Mixed Nondeterministic-Probabilistic Interfaces

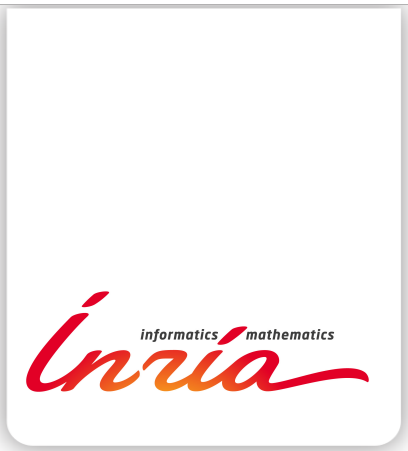
Albert Benveniste, Kim G Larsen, Jean-Baptiste Raclet

Mixed Nondeterministic-Probabilistic Interfaces

Albert Benveniste, Kim G. Larsen, Jean-Baptiste Raclet

RESEARCH REPORT
N° 9372
November 2020
Project-Team Hycomes

ISSN 0249-6399 ISRN INRIA/RR--9372--FR+ENG



Mixed Nondeterministic-Probabilistic Interfaces*

Albert Benveniste†, Kim G. Larsen‡, Jean-Baptiste Raclet§

Project-Team Hycomes

Research Report n° 9372 — November 2020 — 40 pages

Abstract: Interface theories are powerful frameworks supporting incremental and compositional design of systems through refinements and constructs for conjunction, and parallel composition. In this report we present a first Interface Theory—Modal Mixed Interfaces—for systems exhibiting both non-determinism and randomness in their behaviour. The associated component model—Mixed Markov Decision Processes—is also novel and subsumes both ordinary Markov Decision Processes and Probabilistic Automata.

Key-words: Interface theories, Probabilistic interfaces, Probabilistic systems, Nondeterministic systems

* This paper was prepared in 2019 while the second author was supported by an Inria International Chair.

† INRIA/IRISA, Rennes, France. Albert.Benveniste@inria.fr

‡ Department of Computer Science, Aalborg University, Aalborg, Denmark

§ IRIT, Université de Toulouse, Toulouse, France

RESEARCH CENTRE
RENNES – BRETAGNE ATLANTIQUE

Campus universitaire de Beaulieu
35042 Rennes Cedex

Interfaces Mixtes Probabilistes-Nondéterministes

Résumé : Les théories d'interfaces sont des formalismes de spécification. Elles permettent une spécification incrémentale grâce à une algèbre riche d'opérateurs tels que le raffinement, la conjonction et la composition parallèle. Dans ce rapport, on propose une théorie d'interfaces, les Interfaces Modales Mixtes, qui permettent de spécifier des systèmes combinant étroitement des aspects probabilistes et non-déterministes. Les Interfaces Modales Mixtes sont construites au-dessus du modèle de composant des Automates Mixtes, qui étend à la fois les Processus de Décision Markoviens et les Automates Probabilistes.

Mots-clés : Théories d'interfaces, interfaces probabilistes, systèmes probabilistes, systèmes non-déterministes

Contents

1 Introduction

Contract or Interface Theories are powerful frameworks for the incremental and compositional design of systems. Their essence is to handle *components* (for capturing actual designs) and *contracts* or *interfaces* (for capturing specifications). At their heart sits the notion of satisfaction, stating that a design suitably implements a specification. To achieve this, frameworks of components must be equipped with a parallel composition, and interface theories need a richer algebra to support the incremental and compositional design of systems, namely: refinement, conjunction, and parallel composition [3, 5]. Different styles of frameworks for interfaces include de Alfaro-Henzinger *Interface Automata* [10] Larsen et al. *Modal Automata* [1] and their variants, and trace based *Assume/Guarantee contracts* [4].

There are several cases where the underlying class of systems involves a mix of nondeterminism and randomness. Faults and their possible propagation through a system are naturally modelled probabilistically, whereas lack of knowledge of scheduling principles or incomplete information must be modelled through by nondeterminism. Since faults may be affected by scheduling policies, frameworks supporting the joint handling of nondeterminism and randomness are needed. In this paper we thus ask the following natural questions:

- *Question 1.* Can we develop a framework for components able to blend probabilistic and nondeterministic behaviors in a compositional way?
- *Question 2.* Can we develop a theory of interfaces blending probabilistic and nondeterministic aspects to serve as specifications of the former?

Regarding Question 1 about components, Markov Decision Processes (MDP) [20] provide a natural framework for capturing randomness. Runs of an MDP proceed as follows: from a state q some action α can be selected, which brings the system into a probabilistic state π (a probability), from which the next state q' is drawn at random. MDP compose by synchronizing over common actions, whereas probabilistic state-choice is made independently. As a first contribution of this paper we propose a non-deterministic extension of MDP called *Mixed Markov Decision Processes* (MMDP). Runs of MMDP proceed as follows: from a state q some action α can be selected, which brings the system into a *mixed* state S (a system blending nondeterminism and probability, albeit with no dynamics, as illustrated in Figure 1-left), from which

the next state q' is drawn in a mixed nondeterministic/probabilistic way. MMDP compose by synchronizing on their common actions: from (q_1, q_2), performing action α brings the composed MMDP to mixed state $S_1 \times S_2$, from which the next state (q'_1, q'_2) is drawn. One major issue is here the definition of mixed systems and their composition (see Figure 1-mid and right, latter explained in Section 2). Our proposed MMDP component model subsumes that of Probabilistic Automata [19].

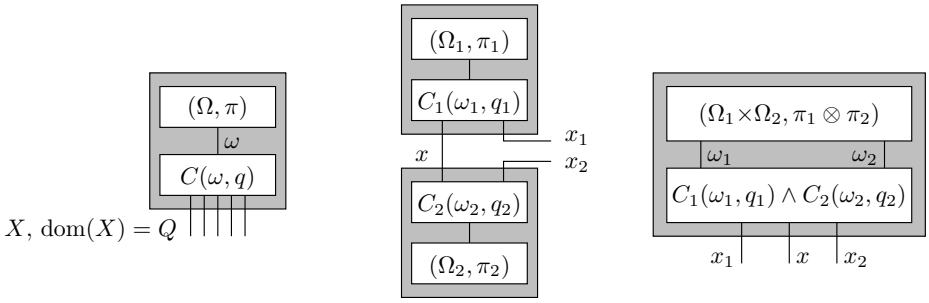


Figure 1: Left: a mixed system; a probability space (Ω, π) produces the private random outcome ω subject to the constraint $C(w, q)$, where q is the visible value taken by a tuple of variables X. Mid: parallel composition of two mixed systems, the intuition: the two systems interact through their shared variables (here x). Right: the actual formal result as another mixed system.

Regarding Question 2 about interfaces, there exist few attempts in this direction, but no complete answer that we are aware of. Caillaud et al. [7, 8] propose the framework of Constrained Markov Chains (CMC) as an extension of Interval Markov Chains [15]. By imposing constraints on transition probabilities, CMCs are a specification theory for discrete time Markov Chains: refinement relations are proposed, as well as constructs for conjunction and parallel composition. The framework is made effective by restricting constraints on transition probabilities to be polynomial. *Abstract Probabilistic Automata* (APA) [11, 12, 13] is a proposal for an interface theory for Probabilistic Automata. APA borrows from the CMC model the idea of setting polynomial constraints on the transition probabilities attached to the probabilistic states, and offer the same algebra as CMC does.

The second and major contribution of this paper is the novel framework of Modal Mixed Interfaces (or Mixed Interfaces for short), which is an interface theory for MMDP. Our approach consists in lifting, to MMDP, the construction of Modal Interfaces [21] on top of automata. Mixed Interfaces offer the usual algebra of interface theories, namely: satisfaction

(also named implementation), refinement, conjunction, and parallel composition. We show that Mixed Interfaces extend CMC regarding satisfaction and refinement, while offering a much cleaner notion of parallel composition.

The paper is organized as follows. In Section 2 we develop the model of Mixed Systems sketched in Figure 1, on top of which MMDP are built in Section 3 to serve as model of component. In Section 4 we show how to embed in MMDP Segala's Probabilistic Automata with nondeterministic transition relations. Section 5 introduces Mixed Modal Interfaces as a specification framework for MMDP and we show in Section 6 how to embed in it the specification framework of Constraint Markov Chains. All proofs are deferred to appendices.

2 Mixed Probabilistic Nondeterministic systems

For (Ω, π) a finite or countable probability space, π is entirely determined by its associated *weighting function* $w(\omega) =_{\text{def}} \pi(\{\omega\})$. By abuse of notation, we denote by $\pi(\omega)$ the weighting function associated to π. Also, for a subset $W \subseteq \Omega$ such that $\pi(W) > 0$, we define the *conditional probability* $\pi(. \mid W)$ by the formula $\pi(V|W) =_{\text{def}} \frac{\pi(V \cap W)}{\pi(W)}$, which is well defined since $\pi(W)>0$. The *support* of π, denoted by $\mathbf{supp}(\pi)$, is the set of all ω such that $\pi(\omega) > 0$. Throughout this paper and unless otherwise specified we consider only finite or countable probability spaces.[1]

We are now ready to define Mixed Probabilistic Nondeterministic systems and give their semantics. This was illustrated in Figure 1.

Definition 1 *A* Mixed Nondeterministic Probabilistic system *or* Mixed System *for short is a tuple:* $S = ((\Omega, \pi), X, C)$*, where* (Ω, π) *is a probability space;* X *is a finite set of variables having finite or countable domain* $Q = \prod_{x \in X} Q_x$ *; and* $C \subseteq \Omega \times Q$ *is a relation.*

A system S *is called* inconsistent *if* $\pi(\exists q.C) = 0$*, otherwise it is said consistent. If* S *is consistent, its* operational semantics *consists in:*

1. *drawing* $\omega \in \Omega$ *at random according to* $\pi(. \mid \exists q.C)$*, and*
2. *nondeterministically selecting* $q \in Q$ *such that* $\omega \, C \, q$*.*

This two-step procedure is denoted by $S \rightsquigarrow q$ *and, for* $\mathcal{S}$ *a set of mixed systems, we write* $\mathcal{S} \rightsquigarrow q$ *if* $S \rightsquigarrow q$ *holds for some* $S \in \mathcal{S}$*.*

[1] The restriction that Ω is at most countable is technically important in the above material. For the general case, we must abandon conditional probabilities and use the notion of *conditional expectation,* which is defined in full generality. Conditional distributions require additional topological assumptions for their definition, and so does the notion of *support.*

In the sequel and unless otherwise specified, we only consider consistent systems.

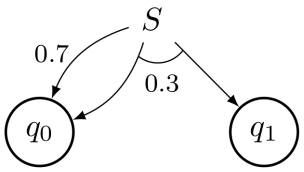


Figure 2: Example 1: a mixed system

Example 1 The following mixed system S is depicted in Figure 2:

- $\Omega = \{\omega_1, \omega_2\}$ with $\pi(\omega_1) = 0.7$ and $\pi(\omega_2) = 0.3$;
- $X = \{x\}$ over $Q_x = \{0, 1\}$. Call q_i for $i \in Q_x$ the state for which $x = i$;
- $C = \{(\omega_1, q_0), (\omega_2, q_0), (\omega_2, q_1)\}$.

Intuitively, S may evolve to q_0 with probability 0.7. It may also nondeterministically evolve to q_0 or q_1 with probability 0.3. □

Example 2 In a mixed system, the randoms are hidden that is, only their effect on the visible system variables is of interest. Now suppose that $\Omega = \Omega_1 \times \Omega_2$ and the constraint C has the form $C(\omega_1, q)$. In this case, Ω_2 is not needed and can be removed, e.g., by replacing (Ω, π) by its marginal (Ω_1, π_1), where $\pi_1(\omega_1) = \sum_{\omega_2} \pi(\omega_1, \omega_2)$. □

This was just a simple case and we now discuss the operation of compression, on top of which a notion of equivalence between systems can be defined. This material is borrowed from [6].

Definition 2 (compression) *For $S = ((\Omega, \pi), X, C)$ a Mixed System, we define the following equivalence relation on Ω:*

$$\omega \sim \omega' \quad \text{iff} \quad \forall q : (\omega, q) \in C \Leftrightarrow (\omega', q) \in C \tag{1}$$

The compression *of S, denoted by $[S] = (([\Omega], [\pi]), X, [C])$, is defined as follows: $[\Omega] = \Omega/\sim$ (its elements are written $[\omega]$), $[C]([\omega], \cdot) = C(\omega, \cdot)$ for $\omega \in [\omega]$ and $[\pi]([\omega]) = \sum_{\omega \in [\omega]} \pi(\omega)$. Say that S is* compressed *if it coincides with its compression.*

Distinguishing ω and ω' is impossible if $\omega \sim \omega'$. Compressing Ω is thus natural. We say that two systems are equivalent if their compressed forms are isomorphic.

Definition 3 (equivalence) *Two compressed mixed system S and S' are called* equivalent*, written $S \equiv S'$, if they possess identical sets of variables $X = X'$ and isomorphic operational semantics, i.e., if, when setting $C_\pi = \{(\omega, q) \in C \mid \pi(\omega) > 0\}$, there exists a bijective map: $\varphi : C_\pi \mapsto C'_{\pi'}$, such that, for every $(\omega, q) \in C_\pi$, we have $\pi(\omega) = \pi'(\omega')$ and $q = q'$, where $(\omega', q') =_{\text{def}} \varphi(\omega, q)$. Say that arbitrary systems S and S' are* equivalent *if their compressions are equivalent.*

Mixed Systems are equipped with a parallel composition by intersection in which probabilistic choices remain local and independent, conditionally to the satisfaction of synchronization constraints.

Definition 4 (parallel composition) *For $S_i, i = 1, 2$ two mixed systems, we define their* parallel composition $S = S_1 \times S_2$ *as the following Mixed System:*

$$\begin{array}{rcl} X & = & X_1 \cup X_2 \ , \ \Omega = \Omega_1 \times \Omega_2 \ , \text{and} \ \ \pi = \pi_1 \otimes \pi_2 \\ C & = & \{(\omega, q) \ \mid \omega_1 \, C_1 \, \mathbf{Pr}_1(q) \wedge \omega_2 \, C_2 \, \mathbf{Pr}_2(q) \, \} \end{array}$$

where $\mathbf{Pr}_i(q)$ denotes the projection of the state q over the variables X_i.

