculated is topic of the remainder of this subsection.

1.2.1 Paths and Probability Measure

Let $\mathcal{M} = (S, \Theta, \tau, \mathcal{C}, succ, C)$ be a CMDP with choice transition function $succ$.

$Paths^{\mathcal{M}}_{choice}$ $\varrho[i]$

A choice path $\varrho = c_0\, c_1 \ldots\, c_n \in \mathcal{C}^*$ of $\mathcal{M}$ is a choice path of $succ$. $Paths^{\mathcal{M}}_{choice}$ is the set of all choice paths of $\mathcal{M}$. Given a choice path $\varrho = c_0\, c_1 \ldots\, c_n$, let $\varrho[i] = c_i$ denote the i-th choice for all $0 \leq i \leq n$. Given a terminal choice path $\varrho = c_0\, c_1 \ldots\, c_n$, let $\tau(\varrho)$ be the choice path target of ϱ, i.e., $\tau(\varrho) = succ(c_n)$; this is properly defined, because in a terminal choice path $succ(c_n) \in \Theta$. Let $s \rightsquigarrow_{\mathcal{M}} \theta$ (read as 's leads to θ') be satisfied, if and only if there exists a terminal choice path ϱ with $C(s) = \varrho[0]$ and $\tau(\varrho) = \theta$.

π $\pi_{\text{⚓}}$ $|\pi_{\text{⚓}}|$

A finite path $\pi = \theta_1\, \theta_2 \ldots\, \theta_n \in \Theta^*$ of $\mathcal{M}$ is a sequence of targets where $\tau(\theta_i) \rightsquigarrow_{\mathcal{M}} \theta_{i+1}$ for all $1 \leq i < n$. The empty sequence $\varnothing$ is also a valid finite path. $FinPaths^{\mathcal{M}}$ is the set of all finite paths of $\mathcal{M}$. An anchored finite path $\pi_{\text{⚓}} = [s, \theta_1\, \theta_2 \ldots\, \theta_n] \in S \times FinPaths^{\mathcal{M}}$ of $\mathcal{M}$ is a pair of a state and a finite path where $s \rightsquigarrow_{\mathcal{M}} \theta_1$. Let $|\pi_{\text{⚓}}| = n$ be the path length of $\pi_{\text{⚓}} = [s, \theta_1\, \theta_2 \ldots\, \theta_n]$. $FinPaths^{\mathcal{M}}_{\text{⚓}}$ is the set of all anchored finite paths of $\mathcal{M}$. $first(\pi_{\text{⚓}}) = s$ be the anchor or the anchored finite path. $FinPaths^{\mathcal{M}}_{s} = (\{s\} \times FinPaths^{\mathcal{M}}) \cap FinPaths^{\mathcal{M}}_{\text{⚓}}$ is the set of all anchored finite paths starting from s. Let $\tau : FinPaths^{\mathcal{M}}_{\text{⚓}} \to S^{\mathcal{M}}$ be the last state of an anchored finite path $[s, \theta_1 \ldots \theta_n]$, i.e., $\tau([s, \varnothing]) = s$ and $\tau([s, \theta_1 \ldots \theta_n]) = \tau(\theta_n)$ otherwise. Given an anchored finite path $\pi_{\text{⚓}} = [s, \theta_1 \ldots \theta_n]$ and a target θ, let $\pi_{\text{⚓}}\theta = [s, \theta_1 \ldots \theta_n\, \theta]$ be the concatenation of the finite path with the target.

$\widehat{\pi}$ $\widehat{\pi}_{\text{⚓}}$

An infinite path $\widehat{\pi} = \theta_1\, \theta_2\, \theta_3 \ldots \in \Theta^\omega$ of $\mathcal{M}$ is a sequence of choice paths where $\tau(\theta_i) \rightsquigarrow_{\mathcal{M}} \theta_{i+1}$ for all $i \geq 1$. $InfPaths^{\mathcal{M}}$ is the set of all infinite paths of $\mathcal{M}$. An anchored infinite path $\widehat{\pi}_{\text{⚓}} = [s, \theta_1\, \theta_2\, \theta_3 \ldots] \in S \times InfPaths^{\mathcal{M}}$ of $\mathcal{M}$ is a pair of a state and an infinite path where $s \rightsquigarrow_{\mathcal{M}} \theta_1$. $InfPaths^{\mathcal{M}}_{\text{⚓}}$ is the set of all anchored infinite paths of $\mathcal{M}$.

