Compositional Design Methodology with Constraint Markov Chains

Benoit Caillaud, Benoît Delahaye, Kim Guldstrand Larsen, Axel Legay, Mikkel L. Pedersen, Andrzej Wasowski

INRIA

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

Compositional Design Methodology with Constraint Markov Chains

Benoît Caillaud, INRIA / IRISA, France
— Benoît Delahaye, Université de Rennes 1 / IRISA, France
— Kim G. Larsen, Aalborg University, Denmark
— Axel Legay, INRIA / IRISA, France
— Mikkel L. Pedersen, Aalborg University, Denmark
— Andrzej Wąsowski, IT University of Copenhagen, Denmark

N° 6993

Juillet 2009

Thèmes COM et SYM

apport de recherche

ISSN 0249-6399 ISRN INRIA/RR--6993--FR+ENG

INSTITUT NATIONAL
DE RECHERCHE
EN INFORMATIQUE
ET EN AUTOMATIQUE

INRIA

centre de recherche
RENNES - BRETAGNE ATLANTIQUE

Compositional Design Methodology with Constraint Markov Chains

Benoît Caillaud, INRIA / IRISA, France
, Benoît Delahaye, Université de Rennes 1 / IRISA, France
, Kim G. Larsen, Aalborg University, Denmark
, Axel Legay, INRIA / IRISA, France
, Mikkel L. Pedersen, Aalborg University, Denmark
, Andrzej Wąsowski, IT University of Copenhagen, Denmark

Thèmes COM et SYM — Systèmes communicants et Systèmes symboliques
Équipe-Projet S4

Rapport de recherche n° 6993 — Juillet 2009 — 28 pages

Abstract: A specification theory combines notions of specification and implementation with a satisfaction relation, a refinement relation and a set of operators that together support stepwise design. We propose a new abstraction, Constraint Markov Chains, and use it to construct a specification theory for Markov Chains. Constraint Markov Chains generalize previously known abstractions by allowing arbitrary constraints on probability distributions. Our theory is the first specification theory for Markov Chains closed under conjunction, parallel composition and synchronization. Moreover, all the operators and relations introduced are computable.

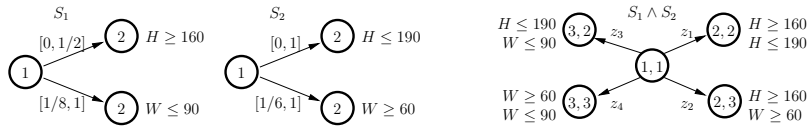
Key-words: Compositional Reasoning, Probability, CMC

Centre de recherche INRIA Rennes – Bretagne Atlantique
IRISA, Campus universitaire de Beaulieu, 35042 Rennes Cedex
Téléphone : +33 2 99 84 71 00 — Télécopie : +33 2 99 84 71 71

Méthode de Conception Compositionelle avec les Chaines de Markov avec Contraintes

Résumé : Une théorie de spécification combine les notions de spécification et implémentation avec des relations de satisfaction et raffinement, et un ensemble d'opérateurs qui permettent une conception incrémentale. Nous proposons une nouvelle abstraction, les chaînes de Markov avec contraintes, et les utilisons pour construire une théorie de spécification pour les chaînes de Markov. Les chaînes de Markov avec contraintes généralisentd'autres abstractions plus anciennes en autorisant des contraintes arbitraires sur les distributions de probabilité. Notre théorie est la première théorie de spécification pour les chaînes de Markov close sous conjonction, composition parallèle et synchronisation. De plus, tous les opérateurs et relations introduits sont calculables.

Mots-clés : Raisonnement Compositionel, Probabilités, CMC



(a) IMCs S_1 and S_2 (b) CMC $S_1 \wedge S_2$

Figure 1: IMCs: non-closure under conjunction

1 Introduction

In this paper we introduce *Constraint Markov Chains* (CMCs) as a foundational specification formalism for component-based development of probabilistic systems. In particular, we provide constructs on CMCs supporting refinement, consistency checking, logical as well as structural composition of specifications – all indispensable ingredients for a compositional design methodology.

Over the years several process algebraic frameworks have been proposed for describing and analysing probabilistic systems based on Markov Chains and Markov Decision Processes, e.g. [12, 1, 20]. Also, a variety of probabilistic logics have been proposed for expressing properties of such systems, e.g. PCTL [9]. Both approaches support refinement between specifications using various notions of probabilistic (bi)simulation (e.g., [8, 15]) and logical entailment (e.g. [11]). Whereas the process algebraic approach favors structural composition (e.g. parallel composition), the logical approach favors logical combinations (e.g. logical conjunction). Neither of the two approaches supports both structural and logical composition.

For functional analysis the notion of Modal Transition Systems (MTS) [17] provides a useful specification formalism supporting refinement as well as logical and structural composition and with recent applications to Interface Theories [18, 22]. Generalizing the notion of Modal Transition Systems to the non-functional analysis of probabilistic systems, the formalism of Interval Markov Chains (IMCs) was introduced in [15] with notions of satisfaction and refinement generalizing probabilistic bisimulation. Informally, an IMC extends the notion of Markov Chains by having transitions labelled by *intervals* (open or closed) of allowed probabilities rather than individual probabilities.

In more recent work, IMCs have been subject to further study: a weaker (yet sound) refinement for IMCs is introduced [8], and model checking procedures for PCTL for such systems are considered [24, 8, 6]. In a very recent work [14] a composition operation has been studied for IMCs augmented with may and must transitions very much in the spirit of [17].

However, the expressive power of IMCs is inadequate to support both logical and structural composition. To see this, consider two IMCs, S_1 and S_2, in Figure 1 specifying different probability constraints related to the height (H) and weight (W) of a given random person. Attempting to express the conjunction $S_1 \wedge S_2$ as an IMC by simple intersection of bounds gives $z_1 \leq 1/2$, $1/6 \leq z_2 \leq 1/2$, $1/8 \leq z_3$ and $1/6 \leq z_4$. However, this naive construction is too coarse and does not adequately capture conjunction: whereas $(z_1, z_2, z_3, z_4) = (1/2, 1/6, 1/8, 5/24)$ is a solution to the above constraints the resulting overall probability of reaching a state satisfying H$\geq$ 160, i.e. $z_1 + z_2 = 2/3$, clearly violates the upper bound $1/2$ specified in S_1. What is needed is the ability to express dependencies between the probabilities z_1, z_2, z_3, z_4 besides that of being a probability distribution, i.e. $z_1 + z_2 + z_3 + z_4 = 1$.

Obviously, the correct conjunctive combination is expressed by the three constraints $z_1 + z_2 \leq 1/2, 1/8 \leq z_3 + z_4, 1/6 \leq z_2 + z_4$, exceeding the expressive power of IMCs. Similarly, simple examples demonstrate that IMCs are also not closed under parallel composition.

Constraint Markov Chains (CMCs) are a further extension of Markov Chains allowing arbitrary constraints on the next-state probabilities from any state. Whereas linear constraints suffice for closure under conjunction, polynomial constraints are, as we shall see, necessary for closure under parallel composition. We define notions of satisfaction and (weak) refinement for CMCs conservatively extending similar notions for IMCs. In particular, as a main theorem, we prove that for deterministic CMCs the notion of weak refinement is complete with respect to the inclusion of implementation-sets. In addition, we provide a construction, which for any CMC S returns a deterministic CMC $\rho(S)$ containing S with respect to weak refinement. Finally, we show that refinement between CMCs with polynomial constraints can be decided in essentially single exponential time.

2 Constraint Markov Chains

Let A, B be sets of propositions with $A \subseteq B$. The *restriction of $T \subseteq B$ to A* is given by $T{\downarrow_A} \equiv T \cap A$. If $T \subseteq 2^B$, then $T{\downarrow_A} \equiv \{W{\downarrow_A} \mid W \in T\}$. For $V \subseteq A$ define the *extension of V to B* as $T{\uparrow^B} \equiv \{W \subseteq B \mid W{\downarrow_A} = T\}$, so the set of sets whose restriction to A is T. Lift it to sets of sets as follows: if $T \subseteq 2^A$ then $T{\uparrow^B} \equiv \{W \subseteq B \mid W{\downarrow_A} \in T\}$. Let $M \in [0,1]^{n \times k}$ be a matrix and $x \in [0,1]^{1 \times k}$ be a vector. We write M_{ij} for the cell in ith row and jth column of M, M_p for the pth row of M, and x_i for the ith element of x. Finally, M is a *correspondence matrix* iff $0 \leq \sum_{j=1}^{k} \Delta_{ij} \leq 1$ for all $1 \leq i \leq n$.