The definition of C expresses that the two systems must agree on their shared variables $X_1 \cap X_2$. For the next definition, $\mathbf{Pr}_{12}(.)$ denotes the projection over the shared variables $X_1 \cap X_2$. We write $q_1 \bowtie q_2$ and say that q_1 and q_2 are *compatible* if $\mathbf{Pr}_{12}(q_1) = \mathbf{Pr}_{12}(q_2)$. If $q_1 \bowtie q_2$, we define the *join* $q_1 \sqcup q_2$ as the unique q projecting over q_1 and q_2. Using this notation, C in Definition 4 rewrites

$$C = \{(\omega, q_1 \sqcup q_2) \mid q_1 \bowtie q_2 \ \wedge \ \omega_1 C_1 q_1 \ \wedge \ \omega_2 C_2 q_2\} \tag{2}$$

Observe that the composition of two consistent systems may be inconsistent.

Lemma 1 *For mixed systems, equivalence is a congruence, i.e., $S_i \equiv S'_i$ for $i = 1, 2$ implies $S_1 \times S_2 \equiv S'_1 \times S'_2$.*

Proof See Appendix A.1. □

Let $\mathcal{S}(X)$ denote the collection of all mixed systems having X as set of variables.

Definition 5 (lifting relations) *Relation* $\rho^{\mathcal{S}} \subseteq \mathcal{S}(X_1) \times \mathcal{S}(X_2)$ *is called the* lifting *of relation* $\rho \subseteq Q_1 \times Q_2$ *if there exists a* weighting function $w : \Omega_1 \times \Omega_2 \to [0,1]$ *such that:*

1. *For every triple* $(\omega_1, \omega_2; q_1)$ *such that* $w(\omega_1, \omega_2) > 0$ *and* $\omega_1 \, C_1 \, q_1$*, there exists* q_2 *such that* $\omega_2 \, C_2 \, q_2$*, and* $q_1 \, \rho \, q_2$*;*
2. $\sum_{\omega_2} w(\omega_1, \omega_2) = \pi_1(\omega_1)$ *and* $\sum_{\omega_1} w(\omega_1, \omega_2) = \pi_2(\omega_2)$.

Note the existential quantifier in Condition 1. By Condition 2, w induces a probability on $\Omega_1 \times \Omega_2$. We write $S_1 \, \rho^{\mathcal{S}} \, S_2$ to mean $(S_1, S_2) \in \rho^{\mathcal{S}}$.

Example 3 Consider the mixed systems S_1 and S_2 depicted in Figure 3. We can lift the relation ρ such that $\rho = \{(q_{10}, q_{20}), (q_{11}, q_{20}), (q_{11}, q_{21})\}$ and see that $S_1 \, \rho^{\mathcal{S}} \, S_2$ by considering the weighting function shown in red. However, the relation ρ' such that $\rho' = \{(q_{10}, q_{20}), (q_{11}, q_{21})\}$ cannot be lift as a witness w does not exist. □

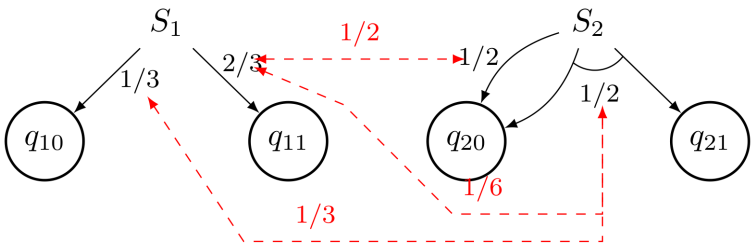


Figure 3: Example 3: lifted relation

Lemma 2 *$S_1 \, \rho^{\mathcal{S}} \, S_2$ and $S_1' \equiv S_1$ together imply $S_1' \, \rho^{\mathcal{S}} \, S_2$.*

Proof See Appendix A.2. □

Lemma 2 expresses that mixed system equivalence is also a congruence with respect to the lifting of relations.

Definition 6 *Given $\rho \subseteq Q_1 \times Q_2$ and $\mathcal{S}_i \subseteq \mathcal{S}(Q_i)$ for $i = 1, 2$, define*

$$\mathcal{S}_1 \subseteq^{\rho} \mathcal{S}_2 \text{ iff } \forall S_1 \in \mathcal{S}_1, \exists S_2 \in \mathcal{S}_2 : S_1 \, \rho^{\mathcal{S}} \, S_2 \,,$$

and define $\mathcal{S}_1 \supseteq^{\rho} \mathcal{S}_2$ as being $\mathcal{S}_2 \subseteq^{\widetilde{\rho}} \mathcal{S}_1$, where $\widetilde{\rho}$ denotes the transpose of ρ. Write $S \in^{\rho} \mathcal{S}$ to mean $\{S\} \subseteq^{\rho} \mathcal{S}$ and $\mathcal{S} \ni^{\rho} S$ to mean $\mathcal{S} \supseteq^{\rho} \{S\}$.

For Q_1, Q_2, and Q_3 three finite or countable sets, and $\rho_{12} \subseteq Q_1 \times Q_2$ and $\rho_{23} \subseteq Q_2 \times Q_3$ two relations, define:

$$\rho_{12} \bullet \rho_{23} \quad =_{\text{def}} \quad \mathbf{Pr}_{Q_1 \times Q_3}(\rho_{12} \wedge \rho_{23}) \tag{3}$$

that is, $\rho_{12} \bullet \rho_{23} \subseteq Q_1 \times Q_3$ and $q_1 (\rho_{12} \bullet \rho_{23}) q_3$ iff $q_1 \, \rho_{12} \, q_2$ and $q_2 \, \rho_{23} \, q_3$ for some $q_2 \in Q_2$.

Lemma 3 *We have* $(\rho_{12} \bullet \rho_{23})^{\mathcal{S}} = \rho_{12}^{\mathcal{S}} \bullet \rho_{23}^{\mathcal{S}}$ *and* $\subseteq^{\rho_{12} \bullet \rho_{23}} = \subseteq^{\rho_{12}} \bullet \subseteq^{\rho_{23}}$.

Proof See Appendix A.3.

The set algebra of mixed systems. We have introduced in Definition 3 the notion of equivalence $\equiv$ for mixed systems. Lemmas 1 and 2 show that this equivalence is a congruence with respect to both mixed systems composition and the lifting of relations from state spaces to mixed systems. We now define the set algebra induced by this equivalence. For $\mathcal{S}$ and $\mathcal{S}'$ two sets of mixed systems:

$$\begin{array}{rcl} \mathcal{S} \subseteq \mathcal{S}' & \text{iff} & \forall S \in \mathcal{S}, \exists S' \in \mathcal{S}' : S' \equiv S \\ \mathcal{S} = \mathcal{S}' & \text{iff} & \mathcal{S} \subseteq \mathcal{S}' \text{ and } \mathcal{S}' \subseteq \mathcal{S} \\ \mathcal{S}_1 \cap \mathcal{S}_2 & = & \bigcup \{\mathcal{S} \mid \mathcal{S} \subseteq \mathcal{S}_1 \text{ and } \mathcal{S} \subseteq \mathcal{S}_2\} \end{array} \tag{4}$$

Thanks to this redefinition, we shall freely use the usual set theoretic notations for sets of mixed systems.

3 Mixed Markov Decision Processes

Probabilistic automata have been introduced in [23] for the study of randomization in concurrency theory. They are labeled transitions systems where transitions are from states not to a single target state but to a target state determined by a probability measure. *Markov Decision Processes* [2, 14] exist in mathematics for quite some time. They correspond to *deterministic* probabilistic automata in the following sense: from each state, each action identifies a unique probability measure. In this paper we consider extensions of MDP in which the target of a transition is a mixed probabilistic/nondeterministic system as defined in Section 2:

Definition 7 (mmdp) *A* Mixed Markov Decision Process *(*MMDP*) is a tuple* $M = (\Sigma, X, r_0, \rightarrow)$*, where:*

- Σ *is a finite alphabet of* actions*;*

- *X is a finite set of variables having finite or countable domain $R = \prod_{x \in X} R_x$, and $r_0 \in R$ is the* initial *state;*
- *$\rightarrow \subseteq R \times \Sigma \times \mathcal{S}(X)$ is the* transition relation*; we write $r \xrightarrow{\alpha} S$ (or $r \xrightarrow{\alpha}_M S$) to mean $(r, \alpha, S) \in \rightarrow$, and $r \xrightarrow{\alpha}$ if $r \xrightarrow{\alpha} S$.*

Let $\mathcal{S}(X)$ be the set of all mixed systems S over X, possibly inconsistent. We require that M shall be deterministic*: for any pair $(r, \alpha) \in R \times \Sigma$, $r \xrightarrow{\alpha} S$ and $r \xrightarrow{\alpha} S'$ implies $S = S'$. M is said to be* live *if all its transitions target consistent systems.*

A *run* σ of M is a finite or infinite sequence of states $r_0, r_1, r_2, \ldots$ starting from initial state r_0 and then progressing by a sequence of steps of the form $r_k \xrightarrow{\alpha} S \Rightarrow r_{k+1}$, where $S \rightsquigarrow r'$ is the operational semantics of system S following Definition 1.

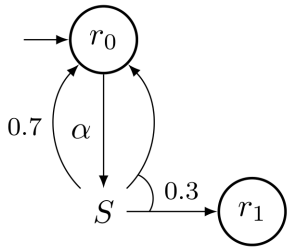


Figure 4: Example of an MMDP (S is the mixed system of Figure 2)

Example 4 An MMDP is depicted in Figure 4 with $\Sigma = \{\alpha\}$; it has only one transition (r_0, α, S) where S is the mixed system of Figure 2. □

Definition 8 (simulation) *Given two* MMDP *M_1 and M_2 over Σ, M_2* simulates *M_1, written $M_1 \leq M_2$, if there exists a relation $\leq \subseteq R_1 \times R_2$ such that:*

- *$r_{0,1} \leq r_{0,2}$ and,*
- *for $r_1 \leq r_2$ and for each transition $r_1 \xrightarrow{\alpha}_{M_1} S_1$, there exists a transition $r_2 \xrightarrow{\alpha}_{M_2} S_2$ such that $S_1 \leq^{\mathcal{S}} S_2$.*

M_1 and M_2 are called simulation equivalent *if they simulate each other.*

The composition of two MMDP having identical alphabets is introduced next. A transition labeled α is available in the product if and only if the components are ready to do simultaneously a transition labeled α.

Definition 9 (composition) *For M_1 and M_2 two* MMDP *having identical alphabet Σ and compatible initial states $r_{0,1} \bowtie r_{0,2}$, their* composition $M_1 \times M_2$ *has alphabet Σ, set of variables $X_1 \cup X_2$, and initial state $r_{0,1} \sqcup r_{0,2}$. Its transition relation is the minimal relation satisfying:*

$$r_i \xrightarrow{\alpha}_{M_i} S_i \text{ for } i = 1,2 \text{ and } r_1 \bowtie r_2 \implies r_1 \sqcup r_2 \xrightarrow{\alpha}_{M} S_1 \times S_2$$

where $S_1 \times S_2$ has been defined in Definition 4.

Parallel composition preserves simulation:

Lemma 4 *Let $M_i, i = 1,2$ be two* MMDP *and let $M_i' \leq M_i, i = 1,2$. Then, we have $M_1' \times M_2' \leq M_1 \times M_2$.*

Proof See Appendix B.1. □

4 Link to Probabilistic Automata

Probabilistic Automata (PA) [19] are a nondeterministic extension of MDPs. We show here that MMDP can capture this nondeterminism by making use of the nondeterminism involved in mixed systems. We discuss here the version of PA with no consideration of internal actions.

Definition 10 *A Probabilistic Automaton* PA *is a tuple $P = (\Sigma, Q, q_0, \rightarrow)$, where Σ is the finite alphabet of actions, Q is a finite state space, $q_0 \in Q$ is the initial state, and $\rightarrow \subseteq Q \times \Sigma \times \mathcal{P}(Q)$ is a probabilistic transition relation where $\mathcal{P}(Q)$ is the set of all probability distributions over Q.*

The operational semantics of P is as follows: if P is in state $q \in Q$, performing $\alpha \in \Sigma$ leads to some target set of probability distributions over Q, of which one is selected, nondeterministically, and then used to draw the next state q'. We can reinterpret this operational semantics as follows: performing $\alpha \in \Sigma$ while being in state $q \in Q$ leads to the same target set of probability distributions over Q, that we use differently. We form the direct product of all distributions belonging to the target set and we perform one trial according to this distribution, i.e., we perform independent random trials for all probabilities belonging to the target set. This yields a tuple of candidate values for the next state, of which we select one, nondeterministically.

Clearly, these two operational semantics produce identical outcomes. Now, the latter is the operational semantics of the MMDP $M_P = (\Sigma, \xi, q_0, \rightarrow_P)$, defined as follows: Σ is as before, ξ is the system variable with domain Q, q_0

is as before, and $\rightarrow_P$ is the transition relation defined as follows: $\rightarrow_P$ maps a pair $(q, \alpha) \in Q \times \Sigma$ to the mixed system $S = ((\Omega, \Pi), \xi, C)$ defined as follows. Let n be the cardinality of the set $\{\pi \mid (q, \alpha, \pi) \in \rightarrow\}$. Take for Ω the product of n copies of Q, so that ω is an n-tuple of states: $\omega = (q_1, \ldots, q_n)$. Take for Π the product of all probabilities belonging to set $\{\pi \mid (q, \alpha, \pi) \in \rightarrow\}$. Finally, $(\omega, q) \in C$ if and only if $q \in \{q_1, \ldots, q_n\}$. The following theorem holds, for which the definitions of simulation and composition of PA are available in [19]:

Theorem 1 *Let P_1, P_2 be two* PA *and M_{P_1}, M_{P_2} be the corresponding* MMDP. *The mapping $P \rightarrow M_P$ preserves both simulation and product: $P_1 \leq P_2$ if and only if $M_{P_1} \leq M_{P_2}$, and $M_{P_1 \times P_2}$ and $M_{P_1} \times M_{P_2}$ are simulation equivalent.*

A reverse mapping also exists. The PA associated to the MMDP of Fig. 4 is easily guessed: performing α leads to the family of two probability spaces over R: (R, π_1) where $\pi_1(r_0) = 1$ and (R, π_2) where $\pi_2(r_0) = 0.7$ and $\pi_2(r_1) = 0.3$. Theorem 1 holds for this inverse mapping as well. So, what is the point in preferring MMDP? The rich algebra developed in Section 2 (with the two key notions of compression and lifting) is essential in supporting a flexible notion of parallel composition. In particular, when extending PA with labeling using sets of atomic propositions (AP), it is required, for the parallel composition to be defined, that the two sets are disjoint. Our MMDP offer the expressive power of AP-labeling without setting any restriction on the parallel composition. See Section 6 for a detailed study of the same issue, for Constraint Markov Chains.