$\mathit{InfPaths}_s^{\mathcal{M}} = (\{s\} \times \mathit{InfPaths}^{\mathcal{M}}) \cap \mathit{InfPaths}_{\lightning}^{\mathcal{M}}$ is the set of all anchored infinite paths starting from s. Let $\widehat{\pi}[..k] = \theta_1\,\theta_2 \ldots \theta_k$ denote the k-th prefix of $\widehat{\pi} = \theta_1\,\theta_2\,\theta_3 \ldots$ and let $\mathit{Pref}(\widehat{\pi}) = \{\pi' \mid \pi' \text{ is prefix of } \widehat{\pi}\}$ denote the set of all prefixes of $\widehat{\pi}$. Also, let $\mathit{Pref}([s, \widehat{\pi}]) = \{[s, \pi] \mid \pi \in \mathit{Pref}(\widehat{\pi})\}$ denote the set of all anchored prefixes of $[s, \widehat{\pi}]$. $\widehat{\pi}[..k]$

In the remainder, both finite and infinite paths are sometimes just called paths when it is clear from the context which one is meant.

A probability measure cannot be defined directly for a CMDP, because a nondeterministic choice is not a "probabilistic construct". With a so called scheduler, the nondeterminism in a CMDP can be resolved, which results in a GMC with a properly defined probability measure. GMCs that are the result of such schedulers provide a view onto the CMDP from the schedulers' perspective. By using different schedulers, a broader view onto the CMDP can be obtained. By consulting all schedulers, minimum and maximum probabilities can be derived. There are two kinds of schedulers in CMDPs: *choice scheduler*, which resolve the nondeterministic choices of choice paths, and *step scheduler*, which select the choice scheduler for each step between two states.

Definition 1.4 (Choice Scheduler of a Choice-aware Markov Decision Process)**.** Let $\mathcal{M} = (S, \Theta, \tau, \mathcal{C}, \mathit{succ}, C)$ be a CMDP. A *choice scheduler* for $\mathcal{M}$ is a partial function $\mathfrak{c} : \mathcal{C} \rightharpoonup \mathcal{C}$ such that for all $c \in \mathcal{C}$, $\mathit{succ}(c) \in 2^{\mathcal{C}}$ implies $\mathfrak{c}(c) \in \mathit{succ}(c)$.

Let $\mathfrak{C}(\mathcal{M})$ be the finite set of all possible choice schedulers for $\mathcal{M}$; let $\mathfrak{C}$ denote $\mathfrak{C}(\mathcal{M})$ if $\mathcal{M}$ is clear from the context. Note that the numbers of $\mathfrak{C}(\mathcal{M})$ is finite, because $\mathcal{C}$ is finite and there is only a limited number of combinations of possible successors for the nondeterministic choices. The choice path $\varrho = c_0\,c_1 \ldots c_n$ of $\mathcal{M}$ is a $\mathfrak{c}$-path if and only if the choice scheduler $\mathfrak{c}$ agrees with all its nondeterministic choices, i.e., if and only if for all $0 \leq i < n$, $\mathit{succ}(c_i) \in 2^{\mathcal{C}}$ implies $\mathfrak{c}(c_i) = c_{i+1}$. $\mathfrak{C}$

Definition 1.5 (Markov Chain of a Choice Scheduler)**.** Let $\mathcal{M} = (S, \Theta, \tau, \mathcal{C}, \mathit{succ}, C)$ be a CMDP with choice transition function succ, and $\mathfrak{c}$ a *choice scheduler* for $\mathcal{M}$. The standard Markov Chain $\mathcal{M}^{\mathfrak{c}}$ induced by $\mathfrak{c}$ is given by $\mathcal{M}^{\mathfrak{c}} = (\mathcal{C} \cup \Theta, R)$ where

