Decision Problems for Interval Markov Chains *

Benoît Delahaye¹, Kim G. Larsen², Axel Legay³, Mikkel L. Pedersen², and Andrzej Wąsowski⁴

¹ Université de Rennes 1/IRISA, France
 ² Aalborg University, Denmark
 ³ INRIA/IRISA, France
 ⁴ IT University of Copenhagen, Denmark

Abstract. Interval Markov Chains (IMC) are the base of a classic probabilistic specification theory by Larsen and Jonsson in 1991. They are also a popular abstraction for probabilistic systems.

In this paper we study complexity of several problems for this abstraction, that stem from compositional modeling methodologies. In particular we close the complexity gap for thorough refinement of two IMCs and for deciding the existence of a common implementation for an unbounded number of IMCs, showing that these problems are EXPTIME-complete. We also prove that deciding consistency of an IMC is polynomial and discuss suitable notions of determinism for such specifications.

1 Introduction

Interval Markov Chains (IMCs for short) extend Markov Chains, by allowing to specify intervals of possible probabilities on state transitions. IMCs have been introduced by Larsen and Jonsson [13] as a *specification* formalism—a basis for a stepwise-refinementlike modeling method, where initial designs are very abstract and underspecified, and then they are made continuously more precise, until they are concrete. Unlike richer specification models such as Constraint Markov Chains [5], IMCs are difficult to use for compositional specification due to lack of basic modeling operators. To address this, we study complexity and algorithms for deciding consistency of conjunctive sets of IMC specifications.

In [13] Jonsson and Larsen have introduced refinement for IMCs, but have not determined its computational complexity. We complete their work on refinement, by classifying the complexity and characterizing it using structural coinductive algorithms in the style of simulation.

Consider the issue of combining multiple specifications of the same system. It turns out that conjunction of IMCs cannot be expressed as an IMC itself, due to a lack of expressiveness of intervals. Let us demonstrate this using a simple specification of a user of a coffee machine. Let the model prescribe that a typical user orders coffee with milk with probability $x \in [0, 0.5]$ and black coffee with probability $y \in [0.2, 0.7]$

^{*} This work was supported by the European STREP-COMBEST project no. 215543, by VKR Centre of Excellence MT-LAB, and by an "Action de Recherche Collaborative" ARC (TP)I.

(customers also buy tea with probability $t \in [0, 0.5]$). Now the vendor of the machine delivers another specification, which prescribes that the machine is serviceable only if coffee (white or black) is ordered with some probability $z \in [0.4, 0.8]$ from among other beverages, otherwise it will run out of coffee powder too frequently, or the powder becomes too old. A conjunction of these two models would describe users who have use patterns compatible with this particular machine. Such a conjunction effectively requires that all the interval constraints are satisfied and that z = x + y holds. However, the solution of this constraint is not described by an interval over x and y. This can be seen by pointing out an extremal point, which is not a solution, while all its coordinates take part in some solution. Say x = 0 and y = 0.2 violates the interval for z, while for each of these two values it is possible to select another one in such a way that z's constraint is also held (for example (x = 0, y = 0.4) and (x = 0.2, y = 0.2)). Thus the solution space is not an interval over x and y.

This lack of closure properties for IMCs motivates us to address the problem of reasoning about conjunction, without constructing it — the, so called, common implementation problem. In this paper we provide algorithms and complexities for consistency, common implementation, and refinement of IMCs, in order to enable compositional modeling. We contribute the following new results:

- In [13] a thorough refinement (TR) between IMCs is defined as an inclusion of implementation sets. We define suitable notions of determinism for IMCs, and show that for deterministic IMCs TR coincides with two simulation-like preorders (the weak refinement and strong refinement), for which there exist co-inductive algorithms terminating in a polynomial number of iterations.
- We show that the thorough refinement procedure given in [13] can be implemented in single exponential time. Furthermore we provide a lower bound, concluding that TR is EXPTIME-complete. While the reduction from TR of modal transition systems [4] used to provide this lower bound is conceptually simple, it requires a rather involved proof of correctness, namely that it preserves sets of implementations in a sound and complete manner.
- A polynomial procedure for checking whether an IMC is *consistent* (C), i.e. it admits an implementation as a Markov Chain.
- An exponential procedure for checking whether k IMCs are consistent in the sense that they share a Markov Chain satisfying all—a *common implementation* (CI). We show that this problem is EXPTIME-complete.
- As a special case we observe, that CI is PTIME for any constant value of k. In particular checking whether two specifications can be simultaneously satisfied, and synthesizing their shared implementation can be done in polynomial time.

For functional analysis of discrete-time non-probabilistic systems, the theory of Modal Transition Systems (MTS) [18] provides a specification formalism supporting refinement, conjunction and parallel composition. Earlier we have obtained EXPTIME-completeness both for the corresponding notion of CI [3] and of TR [4] for MTSs. In [13] it is shown that IMCs properly contain MTSs, which puts our new results in a somewhat surprising light: in the complexity theoretic sense, and as far as CI and TR are considered, the generalization of modalities by probabilities does come for free.

3



Fig. 1: Examples of Markov Chains, Interval Markov Chains and satisfaction relation.

The paper proceeds as follows. In Section 2 we introduce the basic definitions. All results in subsequent sections are new and ours. In Section 3 we discuss deciding TR and other refinement procedures. We expand on the interplay of determinism and refinements in Section 4. The problems of C and CI are addressed in Section 5. We close by discussing the results and related work in Section 6. The proofs are deferred to the Appendix, included for the discretion of the referees.

2 Background

We shall now introduce the basic definitions used throughout the paper. In the following we will write $|ntervals_{[0,1]}|$ for the set of all closed, half-open and open intervals included in [0, 1].

We begin with settling notation for Markov Chains. A Markov Chain (sometimes MC in short) is a tuple $C = \langle P, p_0, \pi, A, V_C \rangle$, where P is a set of states containing the initial state p_0 , A is a set of atomic propositions, $V_C : P \to 2^A$ is a state valuation labeling states with propositions, and $\pi : P \to \text{Distr}(P)$ is a probability distribution assignment such that $\sum_{p' \in P} \pi(p)(p') = 1$ for all $p \in P$. The probability distribution assignment is the only component that is relaxed in IMCs:

Definition 1 (Interval Markov Chain). An Interval Markov Chain is a tuple $I = \langle Q, q_0, \varphi, A, V_I \rangle$, where Q is a set of states containing the initial state q_0 , A is a set of atomic propositions, $V_I : Q \to 2^A$ is a state valuation, and $\varphi : Q \to (Q \to Intervals_{[0,1]})$, which for each $q \in Q$ and $q' \in Q$ gives an interval of probabilities.

Instead of a distribution, as in MCs, in IMCs we have a function mapping elementary events (target states) to intervals of probabilities. We interpret this function as a constraint over distributions. This is expressed in our notation as follows. Given a state $q \in Q$ and a distribution $\sigma \in \text{Distr}(Q)$, we say that $\sigma \in \varphi(q)$ iff $\sigma(q') \in \varphi(q)(q')$ for all $q' \in Q$. Occasionally, it is convenient to think of a Markov Chain as an IMC, in which all probability intervals are closed point intervals.

We visualize IMCs as automata with intervals on transitions. As an example, consider the IMC in Figure 1b. It has two outgoing transitions from the initial state A. No arc is drawn between states, if the probability is zero (or more precisely the interval is [0,0]), so in the example there is zero probability of going from state A to A, or from

B to C, etc. Otherwise the probability distribution over successors of A is constrained to fall into]0.7, 1] and [0, 0.3] for B and C respectively. States B and C have valuation β , whereas state A has valuation α, δ . Figure 1a presents a Markov Chain using the same convention, modulo the intervals. Notice that our formalism does not allow "sink states" with no outgoing transitions. In the figures states with no outgoing transitions are meant to have a self-loop transition with probability 1 (a closed point interval).

There are three known ways of defining refinement for IMCs: the strong refinement (introduced as simulation in [13]), weak refinement (introduced under the name of probabilistic simulation in [9]), and thorough refinement (introduced as refinement in [13]). We will recall their formal definitions:

Definition 2 (Strong Refinement). Let $I_1 = \langle Q, q_0, \varphi_1, A, V_1 \rangle$, $I_2 = \langle S, s_0, \varphi_2, A, V_2 \rangle$ be IMCs. A relation $\mathcal{R} \subseteq Q \times S$ is a strong refinement relation if whenever $q \mathcal{R}$ s then

1. The valuation sets agree: $V_1(q) = V_2(s)$ and

4

- 2. There exists a correspondence function $\delta: Q \to (S \to [0,1])$ such that for all $\sigma \in \text{Distr}(Q)$, if $\sigma \in \varphi_1(q)$, then
 - (a) for each $q' \in Q$ such that $\sigma(q') > 0$, $\delta(q')$ is a distribution on S,
 - (b) for all $s' \in S$, we have $\sum_{q' \in Q} \sigma(q') \cdot \delta(q')(s') \in \varphi_2(s)(s')$, and (c) for all $q' \in Q$ and $s' \in S$, if $\delta(q')(s') > 0$, then $q' \mathcal{R} s'$.

 I_1 strongly refines I_2 , or $I_1 \leq_S I_2$, iff there exists a strong refinement containing (q_0, s_0) .

A strong refinement relation requires existence of a single correspondence, which witnesses satisfaction for any resolution of probability constraint over successors of q and s. Figure 2a illustrates such a correspondence between states A and α of two IMCs. The correspondence function is given by labels on the dashed lines. It is easy to see that regardless of how the probability constraints are resolved the correspondence function distributes the probability mass in a fashion satisfying α .

A weak refinement relation requires that for any resolution of probability constraint over successors in I_1 there exists a correspondence function, which witnesses satisfaction of I_2 . The formal definition of weak refinement is identical to Def. 2, except that the condition opening Point 2 is replaced by a weaker one:

Definition 3 (Weak Refinement). Let $I_1 = \langle Q, q_0, \varphi_1, A, V_1 \rangle$, $I_2 = \langle S, s_0, \varphi_2, A, V_2 \rangle$ be IMCs. A relation $\mathcal{R} \subseteq Q \times S$ is a weak refinement relation if whenever $q \mathcal{R}$ s, then

- Their valuation sets agree: $V_1(q) = V_2(s)$
- For each $\sigma \in \text{Distr}(Q)$ such that $\sigma \in \varphi_1(q)$, there exists a correspondence function $\delta: Q \to (S \to [0,1])$ such that
 - 1. For each $q' \in Q$ such that $\sigma(q') > 0$, $\delta(q')$ is a distribution on S,
 - 2. for all $s' \in S$, we have $\sum_{q' \in Q} \sigma(q') \cdot \delta(q')(s') \in \varphi_2(s)(s')$, and 3. for all $q' \in Q$ and $s' \in S$, if $\delta(q')(s') > 0$, then $q' \mathcal{R} s'$.

 I_1 weakly refines I_2 , or $I_1 \leq_W I_2$, iff there exists a weak refinement containing (q_0, s_0) .



(a) Illustration of a strong refinement relation between an IMC I_1 and an IMC I_2 .

(b) Illustration of a weak refinement relation between an IMC I_3 and an IMC I_2 .

Fig. 2: Illustration of strong and weak refinement relations.

Figure 2b illustrates a weak refinement between states A and α of another two IMCs. Here x stands for a value in [0.2, 1] (arbitrary choice of probability of going to state C from A). Notably, for each choice of x there exists $p \in [0, 1]$ such that $p \cdot x \in [0, 0.6]$ and $(1 - p) \cdot x \in [0.2, 0.4]$.

Satisfaction Relation. This relation establishes compatibility of Markov Chains (implementations) and IMCs (specifications). The original definition has been presented in [13, 14]. Consider a Markov chain $C = \langle P, p_0, \pi, A, V_C \rangle$ as an IMC with only closed point interval probabilities, and let $I = \langle Q, q_0, \varphi, A, V_I \rangle$ be an IMC. We say that C satisfies I, written $C \models I$, iff there exists a weak/strong refinement relation $\mathcal{R} \subseteq P \times Q$, called a *satisfaction relation*, containing (p_0, q_0) . Remark that when C is a Markov Chain, the weak and strong notions of refinement coincide. Whenever $C \models I$, C is called an *implementation* of I. The set of implementations of I is written [I]. Figure 1c presents an example of satisfaction on states 1 and A. The correspondence function is specified using labels on the dashed arrows i.e. the probability mass going from state 1 to 3 is distributed to state B and C with half going to each.