5 Modal Mixed Interfaces

In this section we develop the first part of our agenda, namely a framework of *Modal Mixed Interfaces* (or *Mixed Interfaces* for short) which allow to specify sets of MMDP called the *models* of the interface. Note that in this section sets of probabilities associated to Mixed Interfaces are manipulated by not paying attention to effectiveness. Mixed Interfaces extend to a mixed probabilistic-nondeterministic setting the formalism of Modal Specifications [18, 16, 1]. In this paper we develop our framework for the case of a fixed alphabet Σ of actions. Following [21], alphabet extension techniques allow to handle the general case.

Definition and Semantics. For X a finite set of variables, $\mathcal{S}(X)$ denotes the class of all mixed systems S over X and we call *mixed state* a subset

$\mathcal{S} \subseteq \mathcal{S}(X)$.

Definition 11 *A* Mixed Interface *is defined as a tuple* $\mathcal{C} = (\Sigma, X, q_0, \rightarrow, \dashrightarrow)$, *where:*

- Σ *is the finite alphabet of actions;*
- X *is a finite set of variables having finite domain* $Q =_{\text{def}} \prod_{x \in X} Q_x$*:*
- q_0 *is the* initial state *(we do* not *require that* $q_0 \in Q$*);*
- $\rightarrow, \dashrightarrow \subseteq Q \times \Sigma \times 2^{\mathcal{S}(X)}$ *are the* must *and* may *transition relations.*

We require that $\mathcal{C}$ *is* deterministic *in the following sense: for any pair* $(q, \alpha) \in Q \times \Sigma$, $(q, \alpha, \mathcal{S}) \in \rightarrow$ *and* $(q, \alpha, \mathcal{S}') \in \rightarrow$ *imply* $\mathcal{S} = \mathcal{S}'$, *and similarly for* $\dashrightarrow$.

We write $q \xrightarrow{\alpha} \mathcal{S}$ to mean $(q, \alpha, \mathcal{S}) \in \rightarrow$; $q \overset{\alpha}{\dashrightarrow} \mathcal{S}$ is defined similarly. We write $q \overset{\alpha}{\not\rightarrow}$ if there exists no mixed state $\mathcal{S}$ such that $q \xrightarrow{\alpha} \mathcal{S}$; $q \overset{\alpha}{\not\dashrightarrow}$ is defined similarly. Finally, we write $\mathcal{S} \Rightarrow q'$ to mean that $S \Rightarrow q'$ holds for some $S \in \mathcal{S}$. Note that $q_0 \notin Q$ will typically arise when the subset Q of states is empty; it will be useful to model *unsatisfiable* interfaces. Whenever convenient, we shall write $\mathcal{S}^{\Box}$ and $\mathcal{S}^{\Diamond}$ when referring to mixed states targeted by *must* and *may* transitions, respectively.

Example 5 The following Mixed Interface is depicted in Figure 5-right:

- $\Sigma = \{\alpha\}$;
- $X = \{x\}$ over $Q_x = \{0, 1\}$ with $x = 0$ in $q_{0,1}$ and $x = 1$ in $q_{0,1}$;
- $q_{0,2} \overset{\alpha}{\dashrightarrow} \{S_1, S_2\}$ with S_1 and S_2 two mixed systems.

Note that in the Mixed Interface of Figure 5-left, we have $q_{0,1} \overset{\alpha}{\dashrightarrow} \{S\}$ and $q_{0,1} \xrightarrow{\alpha} \{S\}$ but only the plain arrow corresponding to the must transition is depicted in order to lighten the figure. □

The intuitive semantics is the following: a *must* transition labeled by α must be available in any model with an associated system S selected from $\mathcal{S}^{\Box}$ and then a next state q' is selected according to the operational semantics of S. The same holds for a *may* transition except that in this case, the occurrence of the action is allowed but not required and the selected system belongs to $\mathcal{S}^{\Diamond}$.

We now formally define the notion of *model* of a Mixed Interface over Σ in terms of MMDP over the same alphabet; we make use of Definition 1 for the notion of *consistent system*, Definition 6 for the meaning of $\in^{\models}$ and Definition 7 for *live* MMDP:

Definition 12 (satisfaction) *For* $\mathcal{C}$ *a Mixed Interface such that* $q_0 \in Q$ *and* M *a live* MMDP, *a relation* $\models \subseteq R \times Q$ *is a* satisfaction relation *iff,*

for any (r, q) *such that* $r \models q$*, the following holds:*

$$\left.\begin{array}{l}\text{only } \textit{may} \text{ transitions}\\ \text{of } \mathcal{C} \text{ are allowed for } M\end{array}\right\} \forall \alpha : r \xrightarrow{\alpha}_M S_M \Rightarrow \left[q \overset{\alpha}{\dashrightarrow}_{\mathcal{C}} \mathcal{S}^{\Diamond} \text{ and } S_M \in^{\models} \mathcal{S}^{\Diamond}\right] \quad (5)$$

$$\left.\begin{array}{l}\textit{must} \text{ transitions of } \mathcal{C}\\ \text{are mandatory for } M\end{array}\right\} \forall \alpha : q \xrightarrow{\alpha}_{\mathcal{C}} \mathcal{S}^{\Box} \Rightarrow \left[r \xrightarrow{\alpha}_M S_M \text{ and } S_M \in^{\models} \mathcal{S}^{\Box}\right] \quad (6)$$

M is a model of $\mathcal{C}$, written $M \models \mathcal{C}$, if $r_0 \models q_0$. A Mixed Interface $\mathcal{C}$ such that $q_0 \notin Q$ does not admit any model.

The set of models of a Mixed Interface is closed under the simulation equivalence of Definition 8. Observe moreover that the condition (6) makes only sense because we consider deterministic interfaces, since the system S_M reached by performing action α is unique in this case.

Note that, by definition, $r \models q$ induces constraints on the set of systems associated to the *must* and *may* transitions stemming from q. More precisely, for any α and $\mathcal{S}^{\Diamond}$ and $\mathcal{S}^{\Box}$ as in (5) and (6), the intersection $\mathcal{S}^{\Box} \cap \mathcal{S}^{\Diamond}$ necessarily contains at least one consistent system. In this statement and in the sequel, we stress that the set algebra over sets of Mixed Systems is the one defined in (4).

Definition 13 *A state q is called* inconsistent *if $q \xrightarrow{\alpha}_{\mathcal{C}} \mathcal{S}^{\Box}$, and either $q \overset{\alpha}{\not\dashrightarrow}_{\mathcal{C}}$, or $q \overset{\alpha}{\dashrightarrow}_{\mathcal{C}} \mathcal{S}^{\Diamond}$ but the intersection $\mathcal{S}^{\Box} \cap \mathcal{S}^{\Diamond}$ contains no consistent system.*

The subset of consistent systems of $\mathcal{S}^{\Box} \cap \mathcal{S}^{\Diamond}$ entirely specifies the set of models of the considered Mixed Interface. This leads to the operation of pruning that we introduce next. The *pruning* of $\mathcal{C}$, written $[\mathcal{C}]$, is obtained as follows:

1. Let $\mathcal{C}'$ the Mixed Interface obtained from $\mathcal{C}$ by thinning $\mathcal{S}^{\Box}$ down to the intersection $\mathcal{S}^{\Box} \cap \mathcal{S}^{\Diamond}$;
2. Apply repeatedly the following transformation until fixed point, with initial value $k = 0$ and $\mathcal{C}_0 = \mathcal{C}'$:
   (a) Let $Q_{k,\text{incon}}$ be the set of states q of $\mathcal{C}_k$ such that all inconsistent states of the state space Q_k and set $Q_{k+1} = Q_k - Q_{k,\text{incon}}$; by construction, replacing Q_k by Q_{k+1} does not modify the set of models of $\mathcal{C}$;
   (b) Performing this step may create new inconsistent states, however; and, thus, we set $k \leftarrow k + 1$ and return to step 2a.

Let $[\mathcal{C}]$ be the Mixed Interface obtained at fixed point.

Lemma 5 *By construction, $[\mathcal{C}]$ and $\mathcal{C}$ possess identical sets of models.*

Proof See Appendix D.1. □

Note that by considering that Mixed Interfaces have finite sets of states, the pruning procedure is terminating. A Mixed Interface $\mathcal{C}$ is called *inconsistent* iff it has no model, i.e. iff the initial state q_0 does not belong to the set of states of $[\mathcal{C}]$. Unless otherwise specified, we assume in the sequel that:

$$\begin{array}{c}\text{Pruning has been applied to every}\\ \text{considered Mixed Interface: } [\mathcal{C}] = \mathcal{C}.\end{array} \tag{7}$$

Refinement. We now consider refinement which aims at comparing interfaces at different stages of their design. Intuitively, it allows to check if an interface is a more detailed version of an initial one. More precisely, refining an interface amounts to exclude some potential models from its set of models.

Definition 14 (modal refinement) *Let $\mathcal{C}_i, i = 1, 2$ be two Mixed Interfaces over Σ, a relation $\preceq \subseteq Q_1 \times Q_2$ is a* modal refinement *iff, for all (q_1, q_2) such that $q_1 \preceq q_2$ and for every $\alpha \in \Sigma$:*

$$\begin{array}{rcl} q_1 \overset{\alpha}{\dashrightarrow}_1 \mathcal{S}_1^{\diamond} & \Rightarrow & q_2 \overset{\alpha}{\dashrightarrow}_2 \mathcal{S}_2^{\diamond} \text{ and } \mathcal{S}_1^{\diamond} \subseteq^{\preceq} \mathcal{S}_2^{\diamond} \\ q_2 \overset{\alpha}{\longrightarrow}_2 \mathcal{S}_2^{\square} & \Rightarrow & q_1 \overset{\alpha}{\longrightarrow}_1 \mathcal{S}_1^{\square} \text{ and } \mathcal{S}_1^{\square} \subseteq^{\preceq} \mathcal{S}_2^{\square} \end{array} \tag{8}$$

Say that $\mathcal{C}_1$ is a modal refinement *of $\mathcal{C}_2$, written $\mathcal{C}_1 \preceq \mathcal{C}_2$, if for $q_{0,1} \in Q_1$ and $q_{0,2} \in Q_2$, we have $q_{0,1} \preceq q_{0,2}$.*

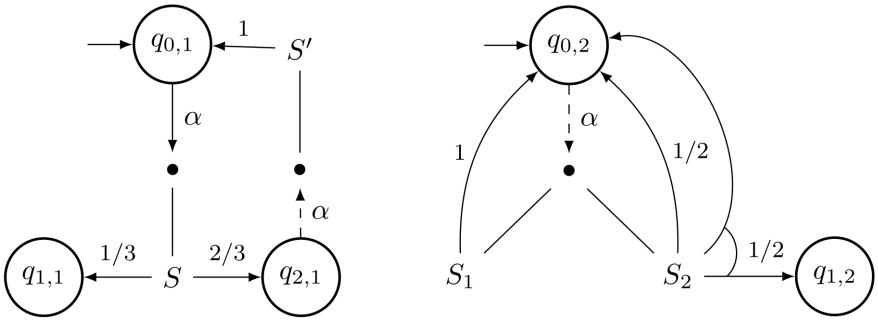


Figure 5: Example of refinement, see Examples 5 and 6.

Example 6 Figure 5 shows an example of refinement. The Mixed Interface on the left is a refinement of the one on the right. Observe in particular that the Mixed Interface on the left still encompasses probabilistic aspects but no longer has nondeterministic select for the next state. This is allowed by the lifting operation on mixed systems as already seen in Example 3. □

Lemma 6 *The modal refinement on Mixed Interfaces is a preorder.*

Proof See Appendix D.2. □

Theorem 2 *For $\mathcal{C}_i, i = 1, 2$ two Mixed Interfaces, if $\mathcal{C}_1 \preceq \mathcal{C}_2$ then every model of $\mathcal{C}_1$ is also a model of $\mathcal{C}_2$.*

Proof See Appendix D.3. □

Despite Mixed Interfaces are taken deterministic in Definition 11, modal refinement is correct but not fully abstract as for Modal Automata [17]: the following counterexample shows that Theorem 2 cannot be strengthened to an if-and-only-if statement. The reason for this is the nondeterminism that sits in the mixed systems themselves.

Counterexample 1 Consider the two "purely non-probabilistic" Mixed Interfaces over $\Sigma = \{a\}$ depicted in Figure 6. They are purely non-probabilistic as any associated random follows a Dirac probability. $\mathcal{C}_1$ has only models that can perform at most two consecutive α-actions. Any such implementation is also an implementation of $\mathcal{C}_2$. However, it is not true that $\mathcal{C}_1 \preceq \mathcal{C}_2$ in the sense of modal refinement. □

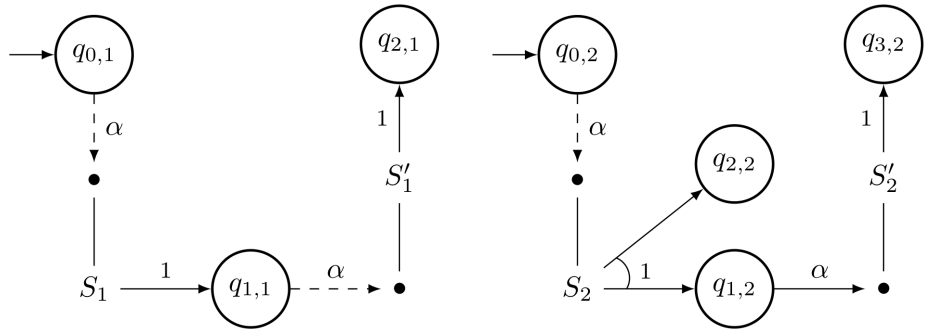


Figure 6: Counterexample 1 showing that modal refinement is not fully abstract

Conjunction. Consider $\mathcal{C}_i, i = 1, 2$ two Mixed Interfaces over Σ with respective sets of variables X_1 and X_2 and state spaces Q_1 and Q_2.

$$\mathcal{S}_1 \times \mathcal{S}_2 \quad = \quad \{S_1 \times S_2 \mid S_i \in \mathcal{S}_i\} \tag{9}$$

where $S_1 \times S_2$ is defined in Definition 4.