- $R(c)(\mathit{succ}(c)) = 1$ if $\mathit{succ}(c) \in \Theta$, and
- $R(c) = \mathit{succ}(c)$ if $\mathit{succ}(c) \in \mathit{Dists}(\mathcal{C})$, and
- $R(c)(c') = 1$ if $\mathit{succ}(c) \in 2^{\mathcal{C}}$ and $\mathfrak{c}(c) = c'$, and
- $R(\theta)(\theta) = 1$, and
- $R(\cdot)(\cdot) = 0$ otherwise.

For state s and choice scheduler $\mathfrak{c}$, let $\mu_s^{\mathfrak{c}}$ be the choice distribution with $\mu_s^{\mathfrak{c}}(\theta) = \mathit{Pr}_{C(s)}^{\mathcal{M}^{\mathfrak{c}}}(\mathbf{F}\,\theta)$.

Definition 1.6 (Step Scheduler of a Choice-aware Markov Decision Process)**.** Let $\mathcal{M} = (S, \Theta, \tau, \mathcal{C}, \mathit{succ}, C)$ be a CMDP. A *step scheduler* for $\mathcal{M}$ is a function $\mathfrak{s} : \mathit{FinPaths}_{\lightning}^{\mathcal{M}} \to (\mathcal{C} \rightharpoonup \mathcal{C})$ such that for all anchored finite paths $\pi_{\lightning} \in \mathit{FinPaths}_{\lightning}^{\mathcal{M}}$, $\mathfrak{s}(\pi_{\lightning})$ is a choice scheduler for $\mathcal{M}$.

Let $\mathfrak{S}(\mathcal{M})$ be the countable set of all possible step schedulers for $\mathcal{M}$; let $\mathfrak{S}$ denote $\mathfrak{S}(\mathcal{M})$ if $\mathcal{M}$ is clear from the context. Let $s \rightsquigarrow_{\mathfrak{c}} \theta$ (read as 'by adhering to $\mathfrak{c}$, s leads to $\mathfrak{S}$

θ') be satisfied, if and only if there exists a terminal choice path ϱ with $C^{\mathcal{M}}(s) = \varrho[0]$ and $\tau(\varrho) = \theta$ and for all $1 \leq i < n$, $succ(c_i) \in 2^{\mathcal{C}}$ implies $\mathfrak{c}(c_i) = c_{i+1}$.

The finite anchored path $[s, \theta_1\, \theta_2 \ldots\, \theta_n]$ of $\mathcal{M}$ is a finite $\mathfrak{s}$-path if the scheduler $\mathfrak{s}$ agrees with all its nondeterministic choices, i.e., iff $s \rightsquigarrow_{\mathfrak{c}_0} \theta_1$ with $\mathfrak{c}_0 = \mathfrak{s}([s, \varnothing])$, and for all $1 \leq i < n$, $\tau(\theta_i) \rightsquigarrow_{\mathfrak{c}_i} \theta_{i+1}$ with $\mathfrak{c}_i = \mathfrak{s}([s, \theta_1\, \theta_2 \ldots\, \theta_i])$. Let $FinPaths_{\mathfrak{t}}^{\mathcal{M},\mathfrak{s}}$ denote the set of all finite $\mathfrak{s}$-paths of $\mathcal{M}$, and $FinPaths_s^{\mathcal{M},\mathfrak{s}} = FinPaths_s^{\mathcal{M}} \cap FinPaths_{\mathfrak{t}}^{\mathcal{M},\mathfrak{s}}$ denote the set of all finite $\mathfrak{s}$-paths of $\mathcal{M}$ starting from s.