Definition 1 *A* Markov Chain (MC in short) *is a tuple $\langle \{1, \ldots, n\}, o, M, A, V \rangle$, where $\{1, \ldots, n\}$ is a set of states containing the initial state o, A is a set of atomic propositions, $V : \{1, \ldots, n\} \to 2^A$ is a state valuation, and $M \in [0,1]^{n \times n}$ is a probability transition matrix: $\sum_{j=1}^{n} M_{ij} = 1$ for $1 \leq i \leq n$.*

We now introduce *Constraint Markov Chains* (CMCs in short), a finite representation for a possibly infinite set of MCs. Roughly speaking, CMCs generalize MCs in that, instead of specifying a concrete transition matrix, they only constrain probability values in the matrix. Constraints are modeled using a *characteristic function*, which for a given source state and a distribution of probabilities of leaving the state evaluates to 1 iff the distribution is permitted by the specification. Similarly, instead of a concrete valuation function for each state, a *constraint on valuations* is used. Here, a valuation is permitted iff it is contained in the set of admissible valuations of the specification.

Definition 2 *A* Constraint Markov Chain *is a tuple $S = \langle \{1, \ldots, k\}, o, \varphi, A, V \rangle$, where $\{1, \ldots, k\}$ is a set of states containing the initial state o, A is a set of atomic propositions, $V : \{1, \ldots, k\} \to 2^{2^A}$ is a set of admissible state valuations. and $\varphi : \{1, \ldots, k\} \to [0,1]^k \to \{0,1\}$ is a* constraint function *such that if $\varphi(j)(x) = 1$ then the x vector is a probability distribution: $0 \leq x_i \leq 1$ and $\sum_{i=1}^{k} x_i = 1$.*

An *Interval Markov Chain* (IMC in short) [15] is a CMC whose constraint functions are represented by intervals, so for all $1 \leq i \leq k$ there exist constants α_i, β_i such that $\varphi(j)(x) = 1$ iff $x_i \in [\alpha_i, \beta_i]$.

EXAMPLE 1. *Two parties, a customer and a vendor, are discussing a design of a relay for an optical telecommunication network. The relay is designed to amplify an optic signal transmitted over a long distance over an optic fiber. The relay should have several modes of operation, modeled by four dynamically changing properties and specified by atomic propositions a, b, c, and e (see Figure 2a).*

The customer presents CMC S_1 (Figure 2b) specifying the admissible behavior of the relay from their point of view. States are labeled with formulas characterizing sets of valuations. For instance, "$(a + b + c \geq 2) \wedge (e = 0)$" at state 2 of S_1 represents $V_1(2) = \{\{a, b\}, \{b, c\}, \{a, c\}, \{a, b, c\}\}$, where a, b, c, and e range over Booleans. State 1 specifies a standby mode, where no signal is emitted and only marginal power is consumed. State 2 is the high power mode, offering a high signal/noise ratio, and hence a high bitrate and low error rate, at the expense of a high power consumption. State 3 is the low power mode, with a low power consumption, low bitrate and high error rate. The customer prescribes that the probability of the high power mode (state 2) is higher than 0.7.

The vendor replies with CMC S_2 (Figure 2c), which represents possible relays that they can build. Because of thermal limitations, the low power mode has a probability higher than 0.2.

A state u of S is *reachable* from a state i if there exists a probability distribution, or a vector $x \in [0, 1]^k$, with a nonzero probability x_u, which satisfies $\varphi(i)(x)$. A CMC S is *deterministic* iff for every state i, states reachable from i have pairwise disjoint admissible valuations:

Definition 3 *Let $S = \langle\{1, \ldots, k\}, o, \varphi, A, V\rangle$ be a CMC. S is* deterministic *iff for all states $i, u, v \in \{1, \ldots, k\}$, if there exists $x \in [0, 1]^k$ such that $(\varphi(i)(x) \wedge (x_u \neq 0))$ and $y \in [0, 1]^k$ such that $(\varphi(i)(y)(\wedge y_v \neq 0))$, then we have that $V(u) \cap V(v) = \emptyset$.*

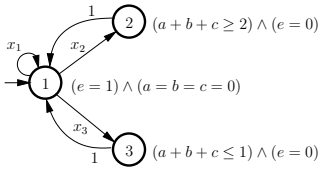
In our example both S_1 and S_2 are deterministic specifications. In particular states 2 and 3, reachable from 1 in both CMCs, have disjoint constraints on valuations (see Figure 2).

We relate CMC specifications to MCs implementing them, by extending the definition of satisfaction presented in [15] to observe the valuations constraints and the full-fledged constraint functions. Crucially, like [15], we abstract from syntactic structure of transitions—a single transition in the implementation MC can contribute to satisfaction of more than one transition in the specification, by distributing its probability mass against several transitions. Similarly many MC transitions can contribute to satisfaction of just one specification transition. This redistribution of probability mass is described by correspondence matrices. Consider the following example:

EXAMPLE 2. *We illustrate the concept of correspondence matrix between Specification S_1 (given in Figure. 2b) and Implementation P_2 (given in Figure 2e). The CMC S_1 has three outgoing transitions from state 1 but, due to constraint function in 1, the transition labeled with x_1 cannot be taken (the constraint implies $x_1 = 0$). The probability mass going from state 1 to states 2 and 3 in P_2 corresponds to the probability allowed by S_1 from its state 1 to its state 2; The redistribution is done with the help of the matrix Δ given in Figure 2h. The ith column in Δ describes how big fraction of each transition probability (for transitions leaving 1) is associated with probability x_i in S_2. Observe that the constraint function $\varphi_1(1)(0, 0.8, 0.2) = \varphi_1(1)((0, 0.7, 0.1, 0.2) \times \Delta)$ is satisfied.*

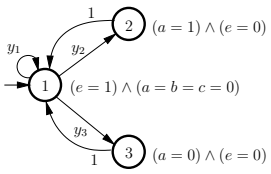
a	ber $\leq 10^{-9}$	The bit error rate is less than 1 per billion bits transmitted.
b	br > 10Gbits/s	The bit rate is higher than 10 Gbits/s.
c	$P < 10$W	Power consumption is less than 10 W.
e	Standby	The relay is not transmitting.

(a) Atomic propositions in the optic relay specifications



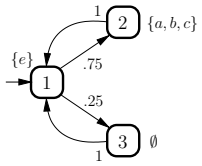
$\varphi_1(1)(x) \equiv (x_1 = 0) \wedge (x_2 \geq 0.7) \wedge (x_2 + x_3 = 1)$

(b) CMC S_1, the customer specification of the optic relay

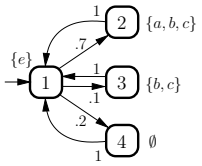


$\varphi_2(1)(y) \equiv (y_1 = 0) \wedge (y_3 \geq 0.2) \wedge (y_2 + y_3 = 1)$

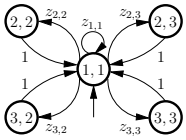
(c) The manufacturer specification, S_2, of the optic relay



(d) Markov Chain P_1 satisfying S_1 and S_2

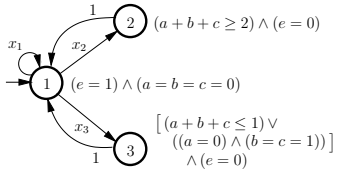


(e) Another Markov Chain P_2 satisfying S_1 and S_2



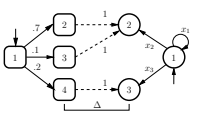
$\varphi_3(1,1)(Z) \equiv \big[(\forall j,\ z_{1,j} = 0) \wedge (z_{2,2} + z_{2,3} \geq 0.7)$
$\wedge\ (z_{2,2} + z_{2,3} + z_{3,2} + z_{3,3} = 1)\big]$
$\wedge\ \big[(\forall i,\ z_{i,1} = 0) \wedge (z_{2,3} + z_{3,3} \geq 0.2)\big]$

(f) Conjunction S_3 of S_1 and S_2. Constraints on propositions, pairwise conjunctions (intersections) of constraints of S_1 and S_2, are left out to avoid clutter



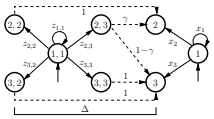
$\varphi_4(1)(x) \equiv (x_1 = 0) \wedge (x_2 \geq 0.7)$
$\wedge\ (x_3 \geq 0.2) \wedge (x_2 + x_3 = 1)$

(g) CMC S_4 generalizing S_3, so $S_3 \preceq S_4$



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

(h) Correspondence for initial states of P_2 and S_1



$$\Delta = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & \gamma & 1-\gamma \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{bmatrix}$$