We are now able to define the conjunction of two Mixed Interfaces.

Definition 15 (conjunction) *Let $\mathcal{C}_i, i = 1, 2$ be two Mixed Interfaces over Σ, their* pre-conjunction *$\mathcal{C}_1 \underline{\wedge} \mathcal{C}_2$ has alphabet Σ, set of variables $X_1 \cup X_2$, initial state $(q_{1,0}, q_{2,0})$, and its may and must transition relations are the minimal relations satisfying the following rules:*

$$\begin{array}{lcl}
\text{[ConjMay]} & : & q_1 \overset{\alpha}{-\!\!\rightarrow}_1 \mathcal{S}_1^{\diamond} \text{ and } q_2 \overset{\alpha}{-\!\!\rightarrow}_2 \mathcal{S}_2^{\diamond} \Rightarrow (q_1,q_2) \overset{\alpha}{-\!\!\rightarrow} \mathcal{S}_1^{\diamond} \times \mathcal{S}_2^{\diamond} \\
\text{[ConjMust0]} & : & q_1 \xrightarrow{\alpha}_1 \mathcal{S}_1^{\square} \text{ and } q_2 \xrightarrow{\alpha}_2 \mathcal{S}_2^{\square} \Rightarrow (q_1,q_2) \xrightarrow{\alpha} \mathcal{S}_1^{\square} \times \mathcal{S}_2^{\square} \\
\text{[ConjMust1]} & : & q_1 \xrightarrow{\alpha}_1 \mathcal{S}_1^{\square} \text{ and } q_2 \overset{\alpha}{\not\rightarrow}_2 \Rightarrow (q_1,q_2) \xrightarrow{\alpha} \mathcal{S}_1^{\square} \times \mathcal{S}(X_2) \\
\text{[ConjMust2]} & : & q_1 \overset{\alpha}{\not\rightarrow}_1 \text{ and } q_2 \xrightarrow{\alpha}_2 \mathcal{S}_2^{\square} \Rightarrow (q_1,q_2) \xrightarrow{\alpha} \mathcal{S}(X_1) \times \mathcal{S}_2^{\square}
\end{array}$$

Pruning for consistency the pre-conjunction $\mathcal{C}_1 \underline{\wedge} \mathcal{C}_2$ yields the conjunction *$\mathcal{C}_1 \wedge \mathcal{C}_2$.*

Inconsistency may result from the rules [ConjMust1] and [ConjMust2].

Theorem 3 *For any Mixed Interface $\mathcal{C}_1$ and $\mathcal{C}_2$, any model of $\mathcal{C}_1 \wedge \mathcal{C}_2$ is also a model of $\mathcal{C}_1$ and $\mathcal{C}_2$.*

Proof See Appendix D.4. □

Parallel composition. Quite often in the literature, an issue of *compatibility* arises along with the parallel composition of interfaces [10, 21]. As clarified in [21], the issue of compatibility is due to the different roles played by the component and its environment in dealing with inputs and outputs. As we do not distinguish inputs and outputs here, compatibility is not an issue for us.

Definition 16 (composition) *Let $\mathcal{C}_i, i = 1, 2$ be two Mixed Interfaces over Σ, their* composition *$\mathcal{C}_1 \otimes \mathcal{C}_2$ has alphabet Σ, set of variables $X_1 \cup X_2$, and initial state $(q_{1,0}, q_{2,0})$. Its transition relations are the minimal relations satisfying the following rules:*

$$\begin{array}{rcl}
q_1 \overset{\alpha}{-\!\!\rightarrow}_1 \mathcal{S}_1^{\diamond} \text{ and } q_2 \overset{\alpha}{-\!\!\rightarrow}_2 \mathcal{S}_2^{\diamond} & \Rightarrow & (q_1,q_2) \overset{\alpha}{-\!\!\rightarrow} \mathcal{S}_1^{\diamond} \times \mathcal{S}_2^{\diamond} \\
q_1 \xrightarrow{\alpha}_1 \mathcal{S}_1^{\square} \text{ and } q_2 \xrightarrow{\alpha}_2 \mathcal{S}_2^{\square} & \Rightarrow & (q_1,q_2) \xrightarrow{\alpha} \mathcal{S}_1^{\square} \times \mathcal{S}_2^{\square}
\end{array}$$

Parallel Composition does not raise any issue of consistency.

Theorem 4 *The parallel composition $\otimes$ satisfies the following properties:*

1. *$\otimes$ is commutative and associative.*
2. *For $\mathcal{C}_1$ and $\mathcal{C}_2$ two Mixed Interfaces, we have:*

$$\forall M_i, i = 1, 2 : M_i \models \mathcal{C}_i \Rightarrow M_1 \times M_2 \models \mathcal{C}_1 \otimes \mathcal{C}_2 \quad (10)$$

$$\mathcal{C}_1 \preceq \mathcal{C}_2 \Rightarrow \forall \mathcal{C} : \mathcal{C} \otimes \mathcal{C}_1 \preceq \mathcal{C} \otimes \mathcal{C}_2 \quad (11)$$

Proof See Appendix D.5. □

Last, let us mention that no quotient exists for Mixed Interfaces. This is inherently due to the nondeterminism involved in Mixed Systems. Probabilistic specification models already suffer from the same limitation.

6 Link to Constraint Markov Chains

Constraint Markov Chains have been proposed in [8] as a specification formalism with Markov Chains as models. Let us first recall their basic definitions.

Let A, B be sets of propositions with $A \subseteq B$. The restriction of $W \subseteq B$ to A is given by $W_{\downarrow A} = W \cap A$. If $T \subseteq 2^B$, then $T_{\downarrow A} = \{W_{\downarrow A} \mid W \in T\}$. Let $\mathcal{P}(Q)$ denote the set of all probabilities over the set Q. For R and Q two at most denumerable state spaces, a *transition probability* Δ, from R to Q, is a map $\Delta : R{\times}Q \to [0,1]$ such that, for every $r \in R$, $\Delta(r,.)$ is a probability over Q. If π_R is a probability distribution over R, then $\pi_R\Delta$ denotes the probability distribution over Q defined by:

$$\pi_R\Delta(q) \quad = \quad \sum_{r\in R} \pi_R(r)\Delta(r,q)\,. \tag{12}$$

A *transition sub-probability* Δ from R to Q is a map $\Delta : R{\times}Q \to [0,1]$ such that, for every $(r,q) \in R{\times}Q$, $\Delta(r,q) \geq 0$ and, for every $r \in R$, $\sum_{q\in Q} \Delta(r,q) \leq 1$.

Definition 17 *A* Markov Chain (MC) *is a tuple* $\mathbf{P} = (R, r_0, \Pi, A, v)$*, where* R *is a set of states containing the initial state* r_0*,* A *is a set of atomic propositions,* $v : R \to 2^A$ *is a state valuation, and* $\Pi : R{\times}R{\to}[0,1]$ *is a transition probability.*

Definition 18 *A* Constraint Markov Chain (CMC) *is a tuple*

$$\mathbf{S} = (Q, q_0, \varphi, A, V)\,,$$

where Q *is a set of states containing the initial state* q_0*,* A *is a set of atomic propositions,* $V : Q{\to}2^{2^A}$ *is a set of admissible state valuations, and* $\varphi : Q{\to}2^{\mathcal{P}(Q)}$ *is a* constraint function*, mapping states to sets of probability distributions over states.*

In practice, constraint functions will be only partially specified, in that a function mapping Q to $[0,1]^Q$ will be implicitly complemented by the additional constraints to make the target being a probability. This consideration

is only practical and does not need to be taken into account for our subsequent development. Whenever needed to avoid confusion, we will denote by $A_{\mathbf{P}}$ and $v_{\mathbf{P}}$, and $A_{\mathbf{S}}$ and $V_{\mathbf{S}}$, the elements A and V of MC $\mathbf{P}$ and CMC $\mathbf{S}$.

Definition 19 (satisfaction) *Let* $\mathbf{P}$ *and* $\mathbf{S}$ *be respectively an* MC *and a* CMC *such that* $A_{\mathbf{S}} \subseteq A_{\mathbf{P}}$. *A* satisfaction relation *between* $\mathbf{P}$ *and* $\mathbf{S}$ *is a relation* $\rho \subseteq R \times Q$ *such that, whenever* $r\ \rho\ q$*:*

1. $v_{\mathbf{P}}(r)_{\downarrow A_{\mathbf{S}}} \in V_{\mathbf{S}}(q)$*;*
2. *there exists a transition sub-probability* Δ*, from* R *to* Q*, such that:*
   (a) *for all* $r' \in R$ *such that* $\Pi(r, r') > 0$, $\Delta(r', q)$ *is a transition probability from* R *to* Q*, and;*
   (b) $\Pi(r, .)\Delta \in \varphi(q)$*, and;*
   (c) *if* $\Delta(r', q') \neq 0$*, then* $r' \rho\ q'$ *holds.*

$\mathbf{P}$ *satisfies* $\mathbf{S}$ *if and only if there exists a satisfaction relation between* $\mathbf{P}$ *and* $\mathbf{S}$ *that contains the two initial states.*

Definition 20 (weak refinement) *Let* $\mathbf{S}_1$ *and* $\mathbf{S}_2$ *be two* CMC *such that* $A_2 \subseteq A_1$*. The relation* $\rho \subseteq Q_1 \times Q_2$ *is a* weak refinement *iff, whenever* $q_1\ \rho\ q_2$*:*

1. $V_1(q_1)_{\downarrow A_2} \subseteq V_2(q_2)$*;*
2. *for any probability distribution* $\pi_1 \in \varphi_1(q_1)$*, there exists a transition sub-probability* Δ*, from* Q_1 *to* Q_2*, such that:*
   (a) *for all* q_1 *such that* $\pi_1(q_1) > 0$, $\Delta(q_1, .)$ *is a probability over* Q_2*;*
   (b) $\pi_1 \Delta \in \varphi_2(q_2)$*;*
   (c) *if* $\Delta(q_1', q_2') > 0$*, then* $q_1'\ \rho\ q_2'$ *holds.*

We say that $\mathbf{S}_1$ weakly refines $\mathbf{S}_2$*, written* $\mathbf{S}_1 \preceq \mathbf{S}_2$*, if* $q_{0,1}\ \rho\ q_{0.2}$*.*

We now show that Mixed Interfaces subsume CMC. First, we define the embedding of MC in MMDP. Given $\mathbf{P} = (R, r_0, \Pi, A, v)$ a Markov Chain, we associate the MMDP $M_{\mathbf{P}} = (\Sigma, X, r_0, \rightarrow)$, where:

- $\Sigma = \{\alpha\}$ (no need to mention the only action labeling transitions);
- $X = \{\xi, v\}$ collects a variable ξ with domain R, and the variable v;
- $r_0 \in R$ is the initial condition for ξ; no initial condition is given for v;
- the transition relation is $r \longrightarrow S$, where the mixed system $S = ((\Omega, \pi), X, C)$ is such that:

$$\Omega{=}R\ ;\ \pi{=}\Pi(r, .)\ \text{ and }\ C = \{(r, r, v(r)) \mid r{\in}R\} \subseteq \Omega{\times}(R{\times}2^A) \quad (13)$$

Lemma 7 *Let* $\mathbf{P}$ *be an* MC*. Then,* $\mathbf{P}$ *and* $M_{\mathbf{P}}$ *possess identical semantics.*

Proof See Appendix E.1. □

Consider now the embedding of CMC in Mixed Interfaces. For any CMC $\mathbf{S} = (Q, q_0, \varphi, A, V)$, we associate a Mixed Interface $\mathcal{C}_\mathbf{S} = (\Sigma, X, q_0, \rightarrow, \dashrightarrow)$, where:

- $\Sigma = \{\alpha\}$ (no need to mention the only action labeling transitions);
- $X = \{\xi, v\}$ collects a variable ξ with domain Q, and a variable v with domain 2^A;
- $q_0 \in Q$ is the initial condition for ξ; no initial condition is given for V;
- the *must* transition relation $\rightarrow$ is empty;
- the *may* transition relation is $q \dashrightarrow \mathcal{S}$, where $\mathcal{S}$ is the set of mixed systems of the form $S_v = ((\Omega, \pi), X, C_v)$, where $v(q)$ ranges over $V(q)$ and:

$$\Omega{=}Q \;;\; \pi{\in}\varphi(q) \;\text{ and }\; C_v = \{(q, q, v(q)) \mid q{\in}Q\} \;\subseteq\; \Omega{\times}(R{\times}2^A) \quad (14)$$

Whenever needed, we will use subscripts to relate items of $\mathbf{P}$ and $\mathbf{S}$ to their respective host entities.

Theorem 5 *Let* $\mathbf{S}$ *be a* CMC*. Then,* $\mathbf{S}$ *and* $\mathcal{C}_\mathbf{S}$ *possess identical semantics.*

The previous Theorem decomposes into the two following lemmas.

Lemma 8 *Let* $\mathbf{P}$ *and* $\mathbf{S}$ *be respectively an* MC *and a* CMC *such that* $A_\mathbf{S} \subseteq A_\mathbf{P}$*. Then,* $\mathbf{P}$ *satisfies* $\mathbf{S}$ *iff* $M_\mathbf{P}$ *is a model of* $\mathcal{C}_\mathbf{S}$*.*

Proof See Appendix E.2. □

Lemma 9 *Let* $\mathbf{S}_1$ *and* $\mathbf{S}_2$ *be two* CMC*s such that* $A_2 \subseteq A_1$*. Then,* $\mathbf{S}_1$ *weakly refines* $\mathbf{S}_2$ *iff* $\mathcal{C}_{\mathbf{S}_1}$ *refines* $\mathcal{C}_{\mathbf{S}_2}$*.*

Proof See Appendix E.3. □

7 Conclusion

We have proposed the first interface theory that allows to mix probabilities and nondeterminism. Our component model is that of Mixed Markov Decision Processes (MMDP) which subsume Probabilistic Automata. Our specification formalism is that of Mixed Interfaces. It offers a complete algebra for interfaces, namely: satisfaction, refinement, conjunction, and

parallel composition. No quotient exists for Mixed Interfaces. This is inherently due to the nondeterminism involved in Mixed Systems. We presented our framework for the case of a fixed alphabet of actions. Following [21], alphabet extension techniques allow to handle the general case, this will be reported in the extended version of this work.