Analogously, the anchored infinite path $\widehat{\pi}_{\mathfrak{t}} = [s, \theta_1\, \theta_2\, \theta_3 \ldots]$ of $\mathcal{M}$ is a $\mathfrak{s}$-path if the scheduler $\mathfrak{s}$ agrees with all its nondeterministic choices, i.e., iff $s \rightsquigarrow_{\mathfrak{c}_0} \theta_0$ with $\mathfrak{c}_0 = \mathfrak{s}([s, \varnothing])$, and for all $1 \leq i$, $\tau(\theta_i) \rightsquigarrow_{\mathfrak{c}_i} \theta_{i+1}$ with $\mathfrak{c}_i = \mathfrak{s}([s, \theta_1\, \theta_2 \ldots\, \theta_i])$. Let $InfPaths_{\mathfrak{t}}^{\mathcal{M},\mathfrak{s}}$ denote the set of all infinite $\mathfrak{s}$-paths of $\mathcal{M}$, and $InfPaths_s^{\mathcal{M},\mathfrak{s}} = InfPaths_s^{\mathcal{M}} \cap InfPaths_{\mathfrak{t}}^{\mathcal{M},\mathfrak{s}}$ denote the set of all infinite $\mathfrak{s}$-paths of $\mathcal{M}$ starting from s.

Definition 1.7 (Markov Chain of a Step Scheduler)**.** Let $\mathcal{M} = (S, \Theta, \tau, \mathcal{C}, succ, C)$ be a CMDP and $\mathfrak{s}$ a *step scheduler* for $\mathcal{M}$. The standard Markov Chain $\mathcal{M}^{\mathfrak{s}}$ induced by $\mathfrak{s}$ is given by $(FinPaths_{\mathfrak{t}}^{\mathcal{M},\mathfrak{s}}, R^{\mathfrak{s}})$ with the *transition distribution* function $R^{\mathfrak{s}} : FinPaths_{\mathfrak{t}}^{\mathcal{M},\mathfrak{s}} \to Dists(FinPaths_{\mathfrak{t}}^{\mathcal{M},\mathfrak{s}})$ where $R^{\mathfrak{s}}(\pi_{\mathfrak{t}}) = \mu$ and $\mathfrak{c} = \mathfrak{s}(\pi_{\mathfrak{t}})$ such that $\mu(\pi_{\mathfrak{t}}\theta_{n+1}) = \mu^{\mathfrak{c}}_{\tau(\pi_{\mathfrak{t}})}(\theta_{n+1})$.

Each finite $\mathfrak{s}$-path $[s, \theta_1\, \theta_2 \ldots\, \theta_n] \in FinPaths_{\mathfrak{t}}^{\mathcal{M},\mathfrak{s}}$ of $\mathcal{M}$ has a corresponding anchored finite path $[[s, \varnothing], [s, \theta_1]\, [s, \theta_1\, \theta_2] \ldots\, [s, \theta_1\, \theta_2 \ldots\, \theta_n]] \in FinPaths_{\mathfrak{t}}^{\mathcal{M}^{\mathfrak{s}}}$ in the MC $\mathcal{M}^{\mathfrak{s}}$, and vice versa. Analogously, each infinite $\mathfrak{s}$-path $\widehat{\pi}_{\mathfrak{t}} \in FinPaths_{\mathfrak{t}}^{\mathcal{M},\mathfrak{s}}$ of the CMDP $\mathcal{M}$ has a corresponding anchored infinite path $\widehat{\pi}^{\bar{c}}_{\mathfrak{t}}$ in the generic Markov chain $\mathcal{M}^{\mathfrak{s}}$, and the other way around.

This correspondence makes it possible to use the probability measure $Pr_s^{\mathcal{M}^{\mathfrak{s}}}$ induced by MC $\mathcal{M}^{\mathfrak{s}}$ to define the probability space of the choice-aware Markov decision process $\mathcal{M}$ with its associated step scheduler $\mathfrak{s}$.