We will say that a state q of an IMC is *consistent*, if its interval constraint $\varphi(q)$ is satisfiable, i.e. there exists a distribution $\sigma \in \text{Distr}(Q)$ satisfying $\varphi(q)$ so: $\sigma \in \varphi(q)$. Obviously, for a given IMC, it is sufficient that all its states are consistent in order to guarantee that the IMC is consistent itself—there exists a Markov Chain satisfying it. We discuss the problem of establishing consistency in a sound and complete manner in Section 5.

Finally, we introduce the thorough refinement as defined in [13]:

Definition 4 (Thorough Refinement). *IMC* I_1 thoroughly refines *IMC* I_2 , written $I_1 \leq_T I_2$, iff each implementation of I_1 implements I_2 : $[I_1] \subseteq [I_2]$

Thorough refinement is the ultimate refinement relation for any specification formalism, as it is based on the semantics of the models.

3 Refinement Relations

In this section, we compare the expressiveness of the refinement relations. It is not hard to see that both strong and weak refinements soundly approximate the thorough refinement (since they are transitive and degrade to satisfaction if the left argument is a 6

Markov Chain). The converse does not hold. We will now discuss procedures to compute weak and strong refinements, and then compare the granularity of these relations, which will lead us to procedures for computing thorough refinement. Observe that both refinements are decidable, as they only rely on the first order theory of real numbers. In concrete cases below the calculations can be done more efficiently due to convexity of solution spaces for interval constraints.

Weak and Strong Refinement. Consider two IMCs $I_1 = \langle P, o_1, \varphi_1, A, V_1 \rangle$ and $I_2 = \langle Q, o_2, \varphi_2, A, V_2 \rangle$. Informally, checking whether a given relation $\mathcal{R} \subseteq P \times Q$ is a weak refinement relation reduces to checking, for each pair $(p, q) \in \mathcal{R}$, whether the following formula is true: $\forall \pi \in \varphi_1(p), \exists \delta : P \to (Q \to [0, 1])$ such that $\pi \times \delta$ satisfies a system of linear equations / inequations. Since the set of distributions satisfying $\varphi_1(p)$ is convex, checking such a system is exponential in the number of variables, here $|P| \cdot |Q|$. As a consequence, checking whether a relation on $P \times Q$ is a weak refinement relation is exponential in $|P| \cdot |Q|$. For strong refinement relations, the only difference appears in the formula that must be checked: $\exists \delta : P \to (Q \to [0, 1])$ such that $\forall \pi \in \varphi_1(p)$, we have that $\pi \times \delta$ satisfies a system of linear equations / inequations. Therefore, checking whether a relation is also exponential in $|P| \cdot |Q|$.

Deciding whether weak (strong) refinement holds between I_1 and I_2 can be done in the usual coinductive fashion by considering the total relation $P \times Q$ and successively removing all the pairs that do not satisfy the above formulae. The refinement holds iff the relation we reach contains the pair (o_1, o_2) . The algorithm will terminate after at most $|P| \cdot |Q|$ iterations. This gives an upper bound on the complexity to establish strong and weak refinements: a polynomial number of iterations over an exponential step. This upper bound may be loose. One could try to reuse techniques for nonstochastic systems [12] in order to reduce the number of iterations. This is left to future work.

Granularity. In [13] an informal statement is made, that the strong refinement is strictly stronger (finer) than the thorough refinement: $(\leq_T) \supseteq (\leq_S)$. In [9] the weak refinement is introduced, but without discussing its relations to neither the strong nor the thorough refinement. The following theorem resolves all open issues in relations between the three:

Theorem 1. The thorough refinement is strictly weaker than the weak refinement, which is strictly weaker than the strong one: $(\leq_T) \supseteq (\leq_W) \supseteq (\leq_S)$.

The first inequality is shown by exhibiting IMCs I_4 and I_5 such that I_4 thoroughly, but not weakly refines I_5 (Figure 3). All implementations of I_4 satisfy I_5 , but state Bcan not refine any of β_1 or β_2 : Let σ be a distribution admitted in B giving probability 1 to state C. Because of the interval [0, 0.5] on the transition from β_1 to δ_1 , at least 0.5 must be assigned to γ_1 , but C and γ_1 can not be related. A similar argument shows that B can not refine β_2 . The second inequality is shown by demonstrating other two IMCs, I_3 and I_2 such that I_3 weakly but not strongly refines I_2 (Figure 2b). State Aweakly refines state α : Given a value x for the transition $A \to C$, we can split it in order to match both transitions $\alpha \xrightarrow{p \cdot x} \delta_1$ and $\alpha \xrightarrow{(1-p) \cdot x} \delta_2$. Define $\delta(C)(\delta_1) = p$ and $\delta(C)(\delta_2) = (1-p)$, with p = 0 if $0.2 \le x \le 0.4$, $p = \frac{x-0.3}{x}$ if 0.4 < x < 0.8, and



Fig. 3: IMCs I_4 and I_5 such that I_4 thoroughly but not weakly refines I_5



Fig. 4: An example of the translation from Modal Transition Systems to IMCs

p = 0.6 if $0.8 \le x$. The correspondence function δ witnesses weak refinement between A and α . However, there is no such value of p that would work uniformly for all x, which is required by the strong refinement.

Deciding Thorough Refinement. As weak and strong refinements are strictly stronger than thorough refinement, it is interesting to investigate complexity of deciding TR. In [13] a procedure computing TR is given, albeit without a complexity class, which we establish now closing the problem:

Theorem 2. The decision problem TR of establishing whether there exists a thorough refinement between two given IMCs is EXPTIME-complete.

The upper-bound in checking whether I_1 thorough refines I_2 is shown by observing that the complexity of the subset-simulation algorithm of [13] is $O(|Q| \cdot 2^{|P|})$, where Q and P are the set of states of I_1 and I_2 , respectively (see Appendix B.1).

Summarizing, all three refinements are in EXPTIME. Still, weak refinement seems easier to check than thorough. For TR the number of iterations on the state-space of the relation is exponential while it is only polynomial for the weak refinement. Also, the constraint solved at each iteration involves a single quantifier alternation for the weak, and three alternations for the thorough refinement.

The lower bound of Theorem 2 is shown by a polynomial reduction of the thorough refinement problem for modal transition systems to TR of IMCs. The former problem is known to be EXPTIME-complete [4].

A modal transition system (an MTS in short) [18] is a tuple $M = (S, s_0, A, \rightarrow, - \rightarrow)$, where S is the set of states, s_0 is the initial state, and $\rightarrow \subseteq S \times A \times S$

7

are the transitions that *must* be taken and $-\rightarrow \subseteq S \times A \times S$ are the transitions that *may* be taken. In addition, it is assumed that $(\rightarrow) \subseteq (-\rightarrow)$. An implementation of an MTS is a labelled transition system, i.e., an MTS where $(\rightarrow) = (-\rightarrow)$. Formal definitions of refinement and satisfaction for MTSs are given in Appendix B.4.

We describe here a translation of MTSs into IMCs which preserves implementations, while we delegate the technicalities of the proof to Appendix B.5. We assume we only work with modal transition systems that have no deadlock-states, in the sense that each state has at least one outgoing must transition. It is easy to transform two arbitrary MTSs into deadlock-free ones, without affecting the thorough refinement between them. See Appendix B.4 for a proof.

The IMC \widehat{M} corresponding to a MTS $M = (S, s_0, A, \rightarrow, - \rightarrow)$ is defined by the tuple $\widehat{M} = \langle Q, q_0, A \cup \{\epsilon\}, \varphi, V \rangle$ where $Q = S \times (\{\epsilon\} \cup A), q_0 = (s_0, \epsilon)$, for all $(s, x) \in Q, V((s, x)) = \{x\}$ and φ is defined as follows: for all $t, s \in S$ and $b, a \in (\{\epsilon\} \cup A), \varphi((t, b))((s, a)) =]0, 1]$ if $t \xrightarrow{a} s; \varphi((t, b))((s, a)) = [0, 0]$ if $t \not\xrightarrow{a} s;$ and $\varphi((t, b))((s, a)) = [0, 1]$ otherwise. The encoding is illustrated in Figure 4.

Now one can show that $I \models M$ iff $\llbracket I \rrbracket \subseteq \llbracket M \rrbracket$, and use this to show that the reduction preserves thorough refinement. This observation, which shows how deep is the link between IMCs and modal transition systems, is formalized in the following theorem lifting the syntactic reduction to the level of extensional semantics:

Theorem 3. Let M and M' be two Modal Transition Systems and \widehat{M} and $\widehat{M'}$ be the corresponding IMCs defined as above. We have

$$M \leq_{\mathsf{T}} M' \iff \widehat{M} \leq_{\mathsf{T}} \widehat{M'}$$

Crucially the translation is polynomial. Thus if we had a subexponential algorithm for TR of IMCs, we could use it to obtain a subexponential algorithm for TR of MTSs, which is impossible [4].

4 Determinism

Although both are in EXPTIME, deciding weak refinement is easier than deciding thorough refinement. Nevertheless, since these two refinements do not coincide, in general, a procedure to check weak refinement cannot be used to decide thorough refinement.

Observe that weak refinement has a syntactic definition very much like simulation for transition systems. On the other hand thorough refinement is a semantic concept, just as trace inclusion for transition systems. It is well known that simulation and trace inclusion coincide for deterministic automata. Similarly for MTSs it is known that TR coincides with modal refinement for deterministic objects. It is thus natural to define deterministic IMCs and check whether thorough and weak refinements coincide on these objects.

In our context, an IMC is deterministic if, from a given state, one cannot reach two states that share common atomic propositions.

Definition 5 (Determinism). An IMC $I = \langle Q, q_0, \varphi, A, V \rangle$ is deterministic iff for all states $q, r, s \in Q$, if there exists a distribution $\sigma \in \varphi(q)$ such that $\sigma(r) > 0$ and $\sigma(s) > 0$, then $V(r) \neq V(s)$.

Weak determinism ensures that two states reachable with the same admissible dis*tribution* always have different valuations. In a semantic interpretation this means that there exists no implementation of I, in which two states with the same valuation can be successors of the same source state. Another, slightly more syntactic but semantically equivalent notion of determinism is given in Appendix C.1.

It is worth mentioning that deterministic IMCs are a strict subclass of IMCs. Figure 9 shows an IMC I whose set of implementations cannot be represented by a deterministic IMC.



We now state the main theorem of the section that shows that for deterministic IMCs, the weak refinement, and indeed also the strong refinement, correctly capture the thorough refinement:

Fig. 5: An IMC I whose implementations cannot be captured by a deterministic IMC.

Theorem 4. For deterministic IMCs I, I' with no inconsistent states $I \leq_T I'$ iff $I \leq_W I'$ iff $I \leq_{\mathsf{S}} I'$.

Common Implementation and Consistency 5

We now turn our attention to the problem of implementation of several IMC specifications by the same probabilistic system modeled as a Markov Chain. We start with defining the problem:

Definition 6 (Common Implementation (CI)). Given k > 1 IMCs I_i , $i = 1 \dots k$, does there exist a Markov Chain C such that $C \models I_i$ for all i?

Somewhat surprisingly we find out that, similarly to the case of TR, the CI problem is not harder for IMCs than for modal transition systems:

Theorem 5. Deciding the existence of a CI between k IMCs is EXPTIME-complete.

We sketch the line of argument below, delegating to Appendix D for details. To establish a lower bound for CI of IMCs, we reduce from CI of modal transition systems, which is known to be EXPTIME-complete [3]. For a set of modal transition systems M_i , $i = 1 \dots k$, translate each M_i , into an IMC \widehat{M}_i , using the same rules as in Section 3. It turns out that the set of created IMCs has a common implementation if and only if the original modal transition systems had. Since the translation is polynomial, the problem of CI for IMCs has to be at least EXPTIME-hard (otherwise it would give a sub-EXPTIME algorithm for CI of MTSs).