Mixed Interfaces extend and clarify the satisfaction and refinement relations defined for Constraint Markov Chains. The same holds for Abstract Probabilistic Automata (APA) [11]. CMC and APA differ from Mixed Interfaces regarding the parallel composition, however. The parallel composition for Mixed Interfaces is general (system variables can be shared), whereas the one for CMC or APA requires that the specifications for composition have disjoint sets of atomic propositions. Also, a subclass of Mixed Interfaces can be defined that tightly emulates the networks of *Price Timed Automata* (PTA) equipped with their stochastic semantics [9]; a complete emulation, however, requires the consideration of some non-compositional priority policy for closed systems in this subclass. Due to lack of space, these additional results were not presented here.

This paper sets the theoretical foundations of formalisms that we plan to apply to safety and vulnerability analysis as ongoing works. To make it effective and amenable of tool development, one step further is needed, namely a finitary syntax for specifying and manipulating sets of Mixed Systems.

References

[1] Adam Antonik, Michael Huth, Kim G. Larsen, Ulrik Nyman, and Andrzej Wasowski. 20 years of modal and mixed specifications. *Bulletin of European Association of Theoretical Computer Science*, 1(94), 2008.

[2] Christel Baier and Marta Z. Kwiatkowska. Domain equations for probabilistic processes. *Mathematical Structures in Computer Science*, 10(6):665–717, 2000.

[3] Sebastian S. Bauer, Alexandre David, Rolf Hennicker, Kim Guldstrand Larsen, Axel Legay, Ulrik Nyman, and Andrzej Wasowski. Moving from specifications to contracts in component-based design. In *Proc. of the 15th International Conference on Fundamental Approaches to Software Engineering (FASE'12)*, volume 7212 of *Lecture Notes in Computer Science*, pages 43–58. Springer, 2012.

[4] Albert Benveniste, Benoît Caillaud, Alberto Ferrari, Leonardo Mangeruca, Roberto Passerone, and Christos Sofronis. Multiple view-

point contract-based specification and design. In *Proc. of the 6th International Symposium on Formal Methods for Components and Objects (FMCO'06)*, volume 5382 of *Lecture Notes in Computer Science*, pages 200–225. Springer, 2007.

[5] Albert Benveniste, Benoît Caillaud, Dejan Nickovic, Roberto Passerone, Jean-Baptiste Raclet, Philipp Reinkemeier, Alberto L. Sangiovanni-Vincentelli, Werner Damm, Thomas A. Henzinger, and Kim G. Larsen. Contracts for system design. *Foundations and Trends in Electronic Design Automation*, 12(2-3):124–400, 2018.

[6] Albert Benveniste, Bernard C. Levy, Eric Fabre, and Paul Le Guernic. A calculus of stochastic systems for the specification, simulation, and hidden state estimation of mixed stochastic/nonstochastic systems. *Theor. Comput. Sci.*, 152(2):171–217, 1995.

[7] Benoît Caillaud, Benoît Delahaye, Kim G. Larsen, Axel Legay, Mikkel L. Pedersen, and Andrzej Wasowski. Compositional design methodology with constraint markov chains. In *Proc. of the 7th International Conference on the Quantitative Evaluation of Systems (QEST'07)*, pages 123–132. IEEE Computer Society, 2010.

[8] Benoît Caillaud, Benoît Delahaye, Kim G. Larsen, Axel Legay, Mikkel L. Pedersen, and Andrzej Wasowski. Constraint markov chains. *Theor. Comput. Sci.*, 412(34):4373–4404, 2011.

[9] Alexandre David, Kim G. Larsen, Axel Legay, Marius Mikucionis, Danny Bøgsted Poulsen, Jonas van Vliet, and Zheng Wang. Stochastic semantics and statistical model checking for networks of priced timed automata. *CoRR*, abs/1106.3961, 2011.

[10] Luca de Alfaro and Thomas A. Henzinger. Interface theories for component-based design. In *Proc. of the 1st International Workshop on Embedded Software (EMSOFT'01)*, volume 2211 of *Lecture Notes in Computer Science*, pages 148–165. Springer, 2001.

[11] Benoît Delahaye, Joost-Pieter Katoen, Kim G. Larsen, Axel Legay, Mikkel L. Pedersen, Falak Sher, and Andrzej Wasowski. Abstract probabilistic automata. In *Proc. of the 12th International Conference on Verification, Model Checking, and Abstract Interpretation (VMCAI'11)*, volume 6538 of *Lecture Notes in Computer Science*, pages 324–339. Springer, 2011.

[12] Benoît Delahaye, Joost-Pieter Katoen, Kim G. Larsen, Axel Legay, Mikkel L. Pedersen, Falak Sher, and Andrzej Wasowski. New results on abstract probabilistic automata. In *Proc. of the 11th International Conference on Application of Concurrency to System Design (ACSD'11)*, pages 118–127. IEEE, 2011.

[13] Benoît Delahaye, Kim G. Larsen, Axel Legay, Mikkel L. Pedersen, and Andrzej Wasowski. Apac: A tool for reasoning about abstract probabilistic automata. In *Proc. of the 8th International Conference on Quantitative Evaluation of Systems (QEST'11)*, pages 151–152. IEEE Computer Society, 2011.

[14] Cyrus Derman. *Finite state Markovian decision processes*. Academic Press, 1970.

[15] Bengt Jonsson and Kim Guldstrand Larsen. Specification and refinement of probabilistic processes. In *Proc. of the 6th Annual Symposium on Logic in Computer Science (LICS'91)*, pages 266–277. IEEE Computer Society, 1991.

[16] Kim Guldstrand Larsen. Modal specifications. In *Automatic Verification Methods for Finite State Systems*, volume 407 of *Lecture Notes in Computer Science*, pages 232–246. Springer, 1989.

[17] Kim Guldstrand Larsen, Ulrik Nyman, and Andrzej Wasowski. On modal refinement and consistency. In *Proc. of the 18th Inter. Conf. on Concurrency Theory (CONCUR'07)*, pages 105–119. Springer, 2007.

[18] Kim Guldstrand Larsen and Bent Thomsen. A modal process logic. In *Proc. of the 3rd Annual Symposium on Logic in Computer Science (LICS'88)*, pages 203–210. IEEE, 1988.

[19] Nancy A. Lynch, Roberto Segala, and Frits W. Vaandrager. Compositionality for probabilistic automata. In *Proc. of the 14th International Conference on Concurreny Theory (CONCUR'03)*, volume 2761 of *Lecture Notes in Computer Science*, pages 204–222. Springer, 2003.

[20] M. L. Puterman. *Markov Decision Processes*. J. Wiley and Sons, 1994.

[21] Jean-Baptiste Raclet, Albert Benveniste, Benoît Caillaud, Axel Legay, and Roberto Passerone. A modal interface theory for component-based design. *Fundamenta Informaticae*, 107:1–32, 2011.

[22] Roberto Segala. Probability and nondeterminism in operational models of concurrency. In *Proc. of the 17th International Conference on Concurrency Theory (CONCUR'06)*, volume 4137 of *Lecture Notes in Computer Science*, pages 64–78. Springer, 2006.

[23] Roberto Segala and Nancy A. Lynch. Probabilistic simulations for probabilistic processes. In *Proc. of the 5th International Conference on Concurrency Theory (CONCUR'94)*, volume 836 of *Lecture Notes in Computer Science*, pages 481–496. Springer, 1994.

A Proofs regarding Mixed Systems

A.1 Proof of Lemma 1

Proof It is enough to prove the result for compressed systems. For $i = 1, 2$, let $S_i \equiv S'_i$ and let φ_i be the bijections defining the two equivalences. With reference to (2), we define

$$\varphi(\omega, q_1 \sqcup q_2) \quad = \quad \big((\omega'_1, \omega'_2), q'_1 \sqcup q'_2\big) \text{ where } (\omega'_i, q'_i) = \varphi_i(\omega_i, q_i), i = 1, 2$$

and we have to verify that φ defines the desired equivalence between $S =_{\text{def}} S_1 \times S_2$ and $S' =_{\text{def}} S'_1 \times S'_2$. Using the expression (2) for C and the fact that $\pi = \pi_1 \otimes \pi_2$, we get

$$\begin{array}{rl} C_\pi = & \{(\omega, q_1 \sqcup q_2) \mid q_1 \bowtie q_2 \ \wedge\ \omega_1 C_1 q_1 \ \wedge\ \pi_1(\omega_1) > 0 \ \wedge\ \omega_2 C_2 q_2 \ \wedge\ \pi_2(\omega_2) > 0\} \\ = & \{(\omega, q_1 \sqcup q_2) \mid q_1 \bowtie q_2 \ \wedge\ (\omega_1, q_1) \in C_{1\pi} \ \wedge\ (\omega_2, q_2) \in C_{2\pi}\} \end{array}$$

Thus, for every $(\omega, q_1 \sqcup q_2) \in C_\pi$, we have $q'_1 = q_1 \bowtie q_2 = q'_2$ and $(\omega'_i, q'_i) \in C_{i\pi}, i = 1, 2$, whence $(\omega', q') \in C'_\pi$ and φ is a bijection. Since $\pi' = \pi'_1 \otimes \pi'_2$ we get $\pi'(\omega') = \pi(\omega)$, which finishes the proof. □

A.2 Proof of Lemma 2

Proof The result is immediate if both S_1 and S'_1 are compressed, see Definition 2. It is thus sufficient to prove the lemma for the following two particular cases: S_1 compresses to S'_1, and the converse.

Consider first the case: S_1 compresses to S'_1. Let $w(\omega_1, \omega_2)$ be the weighting function associated to the lifting $S_1 \, \rho^{\mathcal{S}} \, S_2$, and let $\pi'_1(\omega'_1) = \sum_{\omega_1 \in \omega'_1} \pi_1(\omega_1)$ be the relation between π'_1 and π_1 in the compression of S_1 to S'_1. Then $w'(\omega'_1, \omega_2) = \sum_{\omega_1 \in \omega'_1} w(\omega_1, \omega_2)$ defines the weighting function associated to the lifting $S'_1 \, \rho^{\mathcal{S}} \, S_2$. The other properties required to deduce $S'_1 \, \rho^{\mathcal{S}} \, S_2$ are immediate to prove.

Now, consider the alternative case: S'_1 compresses to S_1, with relation

$$\pi_1(\omega_1) = \textstyle\sum_{\omega'_1 \in \omega_1} \pi'_1(\omega'_1) \tag{15}$$

between π'_1 and π_1, where $\omega'_1 \in \omega_1$ means that ω_1 is the equivalence class of ω'_1 with respect to relation $\sim$ defined in (1) when compressing S'_1. This case is more involved since the construction of the weighting function $w'(\omega'_1, \omega_2)$

is nontrivial. We need $w'(\omega'_1, \omega_2)$ to satisfy the following relations:

$$\begin{array}{rl} \forall \omega'_1 : & \pi'_1(\omega'_1) = \sum_{\omega_2} w'(\omega'_1, \omega_2) \\ \forall \omega_2 : & \pi_2(\omega_2) = \sum_{\omega'_1} w'(\omega'_1, \omega_2) \\ \forall (\omega'_1, \omega_2; q_1) : & \left[\begin{array}{c} w'(\omega'_1, \omega_2) > 0 \\ \omega'_1 \, C'_1 \, q_1 \end{array} \right] \Rightarrow \exists q_2 : \left[\begin{array}{c} \omega_2 \, C_2 \, q_2 \\ q_1 \, \rho \, q_2 \end{array} \right] \end{array} \tag{16}$$

Focus first on the first two lines of (16). We claim that to find a solution w' to the first two lines of (16), it is enough to find a solution to the following system of equations where the unknowns are the values $w'(\omega'_1, \omega_2)$:

$$\begin{array}{rrcl} \forall \omega_1, \omega_2 : & \sum_{\omega'_1 \in \omega_1} w'(\omega'_1, \omega_2) & = & w(\omega_1, \omega_2) \\ \forall \omega'_1 : & \sum_{\omega_2} w'(\omega'_1, \omega_2) & = & \pi'_1(\omega'_1) \end{array} \tag{17}$$

Observe that $\sum_{\omega'_1} w'(\omega'_1, \omega_2) = \sum_{\omega_1} \sum_{\omega'_1 \in \omega_1} w'(\omega'_1, \omega_2) = \sum_{\omega_1} w(\omega_1, \omega_2) = \pi_2(\omega_2)$ since $w(\omega_1, \omega_2)$ is the weighting function of the lifting $S_1 \, \rho^{\mathcal{S}} \, S_2$. Our claim is thus justified.

To solve (17), we observe that it splits into the following independent subsystems in which ω_1 is seen as a parameter ranging over Ω_1:

$$\begin{array}{rrcl} \forall \omega_2 : & \sum_{\omega'_1 \in \omega_1} w'(\omega'_1, \omega_2) & = & w(\omega_1, \omega_2) \\ \forall \omega'_1 \in \omega_1 : & \sum_{\omega_2} w'(\omega'_1, \omega_2) & = & \pi'_1(\omega'_1) \end{array} \tag{18}$$

The rows of System (18) are linked by the following relation: summing over all ω_2 the first set of equations yields $\sum_{\omega_2} \sum_{\omega'_1 \in \omega_1} w'(\omega'_1, \omega_2) = \sum_{\omega_2} w(\omega_1, \omega_2) = \pi_1(\omega_1)$, whereas summing over all $\omega'_1 \in \omega_1$ the second set of equations yields $\sum_{\omega'_1 \in \omega_1} \sum_{\omega_2} w'(\omega'_1, \omega_2) = \sum_{\omega'_1 \in \omega_1} \pi'_1(\omega'_1) = \pi_1(\omega_1)$, and the two resulting equations are identical, by Fubini theorem.

Let K_2 be the cardinal of Ω_2 and L_1 the cardinal of the set $\{\omega'_1 \mid \omega'_1 \in \omega_1\}$. We distinguish the three cases $L_1 = 1$, $K_2 = 1$, and $L_1, K_2 > 1$.

If $L_1 = 1$, setting $\forall \omega_2 : w'(\omega'_1, \omega_2) = w(\omega_1, \omega_2)$ yields a solution to (18) since the last equation of (18) is trivially satisfied.