(i) Weak refinement for initial states of S_3 and S_4

Figure 2: Examples

Definition 4 *Let $P = \langle \{1,\dots,n\}, o_P, M, A_P, V_P\rangle$ be a MC and $S = \langle \{1,\dots,k\}, o_S, \varphi, A_S, V_S\rangle$ be a CMC with $A_s \subseteq A_p$. Then $\mathcal{R} \subseteq \{1,\dots,n\} \times \{1,\dots,k\}$ is a* satisfaction relation *between states of P and S iff whenever $p\,\mathcal{R}\,u$ then (1) $V_P(p)\downarrow_{A_S} \in V_S(u)$, and (2) there exists a correspondence matrix $\Delta \in [0,1]^{n\times k}$ such that (a) for all $1 \le p' \le n$ with $M_{pp'} \neq 0$, $\sum_{j=1}^{k} \Delta_{p'j} = 1$; (b) $\varphi(u)(M_p \times \Delta)$ holds and (c) if $\Delta_{p'u'} \neq 0$ then $p'\,\mathcal{R}\,u'$.*

We write $P \models S$ iff there exists a satisfaction relation relating o_P and o_S, and call P an *implementation* of S. The set of all implementations of S is given by $[\![S]\!] \equiv \{P \mid P \models S\}$. Rows of Δ that correspond to reachable states of P always sum up to 1. This is to guarantee that the entire probability mass of implementation transitions is allocated. For unreachable states, we leave the corresponding rows in Δ unconstrained. P may have a richer alphabet than S, in order to facilitate abstract modeling: this way an implementation can maintain local information using an internal variable.

Remark 1 *Our semantics for CMCs follows the Markov Decision process (MDP in short) semantics tradition [24, 6]. In the literature, the MDP semantic is opposed to the Uncertain Markov Chain (UMC in short) semantics where the probability distribution from each state is fixed a priori.*

3 Consistency, Refinement and Conjunction

We now study the notions of consistency, refinement, and conjunction for Constraint Markov Chains.

3.1 Consistency

A CMC S is *consistent* if it admits at least one implementation. We now discuss how to decide consistency. A state u of S is *valuation consistent* iff $V(u) \neq \emptyset$; it is *constraint consistent* iff there exists a probability distribution vector $x \in [0,1]^{1\times k}$ such that $\varphi(u)(x) = 1$. It is easy to see that if *each state* of S is both valuation and constraint consistent then S is also consistent. However, inconsistency of a state does not imply inconsistency of the specification. The operations presented later in this paper may introduce inconsistent states, leaving a question if a resulting CMC is consistent. In order to decide whether S is inconsistent, local inconsistencies are propagated throughout the entire state-space using a *pruning operator* β that removes inconsistent states from S. The result $\beta(S)$ is a new CMC, which may still contain some inconsistent states. The operator is applied iteratively, until a fixpoint is reached. If the resulting CMC $\beta^*(S)$ contains at least one state then S is consistent. Also S has the same models as $\beta^*(S)$.

We define β formally. Let $S = \langle \{1,\dots,k\}, o, \varphi, A, V\rangle$. If o is locally inconsistent then let $\beta(S) = \emptyset$. If S does not contain inconsistent states then $\beta(S) = S$. Else proceed in two steps. First for $k' < k$ define a function $\nu : \{1,\dots,k\} \to \{\bot, 1,\dots,k'\}$, which will remove inconsistent states. All locally inconsistent states are mapped to $\bot$. For all $1 \le i \le k$ take $\nu(i) = \bot$ iff $[(V(i) = \emptyset) \vee (\forall x \in [0,1]^k,\ \varphi(i)(x) = 0)]$. All remaining states are mapped injectively into $\{1,\dots,k'\}$: $\nu(i) \neq \bot \implies \forall j \neq i,\ \nu(j) \neq \nu(i)$. Then let $\beta(S) = \langle \{1,\dots,k'\}, \nu(o), \varphi', A, V'\rangle$, where $V'(i) = V(\nu^{-1}(i))$ and for all $1 \le j \le k'$ the constraint $\varphi'(j)(y_1,\dots,y_{k'})$ is:

$\exists x_1, \ldots, x_k$ s.t.

$$\Big[\nu(q) = \bot \implies x_q = 0\Big] \text{ and } \big[\forall 1 \leq l \leq k',\ y_l = x_{\nu^{-1}(l)}\big]$$
$$\text{and } \big[\varphi(\nu^{-1}(j))(x_1, \ldots, x_k)\big] \quad .$$

The constraint makes the locally inconsistent states unreachable, and then $\bot$ is dropped as a state.

Theorem 1 *Let $S = \langle\{1, \ldots, k\}, o, \varphi, A, V\rangle\}$ be a CMC and $\beta^*(S) = \lim_{n\to\infty} \beta^n(S)$ be the fixpoint of β. For any MC P, we have (1) $P \models S \iff P \models \beta(S)$ and (2) $[\![S]\!] = [\![\beta^*(S)]\!]$.*

3.2 Refinement

Refinement is a concept that allows to "compare" two specifications. Roughly speaking, if S_1 refines S_2, then any model of S_1 should also be a model of S_2. In [15], Jonsson and Larsen have proposed a notion of strong refinement between IMCs. This definition extends to CMCs in the following way.

Definition 5 *Let $S_1 = \langle\{1, \ldots, k_1\}, o_1, \varphi_1, A_1, V_1\rangle$ and $S_2 = \langle\{1, \ldots, k_2\}, o_2, \varphi_2, A_2, V_2\rangle$ be CMCs with $A_2 \subseteq A_1$. The relation $\mathcal{R} \subseteq \{1, \ldots, k_1\} \times \{1, \ldots, k_2\}$ is a* strong refinement relation *between states of S_1 and S_2 iff whenever $v\,\mathcal{R}\,u$ then (1) $V_1(v)\downarrow_{A_2} \subseteq V_2(u)$ and (2) there exists a correspondence matrix $\Delta \in [0,1]^{k_1 \times k_2}$ such that for all probability distribution vectors $x \in [0,1]^{1\times k_1}$ if $\varphi_1(v)(x)$ holds then (a) $x_i \neq 0 \Rightarrow \sum_{j=1}^{k_2} \Delta_{ij} = 1$; (b) $\varphi_2(u)(x \times \Delta)$ holds and (c) if $\Delta_{v'u'} \neq 0$ then $v'\,\mathcal{R}\,u'$. We say that S_1 strongly refines S_2 iff $o_1\,\mathcal{R}\,o_2$.*

It is easy to see that strong refinement implies implementation set inclusion. However, the converse is not true. The strong refinement imposes a "fixed-in-advance" witness matrix regardless of the probability distribution satisfying the constraint function. We propose a *weak refinement* that is complete for deterministic CMCs. Our definition generalizes the one proposed in [8] for IMCs.

Definition 6 *Let $S_1 = \langle\{1, \ldots, k_1\}, o_1, \varphi_1, A_1, V_1\rangle$ and $S_2 = \langle\{1, \ldots, k_2\}, o_2, \varphi_2, A_2, V_2\rangle$ be two CMCs, with $A_2 \subseteq A_1$. Then $\mathcal{R} \subseteq \{1, \ldots, k_1\} \times \{1, \ldots, k_2\}$ is a* weak refinement relation *iff whenever $v\,\mathcal{R}\,u$ then (1) $V_1(v)\downarrow_{A_2} \subseteq V_2(u)$ and (2) for any probability distribution vector $x \in [0,1]^{1\times k_1}$ such that $\varphi_1(v)(x)$, there exists a matrix $\Delta \in [0,1]^{k_1 \times k_2}$ such that (a) for all S_1 states $1 \leq i \leq k_1$, $x_i \neq 0 \implies \sum_{j=1}^{k_2} \Delta_{ij} = 1$; (b) $\varphi_2(u)(x \times \Delta)$ and (c) $\Delta_{v'u'} \neq 0 \Rightarrow v'\,\mathcal{R}\,u'$. We say that CMC S_1 (weakly) refines S_2, written $S_1 \preceq S_2$, iff $o_1\,\mathcal{R}\,o_2$.*

It is easy to see that the weak refinement implies implementation set inclusion (see Appendix A.8.1 for a formal proof). Showing the converse is more involved. We postpone it to Section 5.

EXAMPLE 3. *Figure 2i illustrates a family of correspondence matrices parameterized by γ witnessing the weak refinement between initial states of S_3 and S_4 (defined in Figure 2). The actual matrix used in proving the weak refinement depends on the probability distribution vector z that satisfies the constraint function φ_3 of state $(1,1)$. Take $\gamma = \frac{0.7-z_{22}}{z_{23}}$ if $z_{22} \leq 0.7$ and $\gamma = \frac{0.8-z_{22}}{z_{23}}$ otherwise. It is easy to see that if $\varphi_3((1,1))(z)$ holds, then $\varphi_4(1)(z \times \Delta)$ holds.*

3.3 Conjunction

Conjunction is a useful operation combining requirements of several specifications.