To address the upper bound we first propose a simple construction to check if there exists a CI for two IMCs. We start with the definition of *consistency relation* that witnesses a common implementation between two IMCs.

Definition 7. Let $I_1 = \langle Q_1, q_0^1, \varphi_1, A, V_1 \rangle$ and $I_2 = \langle Q_2, q_0^2, \varphi_2, A, V_2 \rangle$ be IMCs. Then $\mathcal{R} \subseteq Q_1 \times Q_2$ is a consistency relation on the states of I_1 and I_2 iff whenever $(u, v) \in \mathcal{R}$ then

10 B. Delahaye, K.G. Larsen, A. Legay, M.L. Pedersen, and A. Wąsowski

 $\begin{array}{l} - \ V_{1}(u) = V_{2}(v), \\ - \ there \ exists \ a \ \rho \in {\rm Distr}(Q_{1} \times Q_{2}) \ such \ that \\ 1. \ \forall u' \in Q_{1} : \sum_{v' \in Q_{2}} \rho(u',v') \in \varphi_{1}(u)(u') \ \land \ \forall v' \in Q_{2} : \sum_{u' \in Q_{1}} \rho(u',v') \in \varphi_{2}(v)(v'), \ and \\ 2. \ \forall (u',v') \in Q_{1} \times Q_{2} \ st. \ \rho(u',v') > 0, \ then \ (u',v') \in \mathcal{R}. \end{array}$

It can be shown that two IMCs indeed have a common implementation if and only if there exists a consistency relation containing their initial states. The consistency relation can be computed in polynomial time using a standard coinductive fixpoint iteration, where pairs violating Definition 7 are successively removed from $Q_1 \times Q_2$. Each iteration requires solving a polynomial number of linear systems, which can be done in polynomial time [17]. For the general problem of common implementation of k IMCs, we can extend the above definition of consistency relation to the k-ary relation in the obvious way, and the algorithm becomes exponential in the number of IMCs k, as the size of the state space $\prod_{i=1}^{k} |Q_i|$ is exponential in k.

As a side effect we observe that, exactly like MTSs, CI becomes polynomial for any constant value of k, i.e. when the number of components to be checked is bounded by a constant.

Consistency A related problem is the one of checking consistency of a single IMC I, i.e. whether there exists a Markov chain M such that $M \models I$.

Definition 8 (Consistency (C)). *Given an IMC I, does it hold that* $[I] \neq \emptyset$?

It turns out that, in the complexity theoretic sense, this problem is easy:

Theorem 6. The problem C, to decide if a single IMC is consistent, is polynomial time solvable.

Given an IMC $I = \langle Q, q_0, \varphi, A, V \rangle$, this problem can be solved by constructing a consistency relation over $Q \times Q$ (as if searching for a common implementation of Q with itself). Now there exists an implementation of I iff there exists a consistency relation containing (q_0, q_0) . Obviously, this can be checked in polynomial time.

The fact that C can be decided in polynomial time casts an interesting light on the ability of IMCs to express inconsistency. On one hand, one can clearly specify inconsistent states in IMCs (simply by giving intervals for successor probabilities that cannot be satisfied by any distribution). On the other hand, this inconsistency appears to be local. It does not induce any global constraints on implementations; it does not affect consistency of other states. In this sense IMCs resemble modal transition systems (which at all disallow expressing inconsistency), and are weaker than *mixed transition systems*, not requiring that $(\rightarrow) \subseteq (-\rightarrow)$. It is known that C is trivial for modal transition systems, but EXPTIME-complete for mixed transition systems [3]. Clearly, with a polynomial time C, IMCs cannot possibly express global behaviour inconsistencies in the style of mixed transition systems, where the problem is much harder.

We conclude the section by observing that, given the IMC I and a consistency relation $\mathcal{R} \subseteq Q \times Q$, it is possible to derive a *pruned* IMC $I^* = \langle Q^*, q_0^*, \varphi^*, A, V^* \rangle$ that contains no inconsistent states and accepts the same set of implementations as I. The construction of I^* is as follows: $Q^* = \{q \in Q | (q, q) \in \mathcal{R}\}, q_0^* = q_0, V^*(q^*) = V(q^*)$ for all $q^* \in Q^*$, and for all $q_1^*, q_2^* \in Q^*, \varphi^*(q_1^*)(q_2^*) = \varphi(q_1^*)(q_2^*)$.

11

6 Related Work and Conclusion

This paper provides new results for IMCs [13] that is a specification formalism for probabilistic systems. We have studied the expressiveness and complexity of three refinement preorders for IMCs. The results are of interest as existing articles on IMCs often use one of these preorders to compare specifications (for abstractions) [13, 15, 9]. We have established complexity bounds and decision procedures for these relations, first introduced in [13]. Finally, we have studied the common implementation problem that is to decide whether there exists an implementation that can match the requirements made by two or more specifications. Our solution is constructive in the sense that it can build such a common implementation.

Our results are robust with respect to simple variations of IMCs. For example sets of sets of propositions can be used to label states, instead of sets of propositions. This extends the power of the modeling formalism, which now can not only express abstractions over probability distributions, but also over possible state valuations. Similarly an initial distribution, or even an interval constraint on the initial distribution, could be used instead of the initial state in IMCs without affecting the results.

There exists many other specification formalisms for describing and analyzing stochastic systems; the list includes process algebras [2, 19] or logical frameworks [10]. We believe that IMCs is a good unification model. A logical representation is suited for conjunction, but nor for refinement and vice-versa for process algebra. As an example, it is not clear how one can synthesize a MC (an implementation) that satisfies two Probabilistic Computation Tree Logic formulas.

IMCs served the purpose of *abstraction* in model checking, where a concrete system is being abstracted by a less precise system in order to prove the properties more easily [7, 6, 9, 15]. The main issues related to model checking of IMCs have recently been addressed in [9].

As we already stated, IMCs are not expressive enough to represent many artifacts of compositional design. In [5], we have presented Constraint Markov Chains (CMC) a specification model that, contrary to IMCs, is closed under composition and conjunction. While more expressive than IMCs, CMCs are not an immediate and universal replacement for IMCs, given that complexity of decision procedures for them is much higher. IMCs remain relevant, whenever parallel composition is not required in the application, or when they are used as a coarse abstraction (for example) for CMCs. In the future we expect to see whether our complexity results can be extended to CMCs, and whether IMCs can be used in counter-example guided abstraction-refinement decision procedures for CMCs.

In [15, 16], Katoen et al. have proposed an extension of IMCs to the continuous timed setting. It would be interesting to see whether our results extend to this new model. Another interesting future work would be to extend our results to other specification formalisms for systems that mix both stochastic and non-deterministic aspects. Among them, one finds probabilistic automata [20] where weak/strong refinement would be replaced by probabilistic simulation [21].

In mathematics the abstraction of Markov set-chains [11] lies very close to IMCs. It has been, for instance, used to approximate dynamics of hybrid systems [1]. Markovset chain have different objective, and compositional reasoning operators have not been considered for them, so far. Markov set-chains allow iterative approximation of implementations with increasing state space size. It would be interesting to investigate if these could be used to define size-parametrized versions of our decision problems, and whether these could be solved by iterative approximations.

References

- Abate, A., D'Innocenzo, A., Benedetto, M.D.D., Sastry, S.S.: Markov set-chains as abstractions of stochastic hybrid sytems. In: HSCC. Volume 4981 of LNCS, Springer (2008)
- [2] Andova, S.: Process algebra with probabilistic choice. In: ARTS, London, UK, Springer-Verlag (1999) 111–129
- [3] Antonik, A., Huth, M., Larsen, K.G., Nyman, U., Wąsowski, A.: Modal and mixed specifications: key decision problems and their complexities. MSC 20(01) (2010) 75–103
- [4] Benes, N., Kretínský, J., Larsen, K.G., Srba, J.: Checking thorough refinement on modal transition systems is exptime-complete. In: ICTAC. (2009) 112–126
- [5] Caillaud, B., Delahaye, B., Larsen, K.G., Legay, A., Pedersen, M.L., Wąsowski, A.: Compositional design methodology with constraint markov chains. In: QEST, IEEE Computer (2010)
- [6] Clarke, E.M., Grumberg, O., Jha, S., Lu, Y., Veith, H.: Counterexample-guided abstraction refinement for symbolic model checking. J. ACM 50(5) (2003) 752–794
- [7] Clarke, E.M., Grumberg, O., Long, D.E.: Model checking and abstraction. ACM Transactions on Programming Languages and Systems 16(5) (1994) 1512–1542
- [8] Dams, D.: Abstract Interpretation and Partition Refinement for Model Checking. PhD thesis, Eindhoven University of Technology (July 1996)
- [9] Fecher, H., Leucker, M., Wolf, V.: Don't Know in probabilistic systems. In: SPIN. Volume 3925 of LNCS, Springer (2006) 71–88
- [10] Hansson, H., Jonsson, B.: A logic for reasoning about time and reliability. Formal Asp. Comput. 6(5) (1994) 512–535
- [11] Hartfield, H.J.: Markov Set-Chains. Volume 1695 of Lecture Notes in Mathematics. sv (1998)
- [12] Henzinger, M.R., Henzinger, T.A., Kopke, P.W.: Computing simulations on finite and infinite graphs. In: Proc. FOCS'95. (1995) 453–462
- [13] Jonsson, B., Larsen, K.G.: Specification and refinement of probabilistic processes. In: LICS, IEEE Computer (1991) 266–277
- [14] Jonsson, B., Larsen, K.G., Yi, W.: Probabilistic extensions of process algebras. In: Handbook of Process Algebra, Elsevier (2001) 685–710
- [15] Katoen, J., Klink, D., Leucker, M., Wolf, V.: Three-valued abstraction for continuous-time Markov chains. In: CAV. Volume 4590 of LNCS, Springer (2007) 311–324
- [16] Katoen, J., Klink, D., Neuhäußer, M.R.: Compositional abstraction for stochastic systems. In: FORMATS. Volume 5813 of LNCS, Springer (2009) 195–211
- [17] Khachiyan, L.G.: A polynomial algorithm in linear programming. Dokl. Akad. Nauk SSSR 244(5) (1979) 1093–1096
- [18] Larsen, K.G.: Modal specifications. In: AVMS. Volume 407 of LNCS (1989) 232-246
- [19] López, N., Núñez, M.: An overview of probabilistic process algebras and their equivalences. In: VSS. Volume 2925 of LNCS, Springer (2004) 89–123
- [20] Rabin, M.O.: Probabilistic automata. Inf. and Cont. **6**(3) (1963) 230–245
- [21] Segala, R., Lynch, N.: Probabilistic simulations for probabilistic processes. In: CONCUR. Volume 836 of LNCS, Springer (1994) 481–496



(a) Satisfaction relation between a MC Mand an IMC I using a direct redistribution of the probability mass.

(b) Satisfaction relation between a MC Mand an IMC I using an indirect redistribution of the probability mass.

Fig. 6: Satisfaction relations using direct and indirect redistribution of the probability mass.

On Satisfaction Relations Α

There are two classical ways of defining a satisfaction relation for probabilistic specifications like IMCs, and they are strictly equivalent. In our paper we used an explicit correspondence function in the definition of satisfaction. This is slightly different, but a strictly equivalent form [13, 14]:

Definition 9 ((Direct) Satisfaction Relation). Let $C = \langle P, p_0, \pi, A, V_C \rangle$ be a MC and let $I = \langle Q, q_0, \varphi, A, V_I \rangle$ be an IMC. A relation $\mathcal{R} \subseteq P \times Q$ is called a satisfaction relation if whenever $p \mathcal{R} q$ then

$$- V_C(p) = V_I(q)$$

- there exists a probability distribution $\delta \in \text{Distr}(P \times Q)$ such that 1. $\sum_{q' \in Q} \delta(p', q') = \pi(p)(p')$ for all $p' \in P$, 2. $\sum_{p' \in P} \delta(p', q') \in \varphi(q)(q')$ for all $q' \in Q$, and 3. if $\delta(p', q') > 0$, then $p' \mathcal{R} q'$.

Figure 6 compares the two definitions using an example side by side.