Case $K_2 = 1$ is trivial either, since $w'(\omega'_1, \omega_2) = \pi'(\omega'_1)$ is the unique solution.

For the third case $L_1, K_2 > 1$, the system (18) has more unknowns ($K_2 \times L_1$) than equations ($K_2 + L_1$). To prove that it indeed has solutions, we reorganize the unknowns $w'(\omega'_1, \omega_2)$ into a row matrix by listing as a submatrix

the $w'(\omega'_1, \omega_2)$ for every fixed value of ω'_1 and ω_2 ranging over Ω_2:

$$\begin{array}{c}[w'(\omega'_{11}, \omega_{21}), \ldots, w'(\omega'_{11}, \omega_{2K_2}),\\ w'(\omega'_{12}, \omega_{21}), \ldots, w'(\omega'_{12}, \omega_{2K_2}),\\ \vdots\\ w'(\omega'_{1L_1}, \omega_{21}), \ldots, w'(\omega'_{1L_1}, \omega_{2K_2})]\end{array}$$

We arrange the equations as indicated in (18): we put on top the K_2 equations parameterized by ω_2 followed by the L_1 equations parameterized by ω'_1. For A and A' two matrices, of respective sizes $m{\times}n$ and $m'{\times}n'$, we denote by $A \otimes A'$ their *Kronecker product* obtained by replacing the a_{ij} entry of A by the matrix $a_{ij}.A'$, thus obtaining a matrix of size $(m{\times}m') \times (n{\times}n')$. With these conventions and notations, the matrix of the linear system (18) takes the following form, where $\mathbb{I}_m$ denotes the identity matrix of size $m{\times}m$:

$$M = \begin{bmatrix} [\overbrace{1 \ldots 1}^{L_1 \text{ times}}] \otimes \mathbb{I}_{K_2} \\ \\ \mathbb{I}_{L_1} \otimes [\underbrace{1 \ldots 1}_{K_2 \text{ times}}] \end{bmatrix}, \tag{19}$$

of size $(K_2{+}L_1) \times (K_2{\times}L_1)$. The proof that the first two lines of (16) are satisfied rests on the two lemmas 10 and 11 below.

We move to the third line of (16). The conditions $w'(\omega'_1, \omega_2) > 0$ and $\omega'_1\, C'_1\, q_1$ together imply $w(\omega_1, \omega_2) > 0$ and $\omega_1\, C_1\, q_1$ where ω_1 is the equivalence class of ω'_1, i.e., $\omega'_1 \in \omega_1$. The right hand side then follows since we have $S_1\, \rho^{\mathcal{S}}\, S_2$. This finishes the proof.

Lemma 10 *If $L_1, K_2 > 1$, then the matrix M defined in (19) has row rank equal to $L_1 + K_2 - 1$.*

Proof We proceed by double induction over L_1, K_2. The base case is $L_1{=}K_2{=}2$, for which matrix M is equal to

$$M = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$

M is singular but the submatrix obtained by erasing the first row and the last column in M (the latter are shown in green) is regular. This is proved by observing that this submatrix possesses only one traversal,[2] shown in

[2] A *traversal* of a $p{\times}p$-matrix B is a selection of p non-zero entries of B visiting all columns and rows of B.

red, hence its determinant equals ± 1 and cannot be zero.

In the rest of the proof, we use the convention that symbols written in boldface denote a matrix of suitable sizes filled with the indicated symbol. For example, $\mathbf{0}$ denotes a matrix filled with zeros, the sizes of which depend on the context.

For the induction argument, let $M(L_1, K_2)$ denote the matrix defined in (19) with the values L_1, K_2 and $\overline{M}(L_1, K_2)$ the square submatrix of $M(L_1, K_2)$ obtained by erasing the first row in $M(L_1, K_2)$ and then selecting columns accordingly. Using these notations, the invariant of the induction argument is the following:

$$\text{The number of traversals of } \overline{M}(L_1, K_2) \text{ equals } 1. \tag{20}$$

Increasing L_1 by 1: matrix $M(L_1, K_2)$ becomes

$$M(L_1{+}1, K_2) = \begin{bmatrix} M(L_1, K_2) & \begin{bmatrix} \mathbb{I}_{K_2} \\ \mathbf{0} \end{bmatrix} \\ \mathbf{0} & [\underbrace{1 \dots 1}_{K_2 \text{ times}}] \end{bmatrix} \tag{21}$$

where the added part is highlighted in red. We construct $\overline{M}(L_1{+}1, K_2)$ by adding, to $\overline{M}(L_1, K_2)$, one row below and one among the K_2 new columns shown on the right part of $M(L_1{+}1, K_2)$. For this case the number of traversals keeps constant.

Increasing K_2 by 1: matrix $M(L_1, K_2)$ becomes

$$M(L_1, K_2{+}1) = \begin{bmatrix} [\overbrace{1 \dots 1}^{L_1 \text{ times}}] \otimes \begin{bmatrix} \mathbb{I}_{K_2} & \mathbf{0} \\ \mathbf{0} & 1 \end{bmatrix} \\ \mathbb{I}_{L_1} \otimes [\underbrace{1 \dots 1}_{K_2 \text{ times}} \quad 1] \end{bmatrix}$$

where the additional entries are shown in red. We move the new row

$$[\overbrace{1 \dots 1}^{L_1 \text{ times}}] \otimes [\mathbf{0} \quad 1]$$

to the last line of the matrix. The new columns arising from

$$[\overbrace{1 \dots 1}^{L_1 \text{ times}}] \otimes \begin{bmatrix} \mathbf{0} \\ 1 \\ 1 \end{bmatrix}$$

are all shifted to the right to become the last ones of the matrix while keeping the same order. Having done this, we end up with a reorganized matrix that has the following form:

$$M(L_1, K_2{+}1) = \left[\begin{array}{cc} M(L_1, K_2) & [\ \star\ ] \\ \mathbf{0} & [\underbrace{1 \ldots 1}_{K_2 \text{ times}}] \end{array}\right]$$

where the added part is highlighted in red. Again the number of traversals remains constant.

In the following, for X a matrix, X^T denotes its transpose. Also, we take the convention that vectors identify with column matrices.

Lemma 11 *Let A be an $m{\times}n$ matrix with $m \leq n$ such that A has rank $m-1$, and there exists a non-zero m-vector v such that $v^T A = [0 \ldots 0]$. Then, for every m-vector y such that $v^T y = 0$, the linear system $Ax = y$ possesses a solution.*

Proof We complete v with $m{-}1$ vectors to get a basis of $\mathbb{R}^m$ and denote by C the $m{\times}m$-matrix obtained by taking this basis as its columns, v being the first one. Premultiplying the linear system $Ax = y$ by C^T yields $C^T Ax = C^T y$. Vector $C^T y$ has a 0 as its first entry, completed by an $m{-}1$-vector that we denote by z. Similarly, matrix $C^T A$ has its first row equal to zero, and we denote by B the matrix obtained by erasing the first row of $C^T A$. Our original linear system is then equivalent to the reduced linear system $Bx = z$. By assumption, B has rank $m{-}1$, i.e., full row rank, which ensures that a solution to $Bx = z$ exists (possibly not unique).

To prove that the first two lines of (16) are satisfied, we apply Lemma 10 to the matrix M defined in (19), and then Lemma 11 to the matrix M with

$$v^T = [\underbrace{1 \ \ldots \ 1}_{K_2 \text{ times}} \ \underbrace{-1 \ \ldots \ -1}_{L_1 \text{ times}}]$$

A.3 Proof of Lemma 3

Proof By definition, $S_1 \left(\rho_{12}^{\mathcal{S}} \bullet \rho_{23}^{\mathcal{S}} \right) S_3$ iff there exists $S_2 \in \mathcal{S}(Q_2)$ such that $S_1 \, \rho_{12}^{\mathcal{S}} \, S_2$ and $S_2 \, \rho_{23}^{\mathcal{S}} \, S_3$, that is, there exists two weighted functions w_{12} over $\Omega_1 \times \Omega_2$ and w_{23} over $\Omega_2 \times \Omega_3$, such that

- w_{12} projects to π_1 and π_2, and w_{23} projects to π_2 and π_3, and

- $w_{12}(\omega_1, \omega_2) > 0$ and $\omega_1\, C_1\, q_1$ together imply the existence of a q_2 such that $\omega_2\, C_2\, q_2$ and $q_1\, \rho_{21}\, q_2$;

  $w_{23}(\omega_2, \omega_3) > 0$ and $\omega_2\, C_2\, q_2$ together imply the existence of a q_3 such that $\omega_3\, C_3\, q_3$ and $q_2\, \rho_{23}\, q_3$.

On the other hand, $S_1\, (\rho_{12} \bullet \rho_{23})^{\mathcal{S}}\, S_3$ iff there exists a weighted function w over $\Omega_1 \times \Omega_3$ projecting to π_1 and π_3 and such that: $w(\omega_1, \omega_3) > 0$ and $\omega_1\, C_1\, q_1$ together imply the existence of a q_3 such that $\omega_3\, C_3\, q_3$ and $q_1\, (\rho_{12} \bullet \rho_{23})\, q_3$.

We thus construct the following function w defined over $\Omega_1 \times \Omega_3$:

$$w(\omega_1, \omega_3) = \sum_{\omega_2 \in \Omega_2} w_{12}(\omega_1, \omega_2).w_{23}(\omega_2, \omega_3) \tag{22}$$

To show that $S_1\, (\rho_{12} \bullet \rho_{23})^{\mathcal{S}}\, S_3$, we have to prove the following regarding w:

- if $w(\omega_1, \omega_3) > 0$ and $\omega_1\, C_1\, q_1$ hold, then we can find q_3 such that $\omega_3\, C_3\, q_3$ and $q_1\, (\rho_{12} \bullet \rho_{23})\, q_3$. To show this, note that if $w(\omega_1, \omega_3) > 0$ then, by (22), we can find an ω_2 such that $w_{12}(\omega_1, \omega_2).w_{23}(\omega_2, \omega_3) > 0$. Since $w_{12}(\omega_1, \omega_2) > 0$, there exists some q_2 such that $\omega_2 C_2 q_2$ and $q_1 \rho_{12} q_2$. Since $w_{23}(\omega_2, \omega_3) > 0$, there exists some q_3 such that $\omega_3 C_3 q_3$ and $q_2 \rho_{23} q_3$. Now, we have $q_1\ \rho_{12}\ q_2$ and $q_2\ \rho_{23}\ q_3$, which implies $q_1\ (\rho_{12} \bullet \rho_{23})\ q_3$;

- w projects to π_3:

$$\begin{aligned}
\sum_{\omega_1} w(\omega_1, \omega_3) &= \sum_{\omega_1} \sum_{\omega_2} w_{12}(\omega_1, \omega_2).w_{23}(\omega_2, \omega_3) \\
\text{by Fubini} \quad &= \sum_{\omega_2} \sum_{\omega_1} w_{12}(\omega_1, \omega_2).w_{23}(\omega_2, \omega_3) \\
&= \sum_{\omega_2} w_{23}(\omega_2, \omega_3) \underbrace{\sum_{\omega_1} w_{12}(\omega_1, \omega_2)}_{=1} \\
&= \pi_3(\omega_3)
\end{aligned}$$

- w projects to π_1: this is proved similarly.

Therefore, $S_1\, \left(\rho_{12}^{\mathcal{S}} \bullet \rho_{23}^{\mathcal{S}}\right)\, S_3$ iff $S_1\, (\rho_{12} \bullet \rho_{23})^{\mathcal{S}}\, S_3$.

B Proofs regarding MMDPs

B.1 Proof of Lemma 4

Proof Set $M' =_{\text{def}} M'_1 \times M'_2$ and $M =_{\text{def}} M_1 \times M_2$. Define the relation $\leq$ between R' and R by: $r' \leq r$ iff $r'_1 \leq_1 r_1$ and $r'_2 \leq_2 r_2$. Let us prove that $\leq$ is a simulation.

Let r' be such that $r' \xrightarrow{\alpha}_{M'} S'$ for some consistent S'. Then, $r' = r'_1 \sqcup r'_2$ and $S' = S'_1 \times S'_2$. By definition of the parallel composition, we have $r'_i \xrightarrow{\alpha}_{M'_i} S'_i$ for $i = 1, 2$. Since $r'_i \leq r_i$, we derive the existence (and uniqueness) of consistent systems $S_i, i = 1, 2$ such that $r_i \xrightarrow{\alpha}_{M_i} S_i$. Since $r = r_1 \sqcup r_2$ we have $r_1 \bowtie r_2$ and, thus, by definition of the parallel composition, we deduce $r \xrightarrow{\alpha}_M S_1 \times S_2$.

It remains to show that $S_1 \times S_2$ is consistent. To prove this, remember that $S' = S'_1 \times S'_2$ is consistent. Thus, there exist compatible r'_1 and r'_2 such that $S'_i \rightsquigarrow r'_i, i = 1, 2$. By definition of the simulations $\leq_i$, we deduce that $S_i \rightsquigarrow r_i, i = 1, 2$, which shows that $S_1 \times S_2$ is consistent.

C Proofs regarding Probabilistic Automata

C.1 Proof of Theorem 1

Defining simulation relations for PA requires lifting relations, from states to distributions over states. The formal definition for this lifting, as given in Section 4.1 of [22], corresponds to our Definition 5, when restricted to purely probabilistic mixed systems.

The same holds for the strong simulation relation defined in Section 4.2 of the same reference: it is verbatim our Definition 8, when restricted to purely probabilistic mixed systems. This proves the part of Theorem 1 regarding simulation.