Definition 7 *Let* $S_1 = \langle\{1,\dots,k_1\}, o_1, \varphi_1, A_1, V_1\rangle$ *and* $S_2 = \langle\{1,\dots,k_2\}, o_2, \varphi_2, A_2, V_2\rangle$ *be two CMCs. The conjunction of* S_1 *and* S_2*, written* $S_1 \wedge S_2$*, is the CMC* $S = \langle\{1,\dots,k_1\}\times\{1,\dots,k_2\}, (o_1,o_2), \varphi, A, V\rangle$ *with* $A = A_1 \cup A_2$*,* $V((u,v)) = V_1(u)\uparrow^A \cap V_2(v)\uparrow^A$*, and*

$$\varphi((u,v))(x_{1,1}, x_{1,2}, \dots, x_{2,1}, \dots, x_{k_1,k_2}) \equiv$$

$$\varphi_1(u)(\sum_{j=1}^{k_2} x_{1,j}, \dots, \sum_{j=1}^{k_2} x_{k_1,j}) \wedge \varphi_2(v)(\sum_{i=1}^{k_1} x_{i,1}, \dots, \sum_{i=1}^{k_1} x_{i,k_2}).$$

Conjunction is an operation that conserves determinism and may introduce inconsistent states (see Example 3 below) and thus a use of conjunction should normally be followed by applying the pruning operator β. As we already said in the introduction, the result of conjoining two IMCs is not an IMC in general, but a CMC whose constraint functions are linear.

EXAMPLE 4. *Figure 2f depicts a CMC* S_3 *expressing the conjunction of IMCs* S_1 *and* S_2 *(see Figures 2b–2c). The constraint* $z_{2,3} + z_{3,3} \geq 0.2$ *in state* $(1,1)$ *cannot be expressed as an interval.*

Finally, the following theorem shows the conjunction of two specifications coincides with their greatest lower bound with respect to the weak refinement (also called *shared refinement*).

Theorem 2 *Let* S_1*,* S_2 *and* S_3 *be three CMCs. We have* $((S_1 \wedge S_2) \preceq S_1) \wedge ((S_1 \wedge S_2) \preceq S_2)$ *and* $(S_3 \preceq S_1) \wedge (S_3 \preceq S_2) \Rightarrow S_3 \preceq (S_1 \wedge S_2)$.

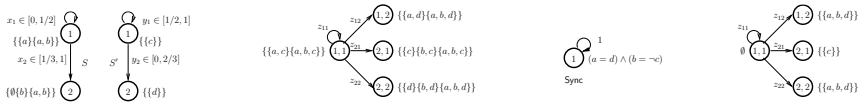
4 Compositional Reasoning

Let us now turn to studying composition of CMCs. We start by discussing how systems and specifications can be composed in a non-synchronizing way, then we introduce a notion of synchronization. The non-synchronizing *independent* composition is largely just a product of two MCs (or CMCs). We begin with composition of MCs.

Definition 8 *Let* $S_1 = \langle\{1,\dots,n_1\}, o_1, M', A_1, V_1\rangle$ *and* $S_2 = \langle\{1,\dots,n_2\}, o_2, M'', A_2, V_2\rangle$ *be two MCs and suppose* $A_1 \cap A_2 = \emptyset$*. The parallel composition of* P_1 *and* P_2 *is the MC* $P_1 \parallel P_2 = \langle\{1,\dots,n_1\}\times\{1,\dots,n_2\}, (o_1,o_2), M, A_1 \cup A_2, V\rangle$ *where:* $M \in [0,1]^{(n_1\times n_2)\times(n_1\times n_2)}$ *is such that* $M_{(p,q)(r,s)} = M'_{pr} \cdot M''_{qs}$*; and* $V((p,q)) = V_1(p) \cup V_2(q)$.

We now define independent parallel composition between CMCs.

Definition 9 *Let* $S_1 = \langle\{1,\dots,k_1\}, o_1, \varphi_1, A_1, V_1\rangle$ *and* $S_2 = \langle\{1,\dots,k_2\}, o_2, \varphi_2, A_2, V_2\rangle$ *be CMCs with* $A_1 \cap A_2 = \emptyset$*. The parallel composition of* S_1 *and* S_2 *is the CMC* $S_1 \parallel S_2 = \langle\{1,\dots,k_1\}\times\{1,\dots,k_2\}, (o_1,o_2), \varphi, A_1 \cup A_2, V\rangle$*, where* $\varphi((u,v))(z_{1,1}, z_{1,2}, \dots z_{2,1}, \dots, z_{k_1,k_2}) = \exists x_1,\dots,x_{k_1}, y_1,\dots,y_{k_2} \in [0,1]$ *such that* $\forall (i,j) \in \{1,\dots,k_1\}\times\{1,\dots,k_2\}$ *we have* $z_{i,j} = x_i \cdot y_j$ *and* $\varphi_1(u)(x_1, \dots, x_{k_1}) = \varphi_2(v)(y_1,\dots,y_{k_2}) = 1$*; Finally,* $V((u,v)) = \{Q_1 \cup Q_2 \mid Q_1 \in V_1(u), Q_2 \in V_2(v)\}$.



(a) Two CMCs S and S' (b) $S \parallel S'$ (c) Synchronizer Sync (d) $(S \parallel S') \wedge$ Sync

Figure 3: Synchronization

Composition preserves determinism. It is worth mentioning that IMCs are not closed under composition. Consider IMCs S and S' given in Figure 3a and their composition $S \parallel S'$ given in Figure 3b. Assume first that $S \parallel S'$ is an IMC. As a variable z_{ij} is the product of two variables x_i and y_j, if $S \parallel S'$ is an IMC, then one can show that the interval for z_{ij} is obtained by computing the products of the bounds of the intervals over which x_i and y_j range. Hence, we can show that $z_{11} \in [0, 1/2], z_{12} \in [0, 1/3], z_{21} \in [1/6, 1], z_{22} \in [0, 2/3]$. Let $[a, b]$ be the interval for the constraint z_{ij}, it is easy to see that there exists implementations I_1 of S_1 and I_2 of S_2 such that $I_1 \parallel I_2$ satisfies the constrain $z_{ij} = a$ (resp. $z_{ij} = b$). However, while each bound of each interval can be satisfied independently, some points in the polytope defined by the intervals and the constraint $\sum z_{ij} = 1$ cannot be reached. As an example, consider $z_{11} = 0, z_{12} = 1/3, z_{21} = 1/3, z_{22} = 1/3$. It is clearly inside the polytope, but one cannot find an implementation I of $S \parallel S'$ satisfying the constraints given by the parallel composition. Indeed, having $z_{11} = 0$ implies that $x_1 = 0$ and thus that $z_{12} = 0$.

Theorem 3 *If S'_1, S'_2, S_1, S_2 are CMCs then $S'_1 \preceq S_1 \wedge S'_2 \preceq S_2$ implies $S'_1 \parallel S'_2 \preceq S_1 \parallel S_2$, so the weak refinement is a precongruence with respect to parallel composition. Consequently, for any MCs P_1 and P_2 we have that $P_1 \models S_1 \wedge P_2 \models S_2$ implies $P_1 \parallel P_2 \models S_1 \parallel S_2$.*

As alphabets of composed CMCs have to be disjoint, the composition does not synchronize the components on state valuations like it is typically done for other (non-probabilistic) models. However, synchronization can be introduced by conjoining the composition with a *synchronizer*—a single-state CMC whose constraint function relates the atomic propositions of the composed CMCs.

EXAMPLE 5. *The CMC $S \parallel S'$ of Figure 3b is synchronized with the synchronizer* Sync *given in Figure 3c.* Sync *removes from $S \parallel S'$ all the valuations that do not satisfy $(a = d) \wedge (b = \neg c)$. The resulting CMC is given in Figure 3d. Observe that an inconsistency appears in State $(1, 1)$. This is because there is no implementations of the two CMCs that can synchronize in the prescribed way. In general inconsistencies like this one can be uncovered by applying the pruning operator, which would return an empty specification. So synchronizers enable discovery of incompatibilities between component specifications in the same way as it is known for non-probabilistic specification models.*

The following theorem states that synchronization is associative with respect to composition.

Theorem 4 *Let S_1, S_2 and S_3 be three CMCs with pairwise disjoint sets of propositions A_1, A_2 and A_3. Let Sync_{123} be a synchronizer over $A_1 \cup A_2 \cup A_3$ and let*

Sync_{12} *be the same synchronizer with its set of propositions restricted to* $A_1 \cup A_2$*. The following holds* $[\![((S_1 \parallel S_2) \wedge \mathsf{Sync}_{12}) \parallel S_3] \wedge \mathsf{Sync}_{123}]\!] = [\![(S_1 \parallel S_2 \parallel S_3) \wedge S_{123}]\!]$.