On Refinement Relations B

Subset Simulation B.1

For the sake of completeness, and in order to clarify several typesetting inaccuracies of the original presentation, we quote the construction of [13] below and subsequently analyze its complexity:

Definition 10 (Subset simulation). Let $I_1 = \langle Q, q_0, \varphi_Q, A, V_Q \rangle$, $I_2 = \langle P, p_0, \varphi_P, A, V_P \rangle$ be IMCs. A total relation $\mathcal{R} \subseteq Q \times 2^P$ is a subset-simulation iff for each state $q \in Q$:

1.
$$q \mathcal{R} T$$
 implies $V_Q(q) = V_P(t)$ for all $t \in T$

14 B. Delahaye, K.G. Larsen, A. Legay, M.L. Pedersen, and A. Wąsowski

- 2. For each probability distribution $\pi_Q \in \varphi_Q(q)$ and each correspondence function $\delta_Q : Q \to (2^P \to [0,1])$ such that $\text{support}(\delta_Q) \subseteq \mathcal{R}$, there exists a set T such that $q \mathcal{R}T$ and for each $t \in T$, there exists a probability distribution $\pi_P \in \varphi_P(t)$ and a correspondence function $\delta_P : P \to (2^P \to [0,1])$ such that
 - (a) if $\delta_P(t')(T') > 0$ then $t' \in T'$.

(b) For all
$$T' \in 2^P$$
 we have $\sum_{q' \in Q} \pi_Q(q') \delta_Q(q')(T') = \sum_{p' \in P} \pi_P(p') \delta_P(p')(T').$

Intuitively, this relation associates to every state q of I_1 a sample of sets of states (T_1, \ldots, T_k) of I_2 that are "compatible" with q. Then, for each admissible redistribution δ of the successor states of q, it states that there exists one of the sets T_i such that for each of its states t', there is a redistribution γ of the successor states of t' that is compatible with δ . In [13] it is shown that the existence of a subset-simulation between two IMCs I_1 and I_2 is equivalent to thorough refinement between them. We include an example for this construction in Appendix B.2, for convenience of the reader.

The existence of a subset simulation between two IMCs is decided using a standard co-inductive fixpoint calculation. The algorithm works as follows: first consider the total relation and check whether it is a subset-simulation. Then refine it, by removing violating pairs of states, and check again until a fixpoint is reached (it becomes a subset-simulation or it is empty). Checking whether a given relation is a subset simulation has a single exponential complexity. Checking the second condition in the definition can be done in single exponential time by solving polynomial constraints with fixed quantifiers for each pair (q, T) in the relation. There are at most $|Q| \cdot 2^{|P|}$ such pairs, which gives a single exponential time bound for the cost of one iteration of the fixpoint loop. There are at most $|Q| \cdot 2^{|P|}$ elements in the total relation and at least one is removed in an iteration, which gives $O(|Q| \cdot 2^{|P|})$ as the bound on the number of iterations. Since a polynomial of two exponentials, is still an exponential, we obtain a single exponential time for running time of this computation.

B.2 Example of a Subset Simulation

This is example is included for convenience of the reader. The original presentation of this subset simulation relation can be found in [13], but the example used here is ours.

Example 1. Consider the IMCs $I_4 = \langle \{A, B, C, D\}, A, \varphi_4, \{a, b, c, d\}, V_4 \rangle$ and $I_5 = \langle \{\alpha, \beta_1, \beta_2, \delta_1, \delta_2, \rangle$

 γ_1, γ_2 , $\alpha, \varphi_5, \{a, b, c, d\}, V_5$ given in Figure 3. They are such that I_4 thoroughly but not weakly refines I_5 (c.f. proof of Theorem 1). Since thorough refinement holds, we can exhibit a subset simulation $\mathcal{R} \subseteq P \times 2^Q$ between I_4 and I_5 : Let

 $\mathcal{R} = \{ (A, \{\alpha\}), (B, \{\beta_1\}), (B, \{\beta_2\}), (C, \{\delta_1, \delta_2\}), (D, \{\gamma_1, \gamma_2\}) \}.$

- We illustrate the unfolding of \mathcal{R} for states A and B of I_4 . The rest is left to the reader. Consider state A of I_4 .
- 1. We have $A \mathcal{R}\{\alpha\}$, and $V_4(A) = a = V_5(\alpha)$.



Fig. 7: Illustration of the weak refinement relation between IMC I_3 and IMC I_2 ; p is a parameter.

- 2. The only distribution $\pi \in \varphi_4(A)$ is such that $\pi(B) = 1$. Let for example $\Delta^1 \in [0,1]^{4 \times 2^7}$ be the correspondance matrix such that $\Delta^1_{B,\{\beta_1\}} = 1/2$ and $\Delta^1_{B,\{\beta_2\}} = 1/2$. Let $\{\alpha\}$ be the set such that $A\mathcal{R}\{\alpha\}$. Let ρ be the distribution on Q such that $\rho(\beta_1) = \rho(\beta_2) = 1/2$. ρ is indeed in $\varphi_5(\alpha)$. Let $\Delta^2 \in [0,1]^{7 \times 2^7}$ be the correspondance matrix such that $\Delta^2_{\beta_1,\{\beta_1\}} = 1$ and $\Delta^2_{\beta_2,\{\beta_2\}} = 1$. It is then obvious that
 - (a) for all t and T, if $\Delta_{t,T}^2 > 0$, then $t \in T$;
 - (b) $\pi \times \Delta^1 = \rho \times \Delta^2$ holds.

Consider state B of I_4 .

- 1. We have $B \mathcal{R}\{\beta_1\}$ and $B \mathcal{R}\{\beta_2\}$. It holds that $V_4(B) = b = V_5(\beta_1) = V_5(\beta_2)$.
- 2. Consider a distribution $\pi \in \varphi_4(B)$ (for example such that $\pi(C) < 1/2$). Let Δ^1 be an admissible correspondance matrix. We must have $\Delta^1_{C,\{\delta_1,\delta_2\}} = 1$ and $\Delta^1_{D,\{\gamma_1,\gamma_2\}} = 1$. Consider $\{\beta_1\}$ the set such that $B\mathcal{R}\{\beta_1\}$ (if $\pi(C) > 1/2$ then pick up $\{\beta_2\}$ instead). Let ρ be the distribution such that $\rho(\delta_1) = \pi(C)$ and $\rho(\gamma_1) = \pi(D)$. Since $\pi(C) < 1/2$, we have $\rho \in \varphi_5(\beta_1)$. Let Δ^2 be a correspondance matrix such that $\Delta^2_{\delta_1,\{\delta_1,\delta_2\}} = 1$ and $\Delta^2_{\gamma_1,\{\gamma_1,\gamma_2\}} = 1$. It is obvious that
 - (a) for all t and T, if $\Delta_{t,T}^2 > 0$, then $t \in T$;
 - (b) $\pi \times \Delta^1 = \rho \times \Delta^2$ holds.

The rest of the unfolding is obvious, and \mathcal{R} is thus a subset simulation.

B.3 Proof of Thm. 1

In this section, we give IMCs I_3 , I_2 , I_4 and I_5 proving that

$$(\leq_{\mathsf{T}}) \supseteq (\leq_{\mathsf{W}}) \supseteq (\leq_{\mathsf{S}})$$

Consider the IMCs I_3 and I_2 given in Figure 7. We prove that I_3 weakly but not strongly refines I_2 .

Proof. State A weakly refines state α : Given a value x for the transition $A \to C$, we can split it in order to match both transitions $\alpha \xrightarrow{p \cdot x} \delta_1$ and $\alpha \xrightarrow{(1-p) \cdot x} \delta_2$. Define $\delta(C)(\delta_1) = p$ and $\delta(C)(\delta_2) = (1-p)$, with

$$p = \begin{cases} 0 & \text{if } 0.2 \le x \le 0.4\\ \frac{x - 0.3}{x} & \text{if } 0.4 < x < 0.8\\ 0.6 & \text{if } 0.8 \le x \end{cases}$$

 δ_1 is a correspondence function witnessing a weak refinement relation between A and α . However, we cannot find a coefficient p that would work for all x.

Consider the IMCs I_4 and I_5 given in Figure 8. We prove that I_4 thoroughly but not weakly refines I_5 .



Fig. 8: IMCs I_4 and I_5 such that I_4 thoroughly but not weakly refines I_5

Proof. Let M be an implementation of I_4 and \mathcal{R} a corresponding satisfaction relation. Let P be the set of states of M implementing B. Each state $p \in P$ either satisfies β_1 , β_2 or both. Call P_1 the set of states $p \in P$ such that p satisfies β_1 and P_2 the set of states $p \in P$ such that p satisfies β_2 and not β_1 . We build a satisfaction relation \mathcal{R}' such that, for all $q \in M$, if $q \mathcal{R} A$ then $q \mathcal{R} \alpha$; if $q \in P_1$, then $q \mathcal{R}' \beta_1$; if $q \in P_2$, then $q \mathcal{R}' \beta_2$; if $q \mathcal{R} C$, then $q \mathcal{R}' \delta_1$ and $q \mathcal{R}' \delta_2$; and if $q \mathcal{R} D$ then $q \mathcal{R}' \gamma_1$ and $q \mathcal{R}' \gamma_2$. By construction, \mathcal{R}' is a satisfaction relation, and M is an implementation of I_5 . Thus, $[I_4]] \subseteq [I_5]$.

However, it is impossible to define a weak refinement relation between I_4 and I_5 : obviously, B can neither refine β_1 nor β_2 .

B.4 On MTS with no deadlocks

A modal transition system $M = (S, s_0, A, \rightarrow, - \rightarrow)$ refines another modal transition system $N = (T, t_0, A, \rightarrow, - \rightarrow)$ iff there exists a refinement relation $R \subseteq S \times T$ containing (s_0, t_0) such that if $(s, t) \in R$ then

- 1. whenever $t \stackrel{a}{\longrightarrow} t'$ then also $s \stackrel{a}{\longrightarrow} s'$ for some $s' \in S$ and $(s', t') \in R$
- 2. whenever $s \xrightarrow{a} s'$ then also $t \xrightarrow{a} t'$ for some $t' \in T$ and $(s', t') \in R$

A labelled transition system *implements* a MTS if it refines it in the above sense. Thorough refinement of MTSs is defined as inclusion of implementation sets, analogously to IMCs.

In Section 3, we assume that the MTS we consider have no deadlocks, i.e. in every state there is at least one output must transition. In this way, the transformation we present generates IMCs for which all states are consistent. We present here a transformation that takes any two MTS and transform them into MTS without deadlocks preserving the notion of thorough refinement between them.

Let $M = \langle S, s_0, A, \rightarrow, -- \rangle$ be a MTS. Let $\perp \notin A$ be a new action variable, and $q \notin S$ be a new state variable. Define a new MTS $M_{\perp} = \langle S \cup \{q\}, s_0, A \cup \{\perp\}, \rightarrow_{\perp}, -- \rightarrow_{\perp} \rangle$ as follows: for all $s, s' \in S$ and $a \in A, s \xrightarrow{a}_{\perp} s' \iff s \xrightarrow{a} s'$ and $s \xrightarrow{a}_{-} \downarrow s' \iff s \xrightarrow{-a} s'$. Add the following transitions: for all $s \in S \cup \{q\}, s \xrightarrow{\perp}_{\perp} q$ and $s \xrightarrow{-}_{-} \downarrow q$. In this way, every state of M_{\perp} has at least one must outgoing transition. Moreover, it is trivial that this transformation preserves the notion of thorough refinement. This is stated in the following theorem:

Theorem 7. Let M and M' be two MTS. If \perp is in neither of their sets of actions, we have

 $\llbracket M \rrbracket \subseteq \llbracket M' \rrbracket \iff \llbracket M_{\perp} \rrbracket \subseteq \llbracket M'_{\perp} \rrbracket$

Finally we can safely suppose that all the MTS we consider in the rest of the section have no deadlocks.