We move to parallel composition, for which the reader is referred to [19], Section 3. For $P_1 = (\Sigma, Q_1, q_{0,1}, \rightarrow_1)$ and $P_2 = (\Sigma, Q_2, q_{0,2}, \rightarrow_2)$ two PA, their parallel composition is $P = P_1 \times P_2 = (\Sigma, Q_1 \times Q_2, (q_{0,1}, q_{0,2}), \rightarrow)$, where

$$(q_1, q_2) \xrightarrow{\alpha} \pi_1 \otimes \pi_2 \quad \text{iff} \quad q_i \xrightarrow{\alpha}_i \pi_i \text{ for } i = 1, 2 \tag{23}$$

So, on one hand we consider the MMDP M_P. On the other hand, we consider the parallel composition of the mappings M_{P_1} and M_{P_2}, that is $M = M_{P_1} \times M_{P_2} = (\Sigma, \{\xi_1, \xi_2\}, (q_{0,1}, q_{0,2}), \rightarrow_{12})$, so that the state space is the domain

of the pair (ξ_1, ξ_2), namely $Q_1 \times Q_2$, and, since there is no shared variable between the two MMDP, the transition relation $\rightarrow_{12}$ is given by:

$$(q_1, q_2) \xrightarrow{\alpha}_{12} S_1 \times S_2 \quad \text{iff} \quad q_i \xrightarrow{\alpha}_i S_i \text{ for } i = 1, 2 \tag{24}$$

We thus need to show that

$$M_P \text{ and } M \text{ are simulation equivalent.} \tag{25}$$

We will actually show that the identity relation between the two state spaces (both are equal to $Q_1 \times Q_2$) is a simulation relation in both directions.

Observe first that (23) and (24) differ in that the former involves a nondeterministic transition relatiobn, whereas the latter involves a deterministic transition function, mapping states to mixed systems.

Pick $(q_1, q_2) \in Q_1 \times Q_2$ and consider a transition for M_P:

$$(q_1, q_2) \xrightarrow{\alpha}_{M_P} S = ((\Omega, \Pi), \xi, (q_{0,1}, q_{0,2}), C)$$

where we have, for S:

- Ω is the product of n_1 copies of Q_1 and n_2 copies of Q_2, where, for $i = 1, 2$, n_i is the cardinality of the set $\{\pi_i \mid (q_i, \alpha, \pi_i) \in \rightarrow_i\}$, so that ω identifies $n_1 \times n_2$-tuple of states: $\omega = (q_{11}, \ldots, q_{1n_1}; q_{21}, \ldots, q_{2n_2})$;
- Π is the product of all probabilities belonging to set

$$\{\pi_1 \otimes \pi_2 \mid (q_i, \alpha, \pi_i) \in \rightarrow_i\}$$

- ξ has domain $Q_1 \times Q_2$;
- $(\omega, (q_1, q_2)) \in C$ if and only if

$$(q_1, q_2) \in \{(q_{1i_1}, q_{2i_2}) \mid i_1 \in \{1, \ldots, n_1\} \text{ and } i_2 \in \{1, \ldots, n_2\}\}.$$

Next, pick $(q_1, q_2) \in Q_1 \times Q_2$ and consider a transition for M, see (24). We need to detail what $S_1 \times S_2 = ((\Omega', \Pi'), \xi', (q'_{0,1}, q'_{0,2}), C')$ is. We have, for $S_1 \times S_2$:

- Ω' is still the product of n_1 copies of Q_1 and n_2 copies of Q_2;
- Π' is the product $\Pi_1 \otimes \Pi_2$, where Π_i is the product of all probabilities belonging to set $\{\pi_i \mid (q_i, \alpha, \pi_i) \in \rightarrow_i\}$;
- ξ' has domain $Q_1 \times Q_2$;

- $(\omega, (q_1, q_2)) \in C'$ if and only if

$$(q_1, q_2) \in \{(q_{1i_1}, q_{2i_2}) \mid i_1 \in \{1, \ldots, n_1\} \text{ and } i_2 \in \{1, \ldots, n_2\}\}\,.$$

By associativity of $\otimes$, $\Pi' = \Pi$, whereas other items for S on the one hand and other items for $S_1 \times S_2$ on the other hand, are synctatically identical. Thus (25) follows.

D Proofs regarding Mixed Interfaces

D.1 Proof of Lemma 5

Proof

- We remove from $\mathcal{C}$ inconsistent states q;
  - if $q \overset{\alpha}{\not\dashrightarrow}_{\mathcal{C}}$ and $q \overset{\alpha}{\longrightarrow}_{\mathcal{C}} \mathcal{S}^{\Box}$ then q cannot be involved in a simulation relation allowing to state that M is a model of $\mathcal{C}$ because of (5) in the definition of the model relation.
  - if $q \overset{\alpha}{\longrightarrow}_{\mathcal{C}}$ and $q \overset{\alpha}{\dashrightarrow}_{\mathcal{C}} \mathcal{S}^{\Diamond}$ but $\mathcal{S}^{\Box} \cap \mathcal{S}^{\Diamond}$ contains no consistent system in the sense of Definition 1 q cannot be involved in a simulation relation allowing to state that M is a model of $\mathcal{C}$ because of (6) in the definition of the model relation.

  As a result, q plays no role in the semantics of $\mathcal{C}$ and its lack in $[\mathcal{C}]$ does not change the semantics.
- We remove from $\mathcal{C}$ some may transitions to inconsistent states which could not be realized by any model $\mathcal{C}$. □

D.2 Proof of Lemma 6

Proof The reflexity of $\preceq$ follows immediately from Definition 14.

Now for the transitivity, assume that $\mathcal{C}_1 \preceq \mathcal{C}_2$ and $\mathcal{C}_2 \preceq \mathcal{C}_3$. with the respective refinement relations $\preceq_{12} \subseteq Q_1 \times Q_2$ and $\preceq_{23} \subseteq Q_2 \times Q_3$.

Define now using notation (3):

$$\preceq_{13} \quad = \quad \preceq_{12} \bullet \preceq_{23} \ . \tag{26}$$

Let q_1 and q_3 such that $q_1 \preceq_{13} q_3$. By 26, we have $q_1 \preceq_{12} q_2$ and $q_2 \preceq_{23} q_3 1$ for some q_2. Thus, for all α such that $q_1 \overset{\alpha}{\dashrightarrow}_1 \mathcal{S}_1^{\Diamond}$, we have $q_2 \overset{\alpha}{\dashrightarrow}_2 \mathcal{S}_2^{\Diamond}$ and

$\mathcal{S}_1^\Diamond \subseteq^{\preceq_{12}} \mathcal{S}_2^\Diamond$. Moreover, $q_3 \overset{\alpha}{\dashrightarrow}_3 \mathcal{S}_3^\Diamond$ and $\mathcal{S}_2^\Diamond \subseteq^{\preceq_{23}} \mathcal{S}_3^\Diamond$. By Lemma 3, we have $\mathcal{S}_1^\Diamond \subseteq^{\preceq_{13}} \mathcal{S}_3^\Diamond$.

Similarly for must transitions, for all α such that $q_3 \xrightarrow{\alpha}_3 \mathcal{S}_3^\Box$, we have $q_2 \xrightarrow{\alpha}_2 \mathcal{S}_2^\Box$ and $\mathcal{S}_2^\Box \subseteq^{\preceq_{23}} \mathcal{S}_3^\Box$. Moreover, $q_1 \xrightarrow{\alpha}_1 \mathcal{S}_1^\Box$ and $\mathcal{S}_1^\Box \subseteq^{\preceq_{12}} \mathcal{S}_2^\Box$. By Lemma 3, we have $\mathcal{S}_1^\Box \subseteq^{\preceq_{13}} \mathcal{S}_3^\Box$. A a result, we have $\mathcal{C}_1 \preceq \mathcal{C}_3$. □

D.3 Proof of Theorem 2

Proof Assume $\mathcal{C}_1 \preceq \mathcal{C}_2$ and consider the refinement relation $\preceq \subseteq Q_1 \times Q_2$. Let M be a model of $\mathcal{C}_1$ and let $(r, q_1) \in R \times Q_1$ satisfy $r \models_1 q_1$. Focus first on the *may* transition relation. By (5) applied to $\models_1$, for any α such that $r \xrightarrow{\alpha}_M S_M$

$$q_1 \overset{\alpha}{\dashrightarrow}_{\mathcal{C}_1} \mathcal{S}_1^\Diamond \text{ and } S_M \in^{\models_1} \mathcal{S}_1^\Diamond \text{ both hold.} \tag{27}$$

Let $q_2 \in Q_2$ be such that $q_1 \preceq q_2$. Using the first condition of (8), we get

$$q_2 \overset{\alpha}{\dashrightarrow}_2 \mathcal{S}_2^\Diamond \text{ and } \mathcal{S}_1^\Diamond \subseteq^{\preceq} \mathcal{S}_2^\Diamond \tag{28}$$

Define the relation: $r \models_2 q_2 \Leftrightarrow \exists q_1 \in Q_1 : r \models_1 q_1$ and $q_1 \preceq q_2$. Using notation (3), we have

$$\models_2 \;=\; \models_1 \bullet \preceq \,. \tag{29}$$

Now, let q_2 be such that $r \models_2 q_2$. Combining (27) and (28) yields

$$q_2 \overset{\alpha}{\dashrightarrow}_2 \mathcal{S}_2^\Diamond \quad \text{and} \quad S_M \in^{\models_1} \mathcal{S}_1^\Diamond \subseteq^{\preceq} \mathcal{S}_2^\Diamond \tag{30}$$

which, by (29) and Lemma 3, yields $S_M \in^{\models_2} \mathcal{S}_2^\Diamond$. Combining this and (30) shows that $r \models_2 q_2$. Focus next on the *must* transition relation. Since M is a model of $\mathcal{C}_1$, (6) applied to $\models_1$ yields the existence of $S_M \in^{\models_1} \mathcal{S}_1^\Box \subseteq^{\preceq} \mathcal{S}_2^\Box$ such that $r \xrightarrow{\alpha}_M S_M$, which implies that (6) holds for $\models_2$ by the same reasoning as before.

D.4 Proof of Theorem 3

Proof Using Theorem 2, the previous statements follow from $\mathcal{C}_1 \wedge \mathcal{C}_2 \preceq \mathcal{C}_i$ for $i = 1, 2$. Take the first projection as the candidate refinement relation, namely: $(q_1, q_2) \preceq q_1$ for (q_1, q_2) and q_1 reachable from their respective initial states. Using the four rules of Definition 15, we get $\mathcal{C}_1 \underline{\wedge} \mathcal{C}_2 \preceq \mathcal{C}_1$, and thus $\mathcal{C}_1 \wedge \mathcal{C}_2 = [\mathcal{C}_1 \underline{\wedge} \mathcal{C}_2] \preceq \mathcal{C}_1$ since $\mathcal{C}_1$ possesses no inconsistent state. The same holds for $\mathcal{C}_2$ by symmetry.

D.5 Proof of Theorem 4

Proof We successively prove the two statements. Regarding Statement 1), the same proof holds as for associativity and commutativity of the conjunction. Regarding Statement 2), Property (10) is an immediate consequence of Definitions 9, 12 and 16. Focus next on (11). Assume

$$\begin{array}{l}(q,q_2)\overset{\alpha}{\dashrightarrow}_{\mathcal{C}\otimes\mathcal{C}_2}\ \mathcal{S}^{\diamond}\times\mathcal{S}_2^{\diamond}\\ (q,q_1)\overset{\alpha}{\longrightarrow}_{\mathcal{C}\otimes\mathcal{C}_1}\ \mathcal{S}^{\square}\times\mathcal{S}_1^{\square}\end{array}$$

By the rules of the composition, we deduce that the premises of (8) holds, so we can apply rule (8) since $\mathcal{C}_1 \preceq \mathcal{C}_2$, which yields

$$\begin{array}{l}q_1\overset{\alpha}{\dashrightarrow}_1 \mathcal{S}_1^{\diamond} \text{ and } \mathcal{S}_2^{\diamond} \subseteq^{\preceq} \mathcal{S}_1^{\diamond}\\ q_2\overset{\alpha}{\longrightarrow}_2 \mathcal{S}_2^{\square} \text{ and } \mathcal{S}_2^{\square} \subseteq^{\preceq} \mathcal{S}_1^{\square}\end{array}$$

which implies

$$\begin{array}{l}(q,q_1)\overset{\alpha}{\dashrightarrow}_{\mathcal{C}\otimes\mathcal{C}_1} \mathcal{S}^{\diamond}\times\mathcal{S}_1^{\diamond} \text{ and } \mathcal{S}^{\diamond}\times\mathcal{S}_2^{\diamond} \subseteq^{\preceq'} \mathcal{S}^{\diamond}\times\mathcal{S}_1^{\diamond}\\ (q,q_2)\overset{\alpha}{\longrightarrow}_{\mathcal{C}\otimes\mathcal{C}_2} \mathcal{S}^{\square}\times\mathcal{S}_2^{\square} \text{ and } \mathcal{S}^{\square}\times\mathcal{S}_2^{\square} \subseteq^{\preceq'} \mathcal{S}^{\square}\times\mathcal{S}_1^{\square}\end{array}$$

where $\preceq'$ is defined by $(q,q_2) \preceq' (q,q_1)$ iff $q_2 \preceq q_1$. This shows that $\preceq'$ is a refinement.

E Proofs regarding CMC

E.1 Proof of Lemma 7

Proof Let us detail the semantics of mixed system S, see Definition 1. First, we draw $r' \in \Omega = R$ according to the probability $\Pi(r,.)$: this corresponds to the drawing of the next state in Markov Chain $\mathbf{P}$. Second, we nondeterministically select $(r'', v(r''))$ in the state space $R\times 2^A$ of S so that $(r', r'', v(r'')) \in C$. The only solution is $(r', r', v(r'))$, which provides us with the second component $v(r')$ of the state. The two semantics coincide. □

E.2 Proof of Lemma 8

Proof To the satisfaction relation $\rho \subseteq R\times Q$ following Definition 19, we associate the relation $\models_\rho \subseteq (R\times 2^{A_{\mathbf{P}}}) \times (Q\times 2^{A_{\mathbf{S}}})$, defined by

$$(r,\bar{r}) \models_\rho (q,\bar{q}) \quad \text{iff} \quad \begin{cases} r\ \rho\ q \\ \bar{r} = v_{\mathbf{P}}(r) \\ \bar{q} = v_{\mathbf{S}}(q) \\ \bar{r}_{\downarrow A_{\mathbf{S}}} = \bar{q} \end{cases} \tag{31}$$

Observe that, vice versa, we recover ρ from $\models_\rho$ by keeping only the first condition of it. We have to prove that

$$\rho \text{ is a satisfaction relation for CMC if and only if } \models_\rho \text{ is a satisfaction relation for Mixed Interface.} \tag{32}$$

We first prove the "only if" part of (32) Let (r, q) satisfy $r \,\rho\, q$. By (31), $\models_\rho$ is a relation between the states of MMDP $M_{\mathbf{P}}$ and Mixed Interface $\mathcal{C}_{\mathbf{S}}$. With reference to Definition 12, to show that $\models_\rho$ is a satisfaction relation, it is enough to show that only *may* transitions of $\mathcal{C}_{\mathbf{S}}$ are allowed for $M_{\mathbf{P}}$—the condition related to the *must* transitions is vacuously satisfied.