5 Deterministic CMCs

Clearly, if all implementations of a specification S_1 are also implementations of a specification S_2, then a designer can consider the former to be a proper strengthening of the latter. Indeed, S_1 specifies implementations that break no assumptions that can be made about implementations of S_2. Thus implementation set inclusion *is* a desirable refinement for specifications. Unfortunately, it is not directly computable. However, as we have already said, the weak refinement soundly approximates it. Had that approximation been complete, we would have an effective decision procedure for implementation set inclusion. Indeed this is the case for an important subclass of specifications: the one of deterministic CMCs. We introduce the definition of *Single Valuation Normal Form*, which plays an important role in both the determinization algorithm and in the proof of completeness.

Definition 10 *A CMC is in a* Single Valuation Normal Form *if all its admissible valuation sets are singleton (*$|V(i)| = 1$ *for each* $1 \leq i \leq k$*).*

It turns out that every consistent CMC (except those that have more than one admissible valuation in the initial state) can be transformed into the normal form preserving its implementation set. Due to space constraints, the polynomial time normalization algorithm can be found in Appendix A.7.

We now present a determinization algorithm that can be applied to any CMC S whose initial state is a single valuation set. This algorithm relies on normalizing the specification first, and otherwise applies an algorithm which resembles determinization of automata. The result of the algorithm is a new CMC whose set of implementations includes the one of S. This weakening character of determinization resembles the known determinization algorithms for modal transition systems [3].

Definition 11 *Let* $S = \langle \{1, \ldots, k\}, o, \varphi, A, V \rangle$ *be a consistent CMC in the single valuation normal form. Let* $m < k$ *and* $h : \{1, \ldots, k\} \to \{1, \ldots, m\}$ *be a surjection such that (1)* $\{1, \ldots, k\} = \cup_{v \in \{1, \ldots, m\}} h^{-1}(v)$ *and (2) for all* $1 \leq i \neq j \leq k$*, if there exists* $1 \leq u \leq k$ *and* $x, y \in [0,1]^k$ *such that* $(\varphi(u)(x) \wedge x_i \neq 0)$ *and* $(\varphi(u)(y) \wedge y_j \neq 0)$*, then* $(h(i) = h(j) \iff V(i) = V(j))$*; otherwise* $h(i) \neq h(j)$*. A deterministic CMC for* S *is the CMC* $\rho(S) = \langle \{1, \ldots, m\}, o', \varphi', A, V' \rangle$ *where* $o' = h(o)$*,* $\forall 1 \leq i \leq k$*,* $V'(h(i)) = V(i)$*, and for each* $1 \leq i \leq m$*,*

$$\varphi'(i)(y_1, \ldots, y_m) = \exists x_1, \ldots, x_k,$$
$$\bigvee_{u \in h^{-1}(i)} [(\forall 1 \leq j \leq m,\ y_j = \sum_{v \in h^{-1}(j)} x_v) \wedge \varphi(u)(x_1, \ldots, x_k)].$$

Theorem 5 *Let* S *be a CMC in* single valuation normal form*, we have* $S \preceq \rho(S)$.

As weak refinement implies inclusion, a direct consequence of Theorem 5 is that $[\![S]\!] \subseteq [\![\rho(S)]\!]$.

We now state the main theorem of the section.

Theorem 6 *Let $S_1 = \langle\{1,\ldots,k_1\}, o_1, \varphi_1, A_1, V_1\rangle$ and $S_2 = \langle\{1,\ldots,k_2\}, o_2, \varphi_2, A_2, V_2\rangle$ be two consistent single valuation normal form deterministic CMCs with $A_2 \subseteq A_1$. We have $[\![S_1]\!] \subseteq [\![S_2]\!] \Rightarrow S_1 \preceq S_2$.*

Proof :
We present a sketch of the proof and refer to Appendix A.8.2 for details. We construct the refinement relation by relating all pairs of states of S_1 and S_2 for which implementation inclusion holds. Let $\mathcal{R} \subseteq \{1,\ldots,k_1\} \times \{1,\ldots,k_2\}$ such that $v\,\mathcal{R}\,u$ iff for all MC I and state p of I, $p \models v \Rightarrow p \models u$. As we consider pruned CMCs, there exist implementations for all states. Then the usual, albeit complex and long in this case, coinductive proof technique is applied, showing that this relation is indeed a weak refinement relation.

The crucial point of the argument lies in proving the closure property — i.e. that if an S_1 state u advances possibly to u' then indeed the corresponding state v of S_2 can also advance to v' and the (u', v') pair is in $\mathcal{R}$. In other words that implementation inclusion of predecessors implies the implementation inclusion of successors. This is proven in an ad absurdum argument, roughly as follows. Assume that there would exist an implementation I' of u' which is not an implementation of v'. Then one can construct an implementation I'' of u which evolves as I'. This implementation would not implement v' but it could implement some other state of S_2. This case will be ruled out by requiring determinism and a normal form of S_2. Then the only way for I'' to evolve is to satisfy v' which contradicts the assumption that I' is not an implementation of v'. □

Observe that since any consistent CMC with a single valuation in initial state can be normalized, Theorem 6 holds even if S_1 and S_2 are not in single valuation normal form. We conclude that weak refinement and the implementation set inclusion coincide on the class of deterministic CMCs with at most single valuation in the initial state.

6 Constraints and Decidability

In the definition of CMCs, no particular type of constraints is implied, and nothing can be said, for instance on the decidability of refinement. For first order constraints over reals all our operators and relations are computable [25]. Several more tractable classes of constraints can be considered: interval, linear or polynomial constraints. Interval constraints are of the form $\varphi(i)(x) = \bigwedge_j\ \alpha_{ij} \leq x_j \leq \beta_{ij}$. Linear constraints are of the form $\varphi(i)(x) = x \times C_i \leq b_i$ where C_i is a matrix and b_i a row vector. Polynomial constraints are first order formulas of the form $\varphi(i)(x) = \exists y, \bigwedge_j \text{sign}(P_{ij}(x,y)) = \sigma_{ij}$ with P_{ij} being polynomials of arbitrary degrees and $\sigma_{ij} \in \{-1, 0, +1\}$. These classes have increasing expressiveness, and yet what really distinguishes them is their closure properties with respect to the independent parallel and conjunction composition operators. Indeed, only the class of polynomial constraints is closed under independent parallel composition, as polynomial equations of the form $z_{ij} - x_i y_j = 0$ are introduced in the resulting constraints. Concerning the conjunction operator, only the linear and polynomial classes are closed under this composition operator, as the resulting constraints are of the form $\varphi(i,j)(x) = \varphi_1(i)(x \times M_1) \wedge \varphi_2(j)(x \times M_2)$ which in general are not interval constraints.

We now consider the refinement checking problem between CMCs with polynomial constraints: Given S_1 and S_2, two CMCs with polynomial constraints and less than n states and s polynomials of degree d, decide whether S_1 refines S_2. It re-

duces to checking the validity of $O(n^2)$ instances of the following first order formula: $\forall x, \varphi_1(i)(x) \Rightarrow \exists \Delta, \varphi_2(j)(x \times \Delta) \wedge \bigwedge_{i'}(\sum_{j'} \Delta_{i'j'} = 1) \wedge \bigwedge_{i',j'}(i' \mathcal{R} j' \vee \Delta_{i'j'} = 0)$ where constraint $\bigwedge_{i'} \sum_{j'} \Delta_{i'j'} = 1$ relates to axiom 2.a of definition 6, under the assumption that an unreachable dummy universal state is inserted in S_2. Deciding the validity of such formulas can be done by quantifier elimination. The cylindrical algebraic decomposition algorithm [4], implemented in several symbolic computation tools (for instance, Maple [26]) performs this quantifier elimination in time double exponential in the number of variables, even when the number of quantifier alternations is constant [5]. With this algorithm, refinement can be decided in time $O(n^2 2^{2^{n^2}})$. However, considering constraints φ contain only existential quantifiers, quantifier alternation is exactly one in our case, and there are quantifier elimination algorithms that have a worst case complexity single exponential only in the number of variables, although they are double exponential in the number of quantifier alternations [2]. Using this algorithm, refinement can be decided in time $O(n^2 s^{n^2} d^{n^2})$.