B.5 Details about the reduction of MTSs into IMCs

We describe here the translation of MTSs into IMCs which preserves implementations. We first recall the transformation presented in Section 3. The IMC \widehat{M} corresponding to a MTS M is defined by the tuple $\widehat{M} = \langle Q, q_0, A \cup \{\epsilon\}, \varphi, V \rangle$ where $Q = S \times (\{\epsilon\} \cup A)$, $q_0 = (s_0, \epsilon)$, for all $(s, x) \in Q$, $V((s, x)) = \{x\}$ and φ is defined as follows : for all $t, s \in S$ and $b, a \in (\{\epsilon\} \cup A), \varphi((t, b))((s', a)) =]0, 1]$ if $t \xrightarrow{a} s$; $\varphi((t, b))((s', a)) = [0, 0]$ if $t \xrightarrow{a} s$; and $\varphi((t, b))((s', a)) = [0, 1]$ otherwise.

We first state two lemmas that will be needed in order to prove the main theorem of the section: the encoding presented above reduces the problem of checking thorough refinement on modal transition systems to checking thorough refinement on IMCs.

Lemma 1. Let $M = (S, s_0, A, \rightarrow, - \rightarrow)$ be an MTS and $I = (S_I, s_0^I, A, \rightarrow)$ be a transition system. We have

$$I \models M \Rightarrow \llbracket \widehat{I} \rrbracket \subseteq \llbracket \widehat{M} \rrbracket$$

Proof. We first recall the definition of a satisfaction relation for MTS: Let $M = (S, s_0, A, \rightarrow, - \rightarrow)$ be an MTS and $I = (S_I, s_0^I, A, \rightarrow)$ be a transition system. $I \models M$ iff there exists a relation $\mathcal{R} \subseteq S_I \times S$ such that

- 1. $s_0^I \mathcal{R} s_0$
- 2. Whenever $s_I \mathcal{R} s$, we have (a) For all $a \in A$, $s'_I \in S_I$, $s_I \xrightarrow{a} s'_I$ in I implies that there exists $s' \in S$ such that $s \xrightarrow{a} s'$ in M and $s'_{I} \mathcal{R} s'$.
 - (b) For all $a \in A$, $s' \in S$, $s \xrightarrow{a} s'$ in M implies that there exists $s'_I \in S_I$ such that $s_I \xrightarrow{a} s'_I$ in M and $s'_I \mathcal{R} s'$.

Such a relation is called a satisfaction relation for MTS.

Let $M = (S, s_0, A, \rightarrow, --)$ be an MTS and $I = (S_I, s_0^I, A, \rightarrow)$ be a transition system. Let $\widehat{M} = \langle Q, q_0, A \cup \{\epsilon\}, \varphi, V \rangle$ and $\widehat{I} = \langle Q_I, (s_0^I, \epsilon), A \cup \{\epsilon\}, \varphi_I, V_I \rangle$ be the IMCs defined as above.

Suppose that $I \models M$. Then there exists a satisfaction relation for MTS $\mathcal{R} \subseteq S_I \times S$ such that $s_0^I \mathcal{R} s_0$. We prove that $[\widehat{I}] \subseteq [\widehat{M}]$.

Let $T = \langle Q_T, p_0, \pi^T, V_T, A \rangle$ be an MC such that $T \in [[\widehat{I}]]$. As a consequence, there exists a satisfaction relation for IMCs $\mathcal{R}_1 \subseteq Q_T \times Q_I$ such that $p_0 \mathcal{R}_1(s_0^I, \epsilon)$. Define the new relation $\mathcal{R}_2 \subseteq Q_T \times Q$ such that $p \mathcal{R}_2(s, x)$ iff there exists $s_I \in S_I$ such that $p \mathcal{R}_1(s_I, x)$ and $s_I \mathcal{R} s$. We prove that \mathcal{R}_2 is a satisfaction relation for IMCs between T and M.

Let p, s, s_I, x such that $p \mathcal{R}_1(s_I, x)$ and $s_I \mathcal{R} s$, i.e. $p \mathcal{R}_2(s, x)$. If $x \neq \bot$, we have

- 1. Since $p \mathcal{R}_1(s_I, x)$, we have $V_T(p) = V_I((s_I, x)) = \{x\}$. $= \{x\}$. Thus $V_T(p) = V((s, x)) = \{x\}$. 2. Let $\delta^1 \in \text{Distr}(Q_T \times Q_I)$ be the probability distribution witnessing $p \mathcal{R}_1(s_I, x)$, and let $\delta^2 \in \text{Distr}(Q_T \times Q)$ such that for all $p' \in Q_T$, $s' \in S$ and $y \in A$, if $\{s'_I \in S_I \mid s'_I \mathcal{R} s'\} \neq \emptyset$ and $s \xrightarrow{y} s'$, then define

$$\delta^2(p',(s',y)) = \sum_{\{s'_I \in S_I \ | \ s'_I \mathcal{R} \ s'\}} \frac{\delta^1(p',(s'_I,y))}{|\{s'' \in S \ | \ s'_I \mathcal{R} \ s'' \ \text{and} \ s \ -\stackrel{y}{\dashrightarrow} \ s''\}|}$$

Else, $\delta^2(p', (s', y)) = 0.$

Recap that we suppose that all must transitions are also may transitions. The definition above potentially gives a non-zero value to $\delta^2(p', (s', y))$ if there exists a may (or must) transition from s to s' in S labelled with y and if there exists a state s'_{t} in I such that $s'_I \mathcal{R} s'$.

Let $p' \in Q_T$. We prove that $\sum_{(s',y)} \delta_2(p',(s',y)) = \pi^T(p)(p')$: By definition of δ^1 , we have $\sum_{(s_I',y)} \delta^1(p',(s_I',y)) = \pi^T(p)(p').$

$$\sum_{(s',y)} \delta^{2}(p',(s',y)) = \sum_{\{(s',y) \mid \exists s'_{I}, s'_{I} \mathcal{R} s' \text{ and } s^{-\frac{y}{-}} s'\}} \sum_{\{s'_{I} \mid s'_{I} \mathcal{R} s'\}} \frac{\delta^{1}(p',(s'_{I},y))}{|\{s'' \in S \mid s'_{I} \mathcal{R} s'' \text{ and } s^{-\frac{y}{-}} s''\}|}.$$
(1)

Clearly, for all (s'_I, y) such that $\delta^1(p', (s'_I, y)) > 0$, the term

$$\frac{\delta^1(p', (s'_I, y))}{|\{s'' \in S \mid s'_I \mathcal{R} s'' \text{ and } s \xrightarrow{y} s''\}|}$$

will appear exactly $|\{s'' \in S \mid s'_I \mathcal{R} s'' \text{ and } s \xrightarrow{y} s''\}|$ times in the expression above. As a consequence,

$$\sum_{(s',y)} \delta^2(p',(s',y)) = \sum_{(s'_I,y)} \delta^1(p',(s'_I,y)) = \pi^T(p)(p').$$

Moreover, we show that for all $(s',y) \in Q$, that $\sum_{p' \in Q^T} \delta^2(p',(s',y)) \in \varphi((s,x)(s',y))$. By construction, $\varphi((s,x)(s',y))$ is either $\{0\}, [0,1]$ or]0,1]. We will thus prove that (a) if $\sum_{p' \in Q^T} \delta^2(p',(s',y)) > 0$, then $\varphi((s,x)(s',y)) \neq \{0\}$; and (b) if $\varphi((s,x)(s',y)) =]0,1]$, then $\sum_{p' \in Q^T} \delta^2(p',(s',y)) > 0$.

(a) Suppose $\sum_{p' \in Q^T} \delta^2(p', (s', y)) > 0$. By definition, there must exist p' such that

 $\delta^2(p', (s', y)) > 0$. As a consequence, by definition of δ^2 , there exists a transition $s \xrightarrow{y} s'$ in M and $\varphi((s, x), (s', y)) \neq \{0\}$.

(b) If $\varphi((s,x)(s',y)) =]0,1]$, then there exists a transition $s \xrightarrow{y} s'$ in M. As a consequence, by \mathcal{R} , there exists $s'_I \in S_I$ such that $s_I \xrightarrow{y} s'_I$ in I and $s'_I \mathcal{R} s'$. Thus $\varphi_I((s_I, x), (s'_I, y)) =]0,1]$. By definition of δ^1 , we know that $\sum_{p' \in Q^T} \delta^1(p', (s'_I, y))$

> 0, thus there exists $p' \in Q_T$ such that $\delta^1(p', (s'_I, y)) > 0$. Since $s'_I \mathcal{R} s'$ and $s \xrightarrow{y} s'$, we have $\delta^2(p', (s', y)) > 0$, thus

$$\sum_{p'' \in Q^T} \delta^2(p'', (s', y)) > 0.$$

Finally, if $\delta^2(p', (s', y)) > 0$, there exists $s'_I \in S_I$ such that $s'_I \mathcal{R} s'$ and $\delta^1(p', (s'_I, y)) > 0$. By definition of δ^1 , we have $p' \mathcal{R}_1(s'_I, y)$. As a consequence, $p' \mathcal{R}_2(s', y)$.

 \mathcal{R}_2 satisfies the axioms of a satisfaction relation for IMCs, thus $T \in \llbracket \widehat{M} \rrbracket$ and finally $\llbracket \widehat{I} \rrbracket \subseteq \llbracket \widehat{M} \rrbracket$.

Lemma 2. Let $M = (S, s_0, A, \rightarrow, - \rightarrow)$ be an MTS and $I = (S_I, s_0^I, A, \rightarrow)$ be a transition system. We have

$$\llbracket \widehat{I} \rrbracket \subseteq \llbracket \widehat{M} \rrbracket \Rightarrow I \models M$$

Proof. Let $M = (S, s_0, A, \rightarrow, - \rightarrow)$ be an MTS and $I = (S_I, s_0^I, A, \rightarrow)$ be a transition system. Let $\widehat{M} = \langle Q, q_0, A \cup \{\epsilon\}, \varphi, V \rangle$ and $\widehat{I} = \langle Q_I, q_0^I, A \cup \{\epsilon\}, \varphi_I, V_I \rangle$ be the IMCs defined as above.

Suppose that $[\widehat{I}] \subseteq [\widehat{M}]$. We prove that $I \models M$.

20 B. Delahaye, K.G. Larsen, A. Legay, M.L. Pedersen, and A. Wasowski

Let $T = \langle Q_T, p_0, \pi^T, V_T, A \rangle$ be an MC such that $T \in \llbracket \widehat{I} \rrbracket$. As a consequence, there exists two satisfaction relations for IMCs $\mathcal{R}_1 \subseteq Q_T \times Q_I$ and $\mathcal{R}_2 \subseteq Q_T \times Q$ such that $p_0 \mathcal{R}_1(s_0^I, \epsilon)$ and $p_0 \mathcal{R}_2(s_0, \epsilon)$. Define the new relation $\mathcal{R} \subseteq S_I \times S$ such that $s_I \mathcal{R} s$ iff there exists $p \in Q_T$ and $x \in (\{\epsilon\} \cup A)$ such that $p \mathcal{R}_1(s_I, x)$ and $p \mathcal{R}_2(s, x)$. We have

- 1. $p_0 \mathcal{R}_1(s_0^I, \epsilon)$ and $p_0 \mathcal{R}_2(s_0, \epsilon)$. As a consequence, $s_0^I \mathcal{R} s_0$.
- 2. Let s_I, s, p, x such that $p \mathcal{R}_1(s_I, x)$ and $p \mathcal{R}_2(s, x)$ and let $\delta^1 \in \text{Distr}(Q_T \times Q_I)$ and $\delta^2 \in \mathsf{Distr}(Q_T \times Q)$ be the associated probability distributions.
 - (a) Let $y \in A$ and $s'_I \in S_I$ such that $s_I \xrightarrow{y} s'_I$ in I. We prove that there exists $s' \in S$ such that $s \xrightarrow{y} s'$ and $s'_I \mathcal{R} s'$.

By definition of \widehat{I} , we have $\varphi_I((s_I, x), (s'_I, y)) =]0, 1]$. As a consequence, $\sum_{p'' \in Q_T} \delta^1(p'', (s'_I, y)) > 0$. Thus there exists p' in Q_T such that $\delta^1(p', (s'_I, y)) > 0$. y(y) > 0. By definition of δ^1 , we have $p' \mathcal{R}_1(s'_I, y)$, thus $V_T(p') = V_I((s'_I, y)) = V_I(s'_I, y)$ $\{y\}.$

Moreover, by definition of δ^1 , we have $\sum_{(s'',z)\in Q_I} \delta^1(p',(s''_I,z)) = \pi^T(p)(p')$.