$\pi_{\mathfrak{t}}{\uparrow}^{\mathcal{M},\mathfrak{s}}$

The *cylinder set* $\pi_{\mathfrak{t}}{\uparrow}^{\mathcal{M},\mathfrak{s}}$ of the anchored finite path $\pi_{\mathfrak{t}}$ contains all anchored paths of $\mathcal{M}$ that start with $\pi_{\mathfrak{t}}$ and adhere to $\mathfrak{s}$. More formally, $\pi_{\mathfrak{t}}{\uparrow}^{\mathcal{M},\mathfrak{s}} = \{\widehat{\pi}'_{\mathfrak{t}} \in InfPaths_{\mathfrak{t}}^{\mathcal{M},\mathfrak{s}} \mid \pi_{\mathfrak{t}} \in Pref(\widehat{\pi}'_{\mathfrak{t}})\}$. Let $\Pi \subseteq FinPaths_s^{\mathcal{M},\mathfrak{s}}$, then $\Pi{\uparrow}^{\mathcal{M},\mathfrak{s}} = \bigcup_{\pi_{\mathfrak{t}} \in \Pi} \pi_{\mathfrak{t}}{\uparrow}^{\mathcal{M},\mathfrak{s}}$.

Definition 1.8 (Probability Space of a Choice-aware Markov Decision Process induced by a Step Scheduler starting in a certain state)**.** The probability space $(\Omega_s^{\mathcal{M},\mathfrak{s}}, \mathfrak{E}_s^{\mathcal{M},\mathfrak{s}}, Pr_s^{\mathcal{M},\mathfrak{s}})$ of a Choice-aware Markov Decision Process $\mathcal{M}$ induced by a Step Scheduler $\mathfrak{s}$ starting in state $s \in S^{\mathcal{M}}$ consists of

- the sample space $\Omega_s^{\mathcal{M},\mathfrak{s}} = InfPaths_s^{\mathcal{M},\mathfrak{s}}$, and
- the events $\mathfrak{E}_s^{\mathcal{M},\mathfrak{s}}$ as the smallest σ-algebra on $\Omega_s^{\mathcal{M},\mathfrak{s}}$ that contains $\{\pi_{\mathfrak{t}}{\uparrow}^{\mathcal{M},\mathfrak{s}} \mid \pi_{\mathfrak{t}} \in FinPaths_s^{\mathcal{M},\mathfrak{s}}\}$, and
- the probability measure $Pr_s^{\mathcal{M},\mathfrak{s}}$ with $Pr_s^{\mathcal{M},\mathfrak{s}}(\pi_{\mathfrak{t}}{\uparrow}^{\mathcal{M},\mathfrak{s}}) = Pr^{\mathcal{M}^{\mathfrak{s}}}_{[s,\varnothing]}(\pi^c_{\mathfrak{t}}{\uparrow}^{\mathcal{M}^{\mathfrak{s}}})$ where $\pi^c_{\mathfrak{t}}$ is the corresponding path of $\pi_{\mathfrak{t}}$.

Note that the probability measure cannot generally be used on the union of paths of different step schedulers, even if the paths all start in the same state. Thus, given an arbitrary $\Pi \subseteq FinPaths_{\mathfrak{t}}^{\mathcal{M}}$, the probability of that paths cannot be calculated. But the

$\Pi{\restriction}^{\mathfrak{s}}_s$

probability of the $\mathfrak{s}$-paths in Π that start from state s can be calculated. Therefore, the *restriction* to those paths is defined as $\Pi{\restriction}^{\mathfrak{s}}_s = \Pi \cap FinPaths_s^{\mathcal{M},\mathfrak{s}}$.

Bibliography

[Bai98] C. Baier. "On the Algorithmic Verification of Probabilistic Systems." Habilitation. Universität Mannheim, 1998.

[BK08] C. Baier and J.-P. Katoen. *Principles of Model Checking*. Cambridge, MA: MIT Press, 2008. ISBN: 978-0-262-02649-9.

[Leu18] J. Leupolz. "Probabilistic Safety Analysis of Executable Models." Dissertation. University of Augsburg, 2018.

[LK+17] J. Leupolz, A. Knapp, A. Habermaier, and W. Reif. "Qualitative and Quantitative Analysis of Safety-Critical Systems with S#." In: *International Journal on Software Tools for Technology Transfer*. Springer, 2017.