Deciding whether a CMC is deterministic is of particular importance since refinement is not complete in the class of non-deterministic CMCs and that determinization is an abstraction in general. Determinism of a CMC with polynomial constraints can also be decided in time single exponential in the size of the CMC. However, this problem becomes polynomial when restricting constraints to be linear inequalities. Consider a CMC S with linear constraints $\varphi(i)(x) = x \times C_i \leq b_i$. Recall that CMC S is deterministic if and only if for all states i, j such that $i < j$, $V(i) \cap V(j) \neq \emptyset$ implies for all k, $\{x | x \times C_k \leq b_k \wedge x_i = 0\} = \emptyset$ or $\{y | y \times C_k \leq b_k \wedge y_j = 0\} = \emptyset$. This can be decided in polynomial time using Fourrier-Motzkin elimination [23].

7 Related Work and Concluding Remarks

We have presented Constraint Markov Chains—a new model for representing a possibly infinite family of Markov Chains. Unlike the previous attempts [15, 8], our model is closed under many design operations, including composition and conjunction. We have studied these operations as well as several classical compositional reasoning properties, showing that, among others, the CMC specification theory is equipped with a complete refinement relation (for deterministic specifications), which naturally interacts with parallel composition, synchronization and conjunction.

Two recent contributions [8, 14] are strongly related to these results. Fecher et al. [8] propose a definition of weak refinement for Interval Markov Chains that is coarser than the refinement defined in [15] (see also Definition 5 here). They also give a model checking procedure for PCTL [7] and Interval Markov Chains. Our definition of weak refinement coincides with theirs for Interval Markov Chains, which are a subclass of CMCs. Very recently Katoen and coauthors [14] have extended Fecher's work to *Interactive* Markov Chains, a convenient model for performance evaluation [10, 13]. Their abstraction uses the continuous time version of Interval Markov Chains [16] augmented with may and must transitions, very much in the spirit of [17, 21]. Parallel composition is defined and studied for this abstraction, however conjunction has been studied neither in [8] nor in [14].

In future, it would be of interest to design, implement and evaluate efficient algorithms for procedures outlined in this paper. We would also like to define a quotient relation for CMCs, presumably building on results presented in [19]. The quotienting operation is of particular importance for component reuse. One could also investigate applicability of our approach in model checking procedures, in the same style as Fecher

and coauthors have used Interval Markov Chains for model checking PCTL [8]. Finally the model presented in [14] can probably be extended from intervals to more general constraints.

References

[1] S. Andova. Process algebra with probabilistic choice. In *ARTS*, volume 1601 of *LNCS*, pages 111–129. Springer, 1999.

[2] S. Basu. New results on quantifier elimination over real closed fields and applications to constraint databases. *Journal of the ACM*, 46(4):537–555, July 1999.

[3] N. Benes, J. Kretinsky, K. G. Larsen, and J. Srba. On determinism in modal transition systems. To appear in Theoretical Computer Science.

[4] C. W. Brown. Simple cad construction and its applications. *Journal of Symbolic Computation*, 31(5):521–547, May 2001.

[5] C. W. Brown and J. H. Davenport. The complexity of quantifier elimination and cylindrical algeraic decomposition. In *SSAC*, pages 54–60, Waterloo, ON, Canada, 2007.

[6] K. Chatterjee, K. Sen, and T. A. Henzinger. Model-checking omega-regular properties of interval Markov chains. In *FoSSaCS*, volume 4962 of *LNCS*, pages 302–317. Springer, 2008.

[7] F. Ciesinski and M. Größer. On probabilistic computation tree logic. In *Validation of Stochastic Systems*, volume 2925 of *LNCS*, pages 147–188. Springer, 2004.

[8] H. Fecher, M. Leucker, and V. Wolf. Don't Know in probabilistic systems. In *SPIN*, volume 3925 of *LNCS*, pages 71–88. Springer, 2006.

[9] H. Hansson and B. Jonsson. A logic for reasoning about time and reliability. *Formal Asp. Comput.*, 6(5):512–535, 1994.

[10] H. Hermanns, U. Herzog, and J. Katoen. Process algebra for performance evaluation. *Theor. Comput. Sci.*, 274(1-2):43–87, 2002.

[11] H. Hermanns, B. Wachter, and L. Zhang. Probabilistic CEGAR. In *CAV*, volume 5123 of *LNCS*, pages 162–175. Springer, 2008.

[12] H. Hermans. *Interactive Markov Chains*. springer, 2002.

[13] J. Hillston. *A Compositional Approach to Performance Modelling*. Cambridge University Press, 1996.

[14] D. K. J. Katoen and M. R. Neuhauber. Compositional abstraction for stochastic systems. In *FORMATS*, LNCS. Springer, 2009. To appear.

[15] B. Jonsson and K. G. Larsen. Specification and refinement of probabilistic processes. In *LICS*, pages 266–277. IEEE Computer Society, 1991.

[16] J. Katoen, D. Klink, M. Leucker, and V. Wolf. Three-valued abstraction for continuous-time Markov chains. In *CAV*, volume 4590 of *LNCS*, pages 311–324. Springer, 2007.

[17] K. G. Larsen. Modal specifications. In *AVMS*, volume 407 of *LNCS*, pages 232–246. Springer, 1989.

[18] K. G. Larsen, U. Nyman, and A. Wasowski. Modal I/O automata for interface and product line theories. In R. D. Nicola, editor, *ESOP*, volume 4421 of *Lecture Notes in Computer Science*, pages 64–79. Springer, 2007.

[19] K. G. Larsen and A. Skou. Compositional verification of probabilistic processes. In *CONCUR*, volume 630 of *LNCS*, pages 456–471. Springer, 1992.

[20] N. López and M. Núñez. An overview of probabilistic process algebras and their equivalences. In *Validation of Stochastic Systems*, volume 2925 of *LNCS*, pages 89–123. Springer, 2004.

[21] J.-B. Raclet. Residual for component specifications. In *FACS*, 2007.

[22] J.-B. Raclet, E. Badouel, A. Benveniste, B. Caillaud, and R. Passerone. Why are modalities good for interface theories? In *ACSD*. IEEE Computer Society Press, 2009.

[23] A. Schrijver. *Theory of linear and integer programming*. Wiley, April 1998.

[24] K. Sen, M. Viswanathan, and G. Agha. Model-checking Markov chains in the presence of uncertainties. In *TACAS*, pages 394–410, 2006.

[25] A. Tarski. *A Decision Method for Elementary Algebra and Geometry*. RAND Corp., 1948.

[26] H. Yanami and H. Anai. Synrac: a maple toolbox for solving real algebraic constraints. *ACM Communications in Computer Algebra*, 41(3):112–113, September 2007.

A Proofs

The following appendix contains proofs of the most essential claims. It is to be reviewed at the discretion of the programme committee.

A.1 Correspondance matrices

Definition 12 ($\otimes$, $\odot$) *Define the following operations :*

1. *If $\Delta \in [0,1]^{k\times q}$ and $\Delta' \in [0,1]^{k\times r}$ are two correspondance matrices, we define $\Delta'' = \Delta \otimes \Delta'$ by $\Delta'' \in [0,1]^{k\times(q\cdot r)}$ and $\Delta''_{i(j,n)} = \Delta_{ij} \cdot \Delta'_{in}$;*
2. *If $\Delta \in [0,1]^{k\times q}$ and $\Delta' \in [0,1]^{r\times s}$ are two correspondance matrices, we define $\Delta'' = \Delta \odot \Delta'$ by $\Delta'' \in [0,1]^{(k\cdot r)\times(q\cdot s)}$ and $\Delta''_{(i,j)(n,p)} = \Delta_{in} \cdot \Delta'_{jp}$.*

Lemma 1
1. *Let $\Delta \in [0,1]^{k\times q}$ and $\Delta' \in [0,1]^{q\times r}$ be two correspondance matrices. The matrix $\Delta'' = \Delta \times \Delta'$ is a correspondance matrix;*
2. *Let $\Delta \in [0,1]^{k\times q}$ and $\Delta' \in [0,1]^{k\times r}$ be two correspondance matrices. The matrix $\Delta'' = \Delta \otimes \Delta'$ is a correspondance matrix;*
3. *Let $\Delta \in [0,1]^{k\times q}$ and $\Delta' \in [0,1]^{r\times s}$ be two correspondance matrices. The matrix $\Delta'' = \Delta \odot \Delta'$ is a correspondance matrix;*

Proof :

1. *Let $1 \le i \le k$ and $1 \le j \le r$. We have $\Delta''_{ij} = \sum_{n=1}^{q} \Delta_{in} \cdot \Delta'_{nj}$. Thus,*

$$\begin{aligned}\sum_{j=1}^{r} \Delta''_{ij} &= \sum_{j=1}^{r}\sum_{n=1}^{q} \Delta_{in} \cdot \Delta'_{nj} = \sum_{n=1}^{q}\sum_{j=1}^{r} \Delta_{in} \cdot \Delta'_{nj} = \sum_{n=1}^{q} \Delta_{in} \cdot (\sum_{j=1}^{r} \Delta'_{nj}) \\ &= \sum_{n=1}^{q} \Delta_{in} \cdot 1 \le 1.\end{aligned}$$