Since $\delta^1(p', (s'_I, y)) > 0$, we have $\pi^T(p)(p') > 0$. By definition of δ^2 , we know that $\sum_{(s'',z)\in Q} \delta^2(p', (s'', z)) = \pi^T(p)(p') > 0$. As a consequence, there exists $(s', z) \in Q$ such that $\delta^2(p', (s', z)) > 0$. By definition of δ^2 , we have $p' \mathcal{R}_2(s', z)$ and since $V_T(p') = \{y\}$, we must have z = y.

Consequently, $\sum_{p'' \in Q_T} \delta^2(p'', (s', y)) > 0$. By definition of δ^2 , we know that $\sum_{p'' \in Q_T} \delta^2(p'', (s', y)) \in \varphi((s, x), (s', y))$, thus $\varphi((s, x), (s', y)) \neq \{0\}$, which means, by definition of \widehat{M} , that there exists a transition $s \xrightarrow{y} s'$ in M. Moreover, there exits $p' \in Q_T$ such that both $p' \mathcal{R}_1(s'_I, y)$ and $p' \mathcal{R}_2(s', y)$, thus $s'_I \mathcal{R} s'$.

(b) Let $y \in A$ and $s' \in S$ such that $s \xrightarrow{y} s'$ in M. We prove that there exists $s'_I \in S_I$ such that $s_I \xrightarrow{y} s'_I$ in I and $s'_I \mathcal{R} s'$.

By definition of \widehat{M} , we have $\varphi((s, x), (s', y)) =]0, 1]$. As a consequence, $\sum_{p'' \in Q_T} \delta^2(p'', (s', y))$

> 0. Thus there exists p' in Q_T such that $\delta^2(p', (s', y)) > 0$. By definition of δ^2 , we have $p' \mathcal{R}_2(s', y)$, thus $V_T(p') = V((s', y)) = \{y\}$. Moreover, by definition of δ^2 , we have $\sum_{(s'',z)\in Q} \delta^2(p', (s'', z)) = \pi^T(p)(p')$. Since

 $\delta^2(p',(s',y))>0, \text{ we have }\pi^T(p)(p')>0.$

By definition of δ^1 , we know that $\sum_{(s'_I,z)\in Q_I} \delta^1(p',(s''_I,z)) = \pi^T(p)(p') > 0$. As a consequence, there exists $(s'_I,z) \in Q_I$ such that $\delta^1(p',(s'_I,z)) > 0$. By definition of δ^1 , we have $p' \mathcal{R}_1(s'_I, z)$ and since $V_T(p') = \{y\}$, we must have z = y.

Consequently, $\sum_{p'' \in Q_T} \delta^1(p'', (s'_I, y)) > 0$. By definition of δ^1 , we know that $\sum_{p'' \in Q_T} \delta^1(p'', (s'_I, y)) \in \varphi_I((s_I, x), (s'_I, y)), \text{ thus } \varphi_I((s, x), (s', y)) \neq \{0\},\$ which means, by definition of \widehat{I} , that there exists a transition $s_I \xrightarrow{y} s'_I$ in I(remember that I is a classical transition system). Moreover, there exits $p' \in$ Q_T such that both $p' \mathcal{R}_1(s'_I, y)$ and $p' \mathcal{R}_2(s', y)$, thus $s'_I \mathcal{R} s'$. Finally, \mathcal{R} is a satisfaction relation for MTS, and $I \models M$

From the two lemmas stated above, we can deduce the following theorem.

Theorem 8. Let $M = (S, s_0, A, \rightarrow, - \rightarrow)$ be an MTS and $I = (S_I, s_0^I, A, \rightarrow)$ be a transition system. We have

$$I \models M \iff \llbracket \widehat{I} \rrbracket \subseteq \llbracket \widehat{M} \rrbracket$$

We now define a construction f that builds, for all implementations C of \widehat{M} , a corresponding implementation f(C) of M:

Let $M = (S, s_0, A, \rightarrow, - \rightarrow)$ be a MTS. Let $\widehat{M} = \langle S \times (\{\epsilon\} \cup A), (s_0, \epsilon), \{\epsilon\} \cup A, \varphi, V \rangle$ be the transformation of M defined as above. Let $C = \langle Q, q_0, A, \pi, V' \rangle$ be a MC such that $C \models \widehat{M}$ for some satisfaction relation on IMCs \mathcal{R} .

Define $f(C) = (Q, q_0, A, \rightarrow)$ the Transition System such that $q \xrightarrow{a} q'$ whenever $\pi(q, q') > 0$ and $V'(q') = \{a\}$.

By construction, it is trivial that (1) $f(C) \models M$ for some satisfaction relation on MTS \mathcal{R}' and (2) $C \models \widehat{f(C)}$ for some satisfaction relation on IMCs \mathcal{R}'' . These satisfaction relations are defined as follows: $q \mathcal{R}' s$ whenever there exists $x \in \{\epsilon\} \cup A$ such that $q \mathcal{R}(s, x)$; $q \mathcal{R}''(q', x)$ whenever q = q'.

Now we swith to the proof of Theorem 3.

Let M and M' be two Modal Transition Systems and \widehat{M} and $\widehat{M'}$ be the corresponding IMCs defined as above. We have

$$M \preceq^{th} M' \iff \widehat{M} \preceq^{th} \widehat{M'}$$

Proof. Let M and M' be two MTS, and \widehat{M} and $\widehat{M'}$ the corresponding IMCs.

- ⇒ Suppose that $M \preceq^{th} M'$, and let C be a MC such that $C \models \widehat{M}$. We have by construction $f(C) \models M$, thus $f(C) \models M'$. By Theorem 8, we have $\llbracket \widehat{f(C)} \rrbracket \subseteq \llbracket \widehat{M'} \rrbracket$, and we know that $C \models \widehat{f(C)}$. As a consequence, $C \models \widehat{M'}$.
- \Leftarrow Suppose that $\widehat{M} \leq^{th} \widehat{M'}$, and let I be a TS such that $I \models M$. By Theorem 8, we have $\llbracket \widehat{I} \rrbracket \subseteq \llbracket \widehat{M} \rrbracket$, thus by hypothesis $\llbracket \widehat{I} \rrbracket \subseteq \llbracket \widehat{M'} \rrbracket$. Finaly, by Theorem 8, we obtain that $I \models M'$.

C On Determinism

C.1 Strong Determinism

One can also propose another, slightly more syntactic definition of determinism:

Definition 11 (Strong Determinism). Let $I = \langle Q, q_0, \varphi, A, V \rangle$ be an IMC. I is strongly deterministic *iff for all states* $q, r, s \in Q$, *if there exist a probability distribution* $\sigma \in \varphi(q)$ such that $\sigma(r) > 0$ and a probability distribution $\rho \in \varphi(q)$ such that $\rho(s) > 0$, then $V(r) \neq V(s)$.

Strong determinism differs from Def. 5 in that it requires that, from a given state q, one cannot possibly reach two states r and s with the same set of propositions, even using *two different distributions* (implementations). Checking weak determinism requires solving a cubic number of linear constraints: for each state check the linear constraint of the definition—one per each pair of successors of a state. Checking strong determinism can be done by solving only a quadratic number of linear constraints—one per each successor of each state.

Luckily, due to the convexity of the set of admissible distributions in a state, these two notions coincide for IMCs, so the more efficient, strong determinism can be used in algorithms:

Theorem 9. An IMC I is deterministic iff it is strongly deterministic.

C.2 Proof of Thm. 9

Let $I = \langle Q, q_0, \varphi, A, V \rangle$ be an IMC. *I* is weakly deterministic iff it is strongly deterministic.



Fig. 9: An IMC *I* whose semantics cannot be captured by a deterministic IMC

Proof. It directly follows from the definitions

that strong determinism implies weak determinism. We prove that if an IMC I is not strongly deterministic, then it is not weakly deterministic either.

Let $I = \langle Q, q_0, \varphi, A, V \rangle$ be an IMC. If *I* is not strongly deterministic, there exist two admissible distributions on next states for q: σ and $\rho \in \varphi(q)$ such that $\sigma(r) > 0$, $\sigma(s) = 0$, $\rho(r) = 0$, $\rho(s) > 0$ and V(r) = V(s). In order to prove that *I* is not weakly deterministic, we build a distribution γ that we prove correct w.r.t the interval specifications, i.e. $\gamma \in \varphi(q)$, and such that $\gamma(r) > 0$ and $\gamma(s) > 0$.

Since $\sigma(r) > 0$, there exists a > 0 such that $\varphi(q)(r) = [0, a]$ or [0, a[. Moreover, since $\rho(s) > 0$, there exists b > 0 such that $\varphi(q)(s) = [0, b]$ or [0, b[. Let c = Min(a, b), and define $\gamma(q') = \sigma(q')$ for all $q' \notin \{r, s\}, \gamma(r) = \sigma(r) - c/2$, and $\gamma(s) = c/2$. By construction, $\gamma \in \varphi(q)$ and we have $\gamma(r) > 0$ and $\gamma(s) > 0$. As a consequence, I is not weakly deterministic.

Finally, an IMC I is strongly deterministic iff it is also weakly deterministic.

C.3 Proof of Thm. 4

Let I and I' be two deterministic IMCs. It is equivalent to say that (1) I thoroughly refines I', (2) I weakly refines I' and (3) I strongly refines I'.

Proof. It directly follows the definitions that (3) implies (2) and (2) implies (1). We will prove that (1) implies (2), and then that (2) implies (3).

Let $I_1 = \langle Q^1, q_0^1, \varphi_1, A, V_1 \rangle$ and $I_2 = \langle Q^2, q_0^2, \varphi_2, A, V_2 \rangle$ be two consistent and deterministic IMCs such that $\llbracket I_1 \rrbracket \subseteq \llbracket I_2 \rrbracket$.

First, remark that it is safe to suppose that implementations have the same set of atomic propositions as I_1 and I_2 .

- Let R ⊆ Q¹×Q² such that r R s iff for all MC C and state p of C, p ⊨ r ⇒ p ⊨ s. Since we consider pruned IMCs, there exist implementations for all states. Consider r and s such that r R s.
 - (a) By definition of \mathcal{R} , there exists a MC C and a state p of C such that $p \models r$ and $p \models s$. Thus $V_C(p) = V_1(r)$ and $V_C(p) = V_2(s)$. As a consequence, $V_1(r) = V_2(s)$.
 - (b) Consider $\rho \in \varphi_1(r)$ and build the MC $C = \langle Q^1, q_0^1, \pi, A, V_C \rangle$ such that for all $q \in Q^1$,
 - $V_C(q) = V_1(q);$
 - If $q \neq r$, $\pi(q)$ is any distribution in $\varphi_1(q)$. At least one exists because I_1 is pruned;
 - $\pi(r) = \rho.$

When necessary, we will address state q of C as q_C to differentiate it from state q of I_1 . We will now build the correspondence function δ .

C clearly satisfies I_1 with a satisfaction relation $\mathcal{R}_1 = \text{Identity}$, and $r_C \models r$. By hypothesis, we thus have $r_C \models s$. Consider \mathcal{R}_2 the satisfaction relation such that $r_C \mathcal{R}_2 s$ and δ_2 the corresponding correspondence function. Let $\delta = \delta_2$.

- (c) As a consequence,
 - i. By construction of δ , we have that for all $q \in Q^1$, $\delta(q)$ is a probability distribution;
 - ii. By definition of the satisfaction relation \mathcal{R}_2 , we have that for all $s' \in Q^2$, $\sum_{q_C \in Q^1} \rho(q_C) \cdot \delta_2(q_C)(s') \in \varphi_2(s)(s')$. As a consequence, for all $s' \in Q^2$, $\sum_{q \in Q^1} \rho(q) \cdot \delta(q)(s') \in \varphi_2(s)(s')$.
- 2. Let $r' \in Q^1$ and $s' \in Q^2$ such that $\delta_{r's'} \neq 0$. By definition of C and δ , we have $r'_C \models r'$ and $r'_C \models s'$. We want to prove that for all implementations C' and state p' in C', $p' \models r'$ implies $p' \models s'$.