Let $(r, \bar{r}) \models_\rho (q, \bar{q})$ and $(r, \bar{r}) \longrightarrow_{M_{\mathbf{P}}} S_{\mathbf{P}}$, where $S_{\mathbf{P}} = ((\Omega_{\mathbf{P}}, \pi_{\mathbf{P}}), X_{\mathbf{P}}, C_{\mathbf{P}})$ is defined by applying (13) to $M_{\mathbf{P}}$. We must prove that the latter transition is allowed by the *may* transitions of Mixed Interface $\mathcal{C}_{\mathbf{S}}$, i.e., the target mixed system $S_{\mathbf{P}}$ satisfies condition (5), meaning that

$$\begin{array}{l}(q, \bar{q}) \dashrightarrow_{\mathcal{C}_{\mathbf{S}}} \mathcal{S}_{\mathbf{S}} \text{ and there exists} \\ S_{\mathbf{S}} \in \mathcal{S}_{\mathbf{S}} \text{ such that } S_{\mathbf{P}} \models_\rho^{\mathcal{S}} S_{\mathbf{S}}.\end{array} \tag{33}$$

To construct a mixed system $S_{\mathbf{S}}$ satisfying (33), we start from $r \,\rho\, q$, which provides us with a transition sub-probability Δ satisfying the conditions 2) of Definition 19. We then consider the mixed system $S_{\mathbf{S}} = ((\Omega_{\mathbf{S}}, \pi_{\mathbf{S}}), X_{\mathbf{S}}, C_{\mathbf{S}})$, where:

- $\Omega_{\mathbf{S}} = Q$;
- $\pi_{\mathbf{S}} = \Pi(r, .)\Delta$, which belongs to $\varphi(q)$ by Definition 19;
- $C_{\mathbf{S}} \subseteq \Omega_{\mathbf{S}} \times (Q \times 2^{A_{\mathbf{S}}})$ consists of the triples $(q', (q', \bar{q}'))$, where q' ranges over Q, $\bar{q}' = v_{\mathbf{S}}(q')$, and $v_{\mathbf{S}}$ relates to $v_{\mathbf{P}}$ by $v_{\mathbf{S}}(q') = v_{\mathbf{P}}(r')_{\downarrow A_{\mathbf{S}}}$. By Condition 1) of Definition 19, we get $v_{\mathbf{P}}(r')_{\downarrow A_{\mathbf{S}}} \in V_{\mathbf{S}}(q')$.

Let us prove that the so constructed mixed system $S_{\mathbf{S}}$ satisfies $S_{\mathbf{P}} \models_\rho^{\mathcal{S}} S_{\mathbf{S}}$. We must find a weighting function $w : R \times Q \to [0, 1]$ satisfying the conditions of Definition 5. We claim that the wanted weighting function is

$$w(r', q') = \Pi(r, r')\Delta(r', q') \,.$$

We now prove that Conditions 1) and 2) of Definition 5 are satisfied by w. We begin with Condition 2). We have $\sum_{r'} w(r', q') = \sum_{r'} \Pi(r, r')\Delta(r', q') = \Pi(r, .)\Delta(q')$ using (12). On the other hand,

$$\sum_{q'} w(r', q') = \sum_{q'} \Pi(r, r')\Delta(r', q') = \Pi(r, r') \sum_{q} \Delta(r', q') = \Pi(r, r')$$

by Condition 2a of Definition 19.

Focus next on Condition 1) of Definition 5. Pick $(r', q'; (r', v_{\mathbf{P}}(r'))$ such that $w(r', q')>0$, which implies $\Delta(r', q')>0$. Then by Condition 2c of Definition 19, $r' \rho\, q'$ holds. On the other hand, we have $(q', q', v_{\mathbf{P}}(r')_{\downarrow A_{\mathbf{S}}}) \in C$, showing that $(q', v_{\mathbf{P}}(r')_{\downarrow A_{\mathbf{S}}})$ is the state of $S_{\mathbf{S}}$ wanted in Condition 1) of Definition 5. Hence, the so constructed mixed system $S_{\mathbf{S}}$ satisfies $S_{\mathbf{P}} \models_{\rho}^{\mathcal{S}} S_{\mathbf{S}}$. This proves the "only if" part of (32).

We now move to the "if" part of (32) Let $(r, \bar{r}) \models_{\rho} (q, \bar{q})$. Then by the definition (31) of relation $\models_{\rho}$, we deduce that $r\, \rho\, q$ holds and we must prove that ρ is a satisfaction relation for CMC. To this end we use the fact that $\models_{\rho}$ is a satisfaction relation for Mixed Interface, namely: if $(r, \bar{r}) \longrightarrow_{M_{\mathbf{P}}} S_{\mathbf{P}}$, then there exists $S_{\mathbf{S}} \in \mathcal{S}_{\mathbf{S}}$ such that $S_{\mathbf{P}} \models_{\rho}^{\mathcal{S}} S_{\mathbf{S}}$. The target system $S_{\mathbf{S}}$ takes the form $S_{\mathbf{S}} = ((\Omega, \pi), X, C)$, where:

- $\Omega = Q$;
- $\pi(q') = \sum_{r' \in R} w(r', q')$, where $w(r', q')$ is the weighting function associated to the lifting of relation $\models_{\rho}$;
- $C \subseteq \Omega \times (Q \times 2^{A_{\mathbf{S}}})$ consists of the triples of the form $(q', q', v_{\mathbf{P}}(r')_{\downarrow A_{\mathbf{S}}})$, where r' ranges over R and $r'\, \rho\, q'$.

In proving that the relation ρ inferred from $\models_{\rho}$ is a satisfaction relation for CMC, we must find the Δ occurring in Definition 19. We define it as

$$\Delta(r', q') = \begin{cases} \dfrac{w(r', q')}{\Pi(r, r')} \text{ if } \Pi(r, r') > 0 \\ 0 \text{ otherwise.} \end{cases}$$

The conditions of Definition 19 are satisfied. This finishes the proof of the "if" part and the lemma is proved.

E.3 Proof of Lemma 9

Proof The proof follows the same lines as for Lemma 8. To the refinement relation $\rho \subseteq Q_2 \times Q_1$ following Definition 20, we associate the relation

$$\preceq_{\rho} \subseteq (Q_2 \times 2^{A_2}) \times (Q_1 \times 2^{A_1})$$

defined by

$$(q_2, \bar{q}_2) \preceq_\rho (q_1, \bar{q}_1) \quad \text{iff} \quad \begin{cases} q_2 \ \rho \ q_1 \\ \bar{q}_2 = v_2(q_2) \\ \bar{q}_1 = v_1(q_1) \\ \bar{q}_1 = \bar{q}_{2\downarrow A_1} \end{cases} \tag{34}$$

By (34), $\preceq_\rho$ is a relation between the states of Mixed Interface $\mathcal{C}_{\mathbf{S}_2}$ and $\mathcal{C}_{\mathbf{S}_1}$. Observe that, vice versa, we recover ρ from $\preceq_\rho$ by keeping only the first condition of it. We have to prove that

$$\begin{array}{l} \rho \text{ is a weak refinement relation for CMC if and only if} \\ \preceq_\rho \text{ is a refinement relation for Mixed Interfaces.} \end{array} \tag{35}$$

We first prove the "only if" part of (35) Let (q_2, q_1) satisfy $q_2 \, \rho \, q_1$. With reference to Definition 14, to show that $\preceq_\rho$ is a refinement relation, it is enough to show the first condition of (8)—the condition related to the *must* transitions is vacuously satisfied.

From $(q_2, \bar{q}_2) \preceq_\rho (q_1, \bar{q}_1)$ and $q_2 \dashrightarrow_2 \mathcal{S}_2^\diamond$, we have to deduce

$$q_1 \dashrightarrow_1 \mathcal{S}_1^\diamond \text{ and } \mathcal{S}_2^\diamond \subseteq^{\preceq_\rho} \mathcal{S}_1^\diamond ,$$

which translates as

$$\begin{array}{l} \text{for every } S_2 \in \mathcal{S}_2^\diamond \text{ we can find} \\ S_1 \in \mathcal{S}_1^\diamond \text{ such that } S_2 \preceq_\rho^{\mathcal{S}} S_1. \end{array} \tag{36}$$

Let $S_{2,v}$ have the form $S_{2,v} = ((\Omega_2, \pi_2), X_2, C_{2,v})$ following (14). To construct a mixed system S_1 satisfying (36) we start from $q_2 \, \rho \, q_1$, which provides us with a transition sub-probability Δ satisfying the Conditions 2) of Definition 20. We then consider the mixed system $S_1 = ((\Omega_1, \pi_1), X_1, C_1)$, where:

- $\Omega_1 = Q_1$;
- $\pi_1 = \pi_2 \Delta$, which belongs to $\varphi_1(q_1)$ by Definition 20;
- $C_1 \subseteq \Omega_1 \times (Q_1 \times 2^{A_1})$ consists of the triples of the form $(q_1', q_1', v(q_2')_{\downarrow A_1})$, where v is the one arising in the definition of $S_{2,v}$ and q_1' ranges over Q_1. By Condition 1) of Definition 20, we get $v(q_2')_{\downarrow A_1} \subseteq V_1(q_1')$.

Let us prove that the mixed system S_1 satisfies $S_{2,v} \preceq_\rho^{\mathcal{S}} S_1$. We must find a weighting function $w : Q_2 \times Q_1 \to [0, 1]$ satisfying the conditions of Definition 5. We claim that the wanted weighting function is

$$w(q_2', q_1') = \pi_2(q_2') \Delta(q_2', q_1') .$$

Let us prove that Conditions 1) and 2) of Definition 5 are satisfied by w. We begin with Condition 2). We have $\sum_{q_2'} w(q_2', q_1') = \sum_{q_2'} \pi_2(q_2')\Delta(q_2', q_1') = \pi_1(q_1')$ by definition of π_1. On the other hand,

$$\sum_{q_1'} w(q_2', q_1') = \sum_{q_1'} \pi_2(q_2')\Delta(q_2', q_1') = \pi_2(q_2')$$

by Condition 2a of Definition 20.

Focus next on Condition 1) of Definition 5. Pick $(q_2', q_1'; (q_2', v(q_2'))$ such that $w(q_2', q_1') > 0$, which implies $\Delta(q_2', q_1') > 0$. Then by Condition 2c of Definition 20, $q_2' \rho\, q_1'$ holds. On the other hand, we have $(q_1', q_1', v(q_2')_{\downarrow A_1}) \in C_1$, showing that $(q_1', v(q_2')_{\downarrow A_1})$ is the state of S_1 wanted by Condition 1) of Definition 5. Hence, the so constructed mixed system S_1 satisfies $S_{2,v} \preceq_\rho^{\mathcal{S}} S_1$. This proves the "only if" part of (35).

We next move to the "if" part of (35) Let $(q_2, \bar{q}_2) \preceq_\rho (q_1, \bar{q}_1)$. Then by the definition (34) of relation $\preceq_\rho$, we deduce that $q_2 \,\rho\, q_1$ holds and we must prove that ρ is a weak refinement relation for CMC. To this end we use the fact that $\preceq_\rho$ is a modal refinement relation for Mixed Interface, namely: if $q_2 \dashrightarrow_2 \mathcal{S}_2^\diamond$, then $q_1 \dashrightarrow_1 \mathcal{S}_1^\diamond$ and $\mathcal{S}_2^\diamond \subseteq^{\preceq_\rho} \mathcal{S}_1^\diamond$. That is, for any $S_{2,v_2} \in \mathcal{S}_2^\diamond$, of the form $S_{2,v_2} = ((\Omega_2, \pi_2), X_2, C_{2,v_2})$ following (14), there exists $S_{1,v_1} = ((\Omega_1, \pi_1), X_1, C_{1,v_1}) \in \mathcal{S}_1^\diamond$ such that

$$S_{2,v_2} \preceq_\rho^{\mathcal{S}} S_{1,v_1}\,. \tag{37}$$

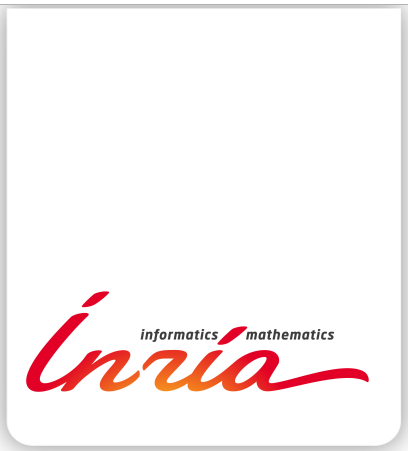
Condition (37) and Definition 5 of the lifting of a relation together imply the existence of a weighting function $w(q_2', q_1')$ satisfying the following conditions:

1. For every triple $(q_2', q_1'; (q_2', v_2(q_2'))$ such that
$$w(q_2', q_1') > 0 \text{ and } (q_2', (q_2', v_2(q_2')) \in C_{2,v_2}\,,$$
there exists $(q_1', v_1(q_1'))$ such that
$$(q_1', (q_1', v_1(q_1')) \in C_{1,v_1} \text{ and } (q_2', \bar{q}_2') \preceq_\rho (q_1', \bar{q}_1')\,.$$
2. $\sum_{q_2'} w(q_2', q_1') = \pi_1(q_1')$ and $\sum_{q_1'} w(q_2', q_1') = \pi_2(q_2')$.

In proving that the relation ρ inferred from $\preceq_\rho$ is a weak refinement relation for CMC, we must find the Δ occurring in Definition 20. We define it as

$$\Delta(q_2', q_1') = \begin{cases} \dfrac{w(q_2', q_1')}{\pi_2(q_2')} \text{ if } \pi_2(q_2') > 0 \\ 0 \text{ otherwise.} \end{cases}$$

The conditions of Definition 20 are satisfied. This finishes the proof of the "if" part and the lemma is proved.



RESEARCH CENTRE
RENNES – BRETAGNE ATLANTIQUE

Campus universitaire de Beaulieu

35042 Rennes Cedex

Publisher
Inria
Domaine de Voluceau - Rocquencourt
BP 105 - 78153 Le Chesnay Cedex
inria.fr

ISSN 0249-6399