2. *Let $1 \le i \le k$ and $(j,n) \in \{1,\dots q\} \times \{1,\dots r\}$. We have $\Delta''_{i(j,n)} = \Delta_{ij} \cdot \Delta'_{in}$. Thus,*

$$\begin{aligned}\sum_{(j,n)\in\{1,\dots q\}\times\{1,\dots r\}} \Delta''_{i(j,n)} &= \sum_{j=1}^{q}\sum_{n=1}^{r} \Delta''_{i(j,n)} = \sum_{j=1}^{q}\sum_{n=1}^{r} \Delta_{ij} \cdot \Delta'_{in} \\ &= \sum_{j=1}^{q} \Delta_{ij} \sum_{n=1}^{r} \Delta'_{in} \le 1.\end{aligned}$$

3. *Let $(i,j) \in \{1,\dots k\} \times \{1,\dots r\}$ and $(n,p) \in \{1,\dots q\} \times \{1,\dots s\}$. We have $\Delta''_{(i,j)(n,p)} = \Delta_{in} \cdot \Delta'_{jp}$. Thus,*

$$\begin{aligned}\sum_{(n,p)\in\{1,\dots q\}\times\{1,\dots s\}} \Delta''_{(i,j)(n,p)} &= \sum_{n=1}^{q}\sum_{p=1}^{s} \Delta_{in} \cdot \Delta'_{jp} = (\sum_{n=1}^{q} \Delta_{in}) \cdot (\sum_{p=1}^{s} \Delta'_{jp}) \\ &\le 1.\end{aligned}$$

□

A.2 Proof of Theorem 1

Proof :
Let $S = \langle \{1,\dots,k\}, o, \varphi, A, V\rangle$ be a CMC (with at least an inconsistent state) and $P = \langle \{1,\dots,n\}, o_P, M, A_P, V_P\rangle$ be a MC. Let $S' = \langle \{1,\dots,k'\}, o', \varphi', A, V'\rangle = \beta(S)$. If $\beta(S)$ is empty, then both S and $\beta(S)$ are inconsistent.

Consider a function ν for removing inconsistent states (one exists because there are inconsistent states), such that $k' < k$ and for all $1 \leq i \leq k$, $\nu(i) = \perp \iff [(V(i) = \emptyset) \vee (\forall x \in [0,1]^k,\ \neg\varphi(i)(x))]$ and $\nu(i) \neq \perp \Rightarrow \forall j \neq i,\ \nu(j) \neq \nu(i)$. We first prove that $P \models S \iff P \models \beta(S)$.

- $\Rightarrow$ *Suppose that $P \models S$. Then there exists a satisfaction relation $\mathcal{R}$ such that $o_P \,\mathcal{R}\, o$. Define the relation $\mathcal{R}' \subseteq \{1,\dots,n\} \times \{1,\dots,k'\}$ such that $p\,\mathcal{R}'\,v$ iff there exists $u \in \{1,\dots,k\}$ such that $p\,\mathcal{R}\,u$ and $\nu(u) = v$. It is clear that $o_P\,\mathcal{R}'\,o'$. We prove that $\mathcal{R}'$ is a satisfaction relation. Let p, u, v such that $p\,\mathcal{R}\,u$ and $\nu(u) = v$.*

  - *As $\nu(u) \neq \perp$, we have by definition that $V'(v) = V(u)$, thus $V_P(p)\downarrow_A \in V'(v)$.*
  - *Let $\Delta \in [0,1]^{n\times k}$ be the correspondence matrix witnessing $p\,\mathcal{R}\,u$. Let $\Delta' \in [0,1]^{n\times k'}$ such that $\Delta'_{qw} = \Delta_{q\nu^{-1}(w)}$. It is clear that Δ' is a correspondence matrix. We first show that*

$$\forall u' \in \{1,\dots,k\},\ (\nu(u') = \perp) \Rightarrow (\forall q \in \{1,\dots,n\},\ \Delta_{qu'} = 0). \quad (1)$$

Let $u' \in \{1,\dots,k\}$ such that $\nu(u') = \perp$, and suppose that there exists $q \in \{1,\dots,n\}$, $\Delta_{qu'} \neq 0$. As Δ is a correspondence matrix, we have $q\,\mathcal{R}\,u'$. Thus $V_P(q)\downarrow_A \in V(u')$, which means that $V(u') \neq \emptyset$, and there exists Δ'' such that $\varphi(u')(M_q \times \Delta'')$. Thus, there exists $x \in [0,1]^{1\times k}$ such that $\varphi(u')(x)$. As a consequence, we cannot have $\nu(u') = \perp$, which is a contradiction, thus (1).

We now prove that $\mathcal{R}'$ satisfies the axioms of a satisfaction relation.

1. *Let $p' \in \{1,\dots,n\}$ such that $M_{pp'} \neq 0$. This implies, by definition, that $\sum_{j=1}^{k} \Delta_{p'j} = 1$. We have $\sum_{j=1}^{k'} \Delta'_{p'j} = \sum_{r\in\{1,\dots,k\} \mid \nu(r)\neq\perp} \Delta_{p'r}$. By (1), $\sum_{r\in\{1,\dots,k\} \mid \nu(r)\neq\perp} \Delta_{p'r} = \sum_{r=1}^{k} \Delta_{p'r} = 1$.*
2. *Let $y = M_p \times \Delta' \in [0,1]^{1\times k'}$ and $x = M_p \times \Delta \in [0,1]^{1\times k}$. We know that $\varphi(u)(x)$ holds. Moreover, by (1), if $\nu(q) = \perp$, then $x_q = 0$, and for all $l \in \{1,\dots,k'\},\ y_l = x_{\nu^{-1}(l)}$. Clearly, this implies that $\varphi'(v)(M_p \times \Delta')$ holds.*
3. *Let $p', v' \in \{1,\dots,n\} \times \{1,\dots,k'\}$ such that $\Delta'_{p'v'} \neq 0$. We have $\Delta'_{p'v'} = \Delta_{p'\nu^{-1}(v')} \neq 0$, thus there exists $u' \in \{1,\dots,k\}$ such that $p'\,\mathcal{R}\,u'$ and $\nu(u') = v'$. Finally $p'\,\mathcal{R}'\,v'$.*

Finally, $\mathcal{R}'$ is a satisfaction relation such that $o_P\,\mathcal{R}'\,o'$, thus $P \models \beta(S)$.

$\Leftarrow$ *Conversely, the reasoning is the same, except that we now build* Δ *from* Δ' *saying that* $\Delta_{qv} = 0$ *if* $\nu(v) = \bot$ *and* $\Delta_{qv} = \Delta'_{q\nu(v)}$ *else.*

We have proved that β *is implementations-conservative, thus the fixpoint of* β *verifies the same property.*

□

A.3 Proof of Theorem 2

Let $S_1 = \langle\{1,\ldots,k_1\}, o_1, \varphi_1, A_1, V_1\rangle$, $S_2 = \langle\{1,\ldots,k_2\}, o_2, \varphi_2, A_2, V_2\rangle$ and $S_3 = \langle\{1,\ldots,k_3\}, o_3,$
$\varphi_3, A_3, V_3\rangle$ be three CMCs. We want to prove that

1. $((S_1 \wedge S_2) \preceq S_1) \wedge ((S_1 \wedge S_2) \preceq S_2)$;
2. $(S_3 \preceq S_1) \wedge (S_3 \preceq S_2) \Rightarrow S_3 \preceq (S_1 \wedge S_2)$.

Proof :

We separately prove the two items of the theorem.

1. *Let* $S_1 \wedge S_2 = S = \langle\{1,\ldots,k_1\} \times \{1,\ldots,k_2\}, o, \varphi, A, V\rangle$.
   Let $\mathcal{R} \subseteq (\{1,\ldots,k_1\} \times \{1,\ldots,k_2\}) \times \{1,\ldots,k_1\}$ *such that* $(u,v)\,\mathcal{R}\,w \iff u = w$. *We will prove that* $\mathcal{R}$ *is a* **strong** *refinement relation. Let* $u \in \{1,\ldots k_1\}$ *and* $v \in \{1,\ldots k_2\}$. *We have* $(u,v)\,\mathcal{R}\,u$. *By definition of* S, *we also have* $V((u,v))\downarrow_{A_1} = (V_1(u)\uparrow^A \cap V_2(v)\uparrow^A)\downarrow_{A_1} \subseteq V_1(u)$.
   Let $\Delta \in [0,1]^{k_1 \cdot k_2 \times k_1}$ *such that* $\Delta_{(i,j),i} = 1$ *and* $\Delta_{(i,j),k} = 0$ *if* $k \neq i$. *By definition, we have* $\forall (i,j)$, $\sum_{k=1}^{k_1} \Delta_{(i,j),k} = 1$. *As a consequence,* Δ *is correspondance matrix. We now prove that it satisfies the axioms of a satifaction relation for* $(u,v)\,\mathcal{R}\,u$.