Suppose that this is not the case. There exists an implementation $C' = \langle P, o, \pi', A, V' \rangle$ and a state p' of C' such that $p' \models r'$ and $p' \not\models s'$. Let \mathcal{R}' be the satisfaction relation witnessing $p' \models r'$.

Consider the MC $\widehat{C} = \langle \widehat{Q^1} \cup \widehat{P}, \widehat{q_0^1}, \widehat{\pi}, A, \widehat{V} \rangle$. Intuitively, $\widehat{Q^1}$ corresponds to C and \widehat{P} to C'. The state r'_C (called $\widehat{r'}$ in \widehat{C}) will be the link between the two and its outgoing transitions will be the ones of p'. Define

- $\begin{array}{l} \ \widehat{\pi}(\widehat{q_1})(\widehat{q_2}) = \pi(q_1)(q_2) \text{ if } q_1, q_2 \in Q^1 \text{ and } \widehat{q_1} \neq \widehat{r'}; \\ \ \widehat{\pi}(\widehat{r'})(q_2) = 0 \text{ if } q_2 \in Q^1; \\ \ \widehat{\pi}(\widehat{q_1})(\widehat{p_2}) = 0 \text{ if } q_1 \in Q^1 \text{ and } \widehat{q_1} \neq \widehat{r'} \text{ and } p_2 \in \widehat{P}; \\ \ \widehat{\pi}(\widehat{r'})(\widehat{p_2}) = \pi'(p')(p_2) \text{ if } p_2 \in P; \\ \ \widehat{\pi}(\widehat{p_1})(\widehat{q_2}) = 0 \text{ if } p_1 \in P \text{ and } q_2 \in Q^1; \end{array}$
- $\widehat{\pi}(\widehat{p_1})(\widehat{p_2}) = \pi'(p_1)(p_2)$ if $p_1, p_2 \in P$;
- $\widehat{V}(\widehat{q}) = V_1(q)$ if $q \in Q^1$;
- $\widehat{V}(\widehat{p_1}) = V'(p_1)$ if $p_1 \in P$.

24 B. Delahaye, K.G. Larsen, A. Legay, M.L. Pedersen, and A. Wąsowski

We want to prove that $\hat{r'}$ satisfies s'. This should imply that $p'_{C'}$ also satisfies s', which is absurd.

Consider the relation $\widehat{\mathcal{R}}$ between the states of \widehat{C} and the states of I_1 defined as follows :

$$\begin{split} \widehat{\mathcal{R}} = &\{ (\widehat{q^{1}}, q^{1'}) \mid (q^{1}_{C}, q^{1'}) \in R_{1} \text{ and } \widehat{q^{1}} \neq \widehat{r'} \} \cup \\ &\{ (\widehat{p^{1}}, q^{1'}) \mid (p^{1}, q^{1'}) \in \mathcal{R'} \} \cup \\ &\{ (\widehat{r'}, q^{1'}) \mid p' \, \mathcal{R'} \, q^{1'} \} \end{split}$$

Intuitively, $\widehat{\mathcal{R}}$ is equal to \mathcal{R}_1 for the states $\widehat{q^1} \in \widehat{Q^1}$, except $\widehat{r'}$, and equal to $\mathcal{R'}$ for the states $\widehat{p^1} \in \widehat{P}$. The states related to $\widehat{r'}$ are the ones that were related to p' with $\mathcal{R'}$.

We will show that $\widehat{\mathcal{R}}$ is a satisfaction relation between \widehat{C} and I_1 .

Let t, w such that $t\hat{\mathcal{R}}w$. For all the pairs where $t \neq r'$, the conditions of the satisfaction relation obviously still hold because they held for \mathcal{R}_1 if $t \in \widehat{Q^1}$ and for \mathcal{R}' otherwise. It remains to check the conditions for the pairs where $t = \widehat{r'}$. Consider w such that $\widehat{r'}\widehat{\mathcal{R}}w$.

- (a) Since r'_C and $p'_{C'}$ are both implementations of r', it is clear that $\widehat{V}(\widehat{r'}) = \widehat{V}(p')$. As $p' \mathcal{R}' w$, we know that $V'(p') = V_1(w)$. Thus, $\widehat{V}(\widehat{r'}) = V_1(w)$.
- (b) Consider the correspondence function $\delta' : P \to (Q^1 \to [0,1])$ given by $p' \mathcal{R}' w$. Let $\hat{\delta} : (\widehat{Q^1} \cup \widehat{P}) \to (Q^1 \to [0,1])$ such that $\hat{\delta}(\widehat{p^1}) = \delta'(p^1)$ whenever $\widehat{p^1} \in \widehat{P}$. Obviously, this is still a probability distribution on Q^1 , and it is such that
 - i. for all $q^1 \in Q^1$, $\sum_{t \in \widehat{Q^1} \cup \widehat{P}} \widehat{\pi}(r')(t) \cdot \widehat{\delta}(t)(q^1) = \sum_{\widehat{p_2} \in \widehat{P}} \pi'(p')(p_2) \cdot \widehat{\delta}(\widehat{p_2})(q^1) = \sum_{p_2 \in P} \pi'(p')(p_2) \cdot \delta'(p_2)(q^1)$. By definition of δ' , this is contained in $\varphi_1(w)(q^1)$.
 - ii. Moreover, if $(\widehat{\pi}(\widehat{r'})(t) \neq 0 \text{ and }) \widehat{\delta}(t)(q^1) \neq 0$, then $t\widehat{\mathcal{R}}q^1$. We only need to consider $t = \widehat{p_1} \in \widehat{P}$ (since otherwise $\widehat{\pi}(\widehat{r'})(t) = 0$) and q^1 such that $\widehat{\delta}(\widehat{p_1})(q^1) \neq 0$. In this case, $\delta'(p_1)(q^1) \neq 0$. As δ' is a witness of $p' \mathcal{R}' w$, it has to be that $p_1 \mathcal{R}' q^1$, which implies, by definition of $\widehat{\mathcal{R}}$, that $t\widehat{\mathcal{R}}q^1$.

Finally \widehat{C} satisfies I_1 , and in particular, $\widehat{r} \models r$. As $r \mathcal{R} s$, it implies that $\widehat{r} \models s$. As a consequence, there exists $\delta'' : (\widehat{Q^1} \cup \widehat{P}) \to (Q^2 \to [0, 1])$ such that, for all $q^2 \in Q^2$,

$$\sum_{t\in\widehat{Q^1}\cup\widehat{P}}\widehat{\pi}(\widehat{r})(t)\cdot\delta''(t)(q^2)\in\varphi_2(s)(q^2)$$

- (A) Consider $q^2 \neq s'$ such that $V_2(q^2) = V_2(s')$. Due to determinism of I_2 , and to the fact that s' is accessible from s, we have $\varphi_2(s)(q^2) = \{0\}$. Since $\widehat{\pi}(\widehat{r})(\widehat{r'}) \neq 0$ and $\widehat{\pi}(\widehat{r})(\widehat{r'}) \cdot \delta''(\widehat{r'})(q^2)$ is part of the sum above, we must have $\delta''(\widehat{r'})(q^2) = 0$.
- (B) Consider q^3 such that $V_2(q^3) \neq V_2(s') = V_1(r')$. It is clear that $\delta''(\hat{r'})(q^3) = 0$ since δ'' is witnessing satisfaction between \hat{C} and I_2 .

(C) Moreover, since $\hat{\pi}(\hat{r})(\hat{r'}) > 0$, we know that $\delta''(\hat{r'})$ is a probability distribution over Q^2 .

According to (A) and (B), the only non-zero value in the distribution in (C) must be $\delta''(\hat{r'})(s')$. Since δ'' is witnessing $\hat{C} \models I_2$, this means that $\hat{r'} \models s'$.

By construction, $\hat{r'}$ and p' only differ by state names. This contradicts the assumption that $p' \not\models s'$. Thus $r' \mathcal{R} s'$, and \mathcal{R} is a weak refinement relation.

Finally, we have by hypothesis that $\llbracket I_1 \rrbracket \subseteq \llbracket I_2 \rrbracket$, which implies that $q_0^1 \mathcal{R} q_0^2$. We thus have (1) implies (2).

We now prove that (2) implies (3).

We start with the following lemma, which is a direct consequence of the notion of determinism. It states that correspondence functions associated to a satisfaction relation for a deterministic IMC are of a particular form.

Lemma 3. Let $I = \langle Q, q_0, \varphi, A, V \rangle$ be a deterministic *IMC*. Let $C = \langle P, p_0, \pi, A, V_C \rangle \in \llbracket I \rrbracket$ and a satisfaction relation \mathcal{R} such that $p_0 \mathcal{R} q_0$. Let $p \in P$ and $q \in Q$ such that $p \mathcal{R} q$, and let δ be the associated correspondence function. We have

$$\forall p' \in P, \pi(p)(p') \neq 0 \Rightarrow$$
$$|\{q' \in Q \mid \delta(p')(q') \neq 0\}| = 1.$$

Obviously, the same holds for correspondence functions associated to refinement relations between deterministic IMCs.

Let $I_1 = \langle Q^1, q_0^1, \varphi_1, A, V_1 \rangle$ and $I_2 = \langle Q^2, q_0^2, \varphi_2, A, V_2 \rangle$ be two deterministic IMCs such that $I_1 \leq I_2$ with a weak refinement relation \mathcal{R} . We prove that \mathcal{R} is in fact a strong refinement relation.

Let $p \in Q^1$ and $q \in Q^2$ such that $p \mathcal{R} q$.

- 1. By hypothesis, $V_1(p) = V_2(q)$;
- 2. We know that for all probability distribution $\sigma \in \varphi_1(p)$, there exists a correspondence function δ^{σ} satisfying the axioms of a (weak) refinement relation. We will build a correspondence function δ^0 that will work for all σ . Let $p' \in Q^1$.
 - If for all $\sigma \in \varphi_1(p)$, we have $\sigma(p') = 0$, then let $\delta^0(p', q') = 0$ for all $q' \in Q^2$;
 - Else, consider $\sigma \in \varphi_1(p)$ such that $\sigma(p') \neq 0$. By hypothesis, there exists a correspondence function δ^{σ} associated to $p \mathcal{R} q$. Let $\delta^0(p') = \delta^{\sigma}(p')$. By Lemma 3, there is a single $q' \in Q^2$ such that $\delta^{\sigma}(p')(q') \neq 0$. Moreover, by definition of δ^{σ} , we know that $\sum_{q'' \in Q^2} \delta^{\sigma}(p')(q'') = 1$, thus $\delta^{\sigma}(p')(q') = 1$. Suppose there exists $\rho \neq \sigma \in \varphi_1(p)$ such that $\rho(p') \neq 0$. Let δ^{ρ} be the associated correspondence function. As for σ , there exists a unique $q'' \in Q^2$ such that $\delta^{\rho}(p')(q'') \neq 0$. Moreover $\delta^{\rho}(p')(q'') = 1$. By definition of δ^{σ} and δ^{ρ} , we have

$$\mu: q^{\prime\prime\prime} \mapsto \sum_{p^{\prime\prime} \in Q^1} (\sigma(p^{\prime\prime}) \cdot \delta^{\sigma}(p^{\prime\prime})(q^{\prime\prime\prime})) \in \varphi_2(q)$$
$$\nu: q^{\prime\prime\prime} \mapsto \sum_{p^{\prime\prime} \in Q^1} (\rho(p^{\prime\prime}) \cdot \delta^{\rho}(p^{\prime\prime})(q^{\prime\prime\prime})) \in \varphi_2(q)$$



Fig. 10: IMCs I_6 , I_7 , and I_8

Moreover, both $\mu(q') > 0$ and $\nu(q'') > 0$. By determinism of I_2 , this implies q' = q''.

As a consequence, we have $\delta^{\sigma}(p') = \delta^{\rho}(p')$, so $\forall \gamma \in \varphi_1(p)$, if $\gamma(p') > 0$, then $\delta^{\gamma}(p') = \delta^0(p')$.

Finally, consider δ^0 defined as above. Let $\sigma \in \varphi_1(p)$. We have

(a) If $\sigma(p') > 0$, then $\delta^0(p') = \delta^{\sigma}(p')$ is a distribution over Q^2 ;

- (b) For all $q' \in Q^2$, $\sum_{p' \in Q^1} (\sigma(p') \cdot \delta^0(p')(q')) = \sum_{p' \in Q^1} (\sigma(p') \cdot \delta^\sigma(p')(q')) \in \varphi_2(q)(q')$ by definition of δ^σ ;
- (c) If $\delta^0(p')(q') > 0$, then there exists $\sigma \in \varphi_1(p)$ such that $\delta^0(p')(q') = \delta^{\sigma}(p'q') > 0$, thus $p' \mathcal{R} q'$ by definition of δ^{σ} .

Finally, \mathcal{R} is a strong refinement relation.

D On Consistency and Common Implementation

Example 2. Consider the three IMCs in Figure 10. We construct a consistency relation \mathcal{R} for k = 3. The triple $(A, 1, \alpha)$ is in the relation \mathcal{R} witnessed by the distribution ρ that assigns $\frac{1}{6}$ to $(B, 2, \beta)$, $\frac{1}{6}$ to $(C, 2, \beta)$, $\frac{1}{3}$ to $(D, 3, \gamma)$, $\frac{1}{6}$ to $(E, 4, \delta)$, and $\frac{1}{6}$ to $(E, 4, \epsilon)$. The triples that are given positive probability by ρ are also in the relation each by the distribution assigning probability 1 to itself. A common implementation $C = \langle P, p_0, \pi, A, V_C \rangle$ can be constructed as follows: $P = \{q | q \in \mathcal{R}\}, p_0 = (A, 1, \alpha), V_C(p)$ is inherited from I_6, I_7 , and I_8 , and $\pi(p)(p') = \rho(p')$, where ρ is the distribution witnessing that $p \in \mathcal{R}$.

To establish a lower bound for common implementation, we propose a reduction from the common implementation problem for modal transition systems (MTS). This latter problem has recently been shown to be EXPTIME-complete when the number of MTS is not known in advance and PTIME-complete otherwise [3]. We first propose the following theorem.

Theorem 10. Let M_i be MTSs for i = 1, ..., k. We have

$$\exists I \forall i : I \models M_i \iff \exists C \forall i : C \models \widehat{M_i},$$

where I is a transition system, C is a Markov Chain and \widehat{M}_i is the IMC obtained with the transformation defined in Section 3.

26

Proof. \Rightarrow : This direction can be proven, by showing that for arbitrary $j \in \{1, \dots, k\}$, $\|\widehat{I}\| \subseteq \|\widehat{M}_i\|$. This is indeed the result of Theorem 8. Now pick a $C \in \|\widehat{I}\|$, and the result follows.

 \Leftarrow : Assume that there exists a C such that $C \models \widehat{M}_i$ for all $i = 1, \ldots, k$. With the transformation defined in section 3, a implementation I for all M_i for all i can be constructed as f(C).

We now prove that the existence of a consistency relation is equivalent to the existence of a common implementation, in the case of k = 2. The above definition and the following theorem extends to general k.

Theorem 11. Let $I_1 = \langle Q_1, q_0^1, \varphi_1, A, V_1 \rangle$ and $I_2 = \langle Q_2, q_0^2, \varphi_2, A, V_2 \rangle$ be IMCs. I_1 and I_2 have a common implementation iff there exists a consistency relation \mathcal{R} such that $q_0^1 \mathcal{R} q_0^2$.

Proof. \Rightarrow : Assume that there exists a MC $C = \langle P, p_0, \pi, A, V_C \rangle$ such that $C \models I_1$ and $C \models I_2$. This implies that there exists satisfaction relations $\mathcal{R}_1 \subseteq P \times Q_1$ and $\mathcal{R}_2 \subseteq P \times Q_2$ such that $p_0 \mathcal{R}_1 q_0^1$ and $p_0 \mathcal{R}_2 q_0^2$.

A relation \mathcal{R} is constructed as $\{(q_1, q_2) | \exists p \in P : p \mathcal{R}_1 q_1 \land p \mathcal{R}_2 q_2\}$. We now prove that \mathcal{R} is a consistency relation relating q_0^1 and q_0^2 ; indeed $(q_0^1, q_0^2) \in \mathcal{R}$ because $p_0 \mathcal{R}_1 q_0^1$ and $p_0 \mathcal{R}_2 q_0^2$. Let $(q_1, q_2) \in \mathcal{R}$ and $p \in P$ such that $p \mathcal{R}_1 q_1$ and $p \mathcal{R}_2 q_2$.

- 1. By \mathcal{R}_1 and \mathcal{R}_2 , $V_1(q_1) = V_C(p) = V_2(q_2)$
- 2. Let δ_1 and δ_2 be the distributions witnessing $p \mathcal{R}_1 q_1$ and $p \mathcal{R}_2 q_2$ (using Definition 9), and let $\rho \in \text{Distr}(Q_1 \times Q_2)$, such that

$$\rho(q_1', q_2') = \sum_{p' \in P \text{ st. } \pi(p)(p') > 0} \frac{\delta_1(p', q_1') \cdot \delta_2(p', q_2')}{\pi(p)(p')}.$$
(2)

Since $\sum_{q'_1 \in Q_1} \sum_{q'_2 \in Q_2} \rho(q'_1, q'_2) = 1$, ρ is indeed a distribution on $Q_1 \times Q_2$. Let $u' \in Q_1$.

$$\begin{split} \sum_{v' \in Q_2} \rho(u',v') &= \sum_{(v' \in Q_2)} \sum_{(p' \in P \text{ st. } \pi(p)(p') > 0)} \frac{\delta_1(p',u') \cdot \delta_2(p',v')}{\pi(p)(p')} \\ &= \sum_{p' \in P \text{ st. } \pi(p)(p') > 0} \delta_1(p',u') \frac{\sum_{v' \in Q_2} \delta_2(p',v')}{\pi(p)(p')} \\ &= \sum_{p' \in P \text{ st. } \pi(p)(p') > 0} \delta_1(p',u') \quad \text{by definition of } \delta_2 \\ &\in \varphi_1(q_1)(u') \quad \text{by definition of } \delta_1. \end{split}$$

Similarly, for all $v' \in Q_2$, $\sum_{u' \in Q_1} \rho(u', v') \in \varphi_2(v)(v')$. 3. Let $q'_1 \in Q_1$ and $q'_2 \in Q_2$ be states such that $\rho(q'_1, q'_2) > 0$. Then at least one term in Eq. (2) is positive. Thus, there exists p' such that $\frac{\delta_1(p',q'_1)\cdot\delta_2(p',q'_2)}{\pi(p)(p')} > 0$. This implies that both factors in the nominator are positive, and by definition of δ_1 and δ_2 , we have that $(p', q'_1) \in \mathcal{R}_1$ and $(p', q'_2) \in \mathcal{R}_2$ and therefore $q'_1 \mathcal{R} q'_2$.

This proves that \mathcal{R} is a consistency relation.

 \Leftarrow : Assume that there exists a consistency relation \mathcal{R} relating q_0^1 and q_0^2 . We now construct a common implementation C, such that $C \models I_1$ and $C \models I_2$; we prove the former first. Let $C = \langle P, p_0, \pi, A, V_C \rangle$ such that

- $P = \{(q_1, q_2) \in Q_1 \times Q_2 \mid q_1 \mathcal{R} q_2\}$ - $p_0 = (q_0^1, q_0^2)$
- $V_C((q_1,q_2)) = V_1(q_1) = V_2(q_2)$ by definition of $\mathcal R$
- For each $(q_1, q_2), (q'_1, q'_2) \in P$, $\pi((q_1, q_2)(q'_1, q'_2)) = \rho(q'_1, q'_2)$, where ρ is the distribution witnessing the membership of (q_1, q_2) in \mathcal{R} .

To show satisfaction between C and I_1 , the relation \mathcal{R}_s is used. It is defined as follows: for all $(u, v) \in P$, $(u, v) \mathcal{R}_s w$ iff u = w. We now show that \mathcal{R}_s is a satisfaction relation between C and I_1 (using Definition 9). Let $(u, v) \in P$ such that $(u, v) \mathcal{R}_s u$.

- 1. By definition of C, $V_C(u, v) = V_1(u)$
- 2. Let δ be the distribution derived as follows: $\delta((u', v'), q_1) = \pi((u, v), (u', v'))$ if $u' = q_1$ and 0 else.
 - (a) Let $(u', v') \in P$.

$$\sum_{q_1 \in Q_1} \delta((u',v'),q_1) = \pi((u,v),(u',v')) \quad \text{by definition}.$$

(b) Let $q_1 \in Q_1$.

$$\begin{split} \sum_{(u',v')\in P} \delta((u',v'),q_1) &= \sum_{(q_1,v')\in P} \pi((u,v),(q_1,v')) \\ &= \sum_{v'\in Q_2} \rho(q_1,v') \\ &\in \varphi_1(u)(q_1) \quad \text{by definition of } \mathcal{R} \end{split}$$

(c) Let $(u', v') \in P$ and $q_1 \in Q_1$ such that $\delta((u', v'), q_1) > 0$. Then $u' = q_1$ and by definition, $(u', v') \mathcal{R}_s q_1$.

 \mathcal{R}_s is a satisfaction relation, and thus $C \models I_1$. Analogously, it can be shown that $C \models I_2$. Finally C is a common implementation of I_1 and I_2 .

Theorem 12. Deciding the existence of a common implementation between 2 IMCs is *PTIME-complete*.

Using the result in [3], we derive the following theorem.

Theorem 13. Deciding the existence of a common implementation between k IMCs is PTIME-complete when k is a constant. Deciding the existence of a common implementation between k IMCs is EXPTIME-complete when k is a variable.

Theorem 14. Given an IMC I and its pruned IMC I^* . Then $[I] = [I^*]$.

- *Proof.* 1. We first prove that $\llbracket I \rrbracket \subseteq \llbracket I^* \rrbracket$. Let $\mathcal{R} \subseteq Q \times Q$ be a consistency relation such that $(q_0, q_0) \in \mathcal{R}$, and let $C = \langle P, p_0, \pi, A, V_C \rangle$ be a MC such that $C \models I$ with satisfaction relation \mathcal{R}_s . We build a satisfaction relation $\mathcal{R}'_s \subseteq P \times Q^*$ where $p \mathcal{R}' q^*$ iff there exists $q \in Q$ such that $p \mathcal{R}_s q$ and $q = q^*$. Let $p \in P, q \in Q$, and $q^* \in Q^*$ such that $(p, q^*) \in \mathcal{R}'$. We now show that \mathcal{R}' is a satisfaction relation between P and I^* .
 - By construction, $V_C(p) = V^*(q^*)$.
 - Let $\delta_1 \in \text{Distr}(P \times Q)$ be the distribution witnessing $p \mathcal{R}_s q$. The distribution $\delta_2 \in \text{Distr}(P \times Q^*)$ is chosen identical to δ_1 . We know that for all $q' \in Q$ such that $\neg \exists \sigma \in \varphi(q')$ then for all $p' \in P$, we have that $\delta_1(p',q') = 0$. To see this, assume the contrary, namely that $\delta_1(p',q') \neq 0$ for a $p' \in P$ and a $q' \in Q$ for which $\neg \exists \sigma \in \varphi(q')$; then $p' \mathcal{R}_s q'$. By the definition af satisfaction, q' allows a distribution, which is a contradiction.

Since δ_1 satisfies the axioms of satisfaction, then δ_2 also satisfies them.

- 2. To show that $\llbracket I^* \rrbracket \subseteq \llbracket I \rrbracket$, we use the same reasoning as above.
 - By mutual inclusion, $\llbracket I \rrbracket = \llbracket I^* \rrbracket$.

Example 3. Consider the IMC I in Figure 11a. Building a consistency relation, we see that (1, 1) is in the relation witnessed by the distribution assigning probability 0.8 to (2, 2) and 0.2 to (4, 4). This probability distribution "avoids" the inconsistent state (3, 3); this state does not admit a probability distribution. Likewise, (2, 2) and (3, 3) are in the relation, witnessed by the distributions that gives probability 1 to (2, 2) and (3, 3), respectively.

 I^* is shown in Figure 11b.



Fig. 11: An IMC and its pruned version