   (a) *If* $x \in [0,1]^{1 \times k_1 \cdot k_2}$ *is such that* $\varphi((u,v))(x)$, *it implies by definition that* $\varphi_1(u)(\sum_{j=1}^{k_2} x_{1,j},$
   $\ldots \sum_{j=1}^{k_2} x_{k_1,j}) = \varphi_1(u)(x \times \Delta)$ *holds.*
   (b) *If* $\Delta_{(u',v'),w'} \neq 0$, *we have by definition* $u' = w'$ *and* $(u',v')\,\mathcal{R}\,u'$.

   From (a) and (b), we conclude that $\mathcal{R}$ *is a* **strong** *refinement relation. Since* $(o_1,o_2)\,\mathcal{R}\,o_1$, *we have* $S_1 \wedge S_2 \preceq S_1$. *By symmetry, we also have* $S_1 \wedge S_2 \preceq S_2$.

2. *Suppose that* $S_3 \preceq S_1$ *and* $S_3 \preceq S_2$. *By definition, there exist two refinement relations* $\mathcal{R}_1 \subseteq \{1,\ldots,k_3\} \times \{1,\ldots,k_1\}$ *and* $\mathcal{R}_2 \subseteq \{1,\ldots,k_3\} \times \{1,\ldots,k_2\}$ *such that* $o_3\,\mathcal{R}_1\,o_1$ *and* $o_3\,\mathcal{R}_2\,o_2$. *Let* $S_1 \wedge S_2 = S = \langle\{1,\ldots,k_1\} \times \{1,\ldots,k_2\}, o, \varphi, A, V\rangle$.
   Let $\mathcal{R} \subseteq \{1,\ldots,k_3\} \times (\{1,\ldots,k_1\} \times \{1,\ldots,k_2\})$ *such that* $u\,\mathcal{R}(v,w) \iff u\,\mathcal{R}_1\,v$ *and* $u\,\mathcal{R}_2\,w$. *We now prove that* $\mathcal{R}$ *is a refinement relation.*
   Consider u,v,w *such that* $u\,\mathcal{R}(v,w)$.

   (a) *By definition, we have* $V_3(u)\downarrow_{A_1} \subseteq V_1(v)$ *and* $V_3(u)\downarrow_{A_2} \subseteq V_2(w)$. *As a consequence,* $V_3(u)\downarrow_A \subseteq V((v,w))$.

(b) Let $x \in [0,1]^{1\times k_3}$ such that $\varphi_3(u)(x)$. Consider the correspondance matrices $\Delta \in [0,1]^{k_3\times k_1}$ and $\Delta' \in [0,1]^{k_3\times k_2}$ given by $u\,\mathcal{R}_1\,v$ and $u\,\mathcal{R}_2\,w$ for the transition vector x. Let $\Delta'' \in [0,1]^{k_3\times k_1\cdot k_2} = \Delta \otimes \Delta'$. By Lemma 1, Δ'' is a correspondance matrix. We now prove that it satisfies the axioms of a refinement relation for $u\,\mathcal{R}(v,w)$.

i. Let $1 \leq i \leq k_3$ such that $x_i \neq 0$. By definition of Δ and Δ', we have $\sum_{j=1}^{k_1} \Delta_{ij} = 1$ and $\sum_{q=1}^{k_2} \Delta'_{iq} = 1$. By construction, $\sum_{(j,q)\in\{1,\ldots,k_1\}\times\{1,\ldots,k_2\}} \Delta''_{i(j,q)} = (\sum_{j=1}^{k_1} \Delta_{ij}) \cdot (\sum_{q=1}^{k_2} \Delta'_{iq}) = 1$.

ii. By definition of Δ and Δ', both $\varphi_1(v)(x\times\Delta)$ and $\varphi_2(w)(x\times\Delta')$ hold. Let $x' = x\times\Delta''$. It is clear that $x\times\Delta = (\sum_{j=1}^{k_2} x'_{1,j}, \ldots, \sum_{j=1}^{k_2} x'_{k_1,j})$ and $x\times\Delta' = (\sum_{i=1}^{k_1} x'_{i,1}, \ldots, \sum_{i=1}^{k_1} x'_{i,k_2})$. As a consequence, $\varphi((v,w))(x\times\Delta'')$ holds.

iii. Let u', v', w' such that $\Delta''_{u'(v',w')} \neq 0$. By construction, this implies $\Delta_{u'v'} \neq 0$ and $\Delta'_{u'w'} \neq 0$. As a consequence, $u'\,\mathcal{R}_1\,v'$ and $u'\,\mathcal{R}_2\,w'$, thus $u'\,\mathcal{R}(v',w')$.

From (i) - (iii), we conclude that $\mathcal{R}$ is a refinement relation. Since $o_3\,\mathcal{R}(o_1,o_2)$, we have $S_3 \preceq (S_1 \wedge S_2)$.

□

A.4 Proof of Theorem 3

Let $S'_1 = \langle\{1,\ldots,k'_1\}, o'_1, \varphi'_1, A'_1, V'_1\rangle$, $S'_2 = \langle\{1,\ldots,k'_2\}, o'_2, \varphi'_2, A'_2, V'_2\rangle$, $S_1 = \langle\{1,\ldots,k_1\}, o_1, \varphi_1,$
$A_1, V_1\rangle$, $S_2 = \langle\{1,\ldots,k_2\}, o_2, \varphi_2, A_2, V_2\rangle$ be four CMCs. Suppose $S'_1 \preceq S_1 \wedge S'_2 \preceq S_2$. We prove that $S'_1 \parallel S'_2 \preceq S_1 \parallel S_2$.

Proof :
Let $S = \langle\{1,\ldots,k_1\}\times\{1,\ldots,k_2\}, (o_1,o_2), \varphi, A, V\rangle = S_1 \parallel S_2$
and $S' = \langle\{1,\ldots,k'_1\}\times\{1,\ldots,k'_2\}, (o'_1,o'_2), \varphi', A', V'\rangle = S'_1 \parallel S'_2$.
By definition, there exist two refinement relations $\mathcal{R}_1$ and $\mathcal{R}_2$ such that $o'_1\,\mathcal{R}_1\,o_1$ and $o'_2\,\mathcal{R}_2\,o_2$. Define $\mathcal{R}$ such that $(u',v')\,\mathcal{R}(u,v) \iff u'\,\mathcal{R}_1\,u$ and $v'\,\mathcal{R}_2\,v$. Consider now such (u',v') and (u,v). We now prove that $\mathcal{R}$ satisfies the axioms of a refinement relation between (u',v') and (u,v).

1. *We have $(V'((u',v')))\downarrow_A = \{Q \subseteq 2^{A'} \mid \exists Q_1 \in V'_1(u'),\ Q_2 \in V'_2(v'),\ Q = Q_1\cup Q_2\}\downarrow_A = \{Q \subseteq 2^A \mid \exists Q_1 \in V'_1(u'),\ Q_2 \in V'_2(v'),\ Q = Q_1\downarrow_{A_1} \cup Q_2\downarrow_{A_2}\}$. Thus $(V'((u',v')))\downarrow_A \subseteq V((u,v))$.*

2. *Let $z' \in [0,1]^{1\times k'_1\cdot k'_2}$ such that $\varphi'(u',v')(z')$. We now build the correspondance matrix Δ witnessing $(u',v')\,\mathcal{R}(u,v)$. Consider the correspondance matrices Δ_1 and Δ_2 given by $u'\,\mathcal{R}_1\,u$ and $v'\,\mathcal{R}_2\,v$ for the transition vector z'. Define $\Delta = \Delta_1 \odot \Delta_2 \in [0,1]^{k'_1\cdot k'_2\times k_1\cdot k_2}$. By Lemma 1, Δ is a correspondence matrix. Moreover, since $\varphi'(u',v')(z')$ holds, there exists $x' \in [0,1]^{1\times k'_1}$ and $y' \in [0,1]^{1\times k'_2}$ such that $\forall i,j,\ z'_{(i,j)} = x'_i \cdot y'_j$ and $\varphi'_1(u')(x')$ and $\varphi'_2(v')(y')$.*

   (a) Let $(u'',v'') \in \{1,\ldots,k'_1\}\times\{1,\ldots,k'_2\}$ such that $z_{(u'',v'')} \neq 0$. By definition of x' and y', this implies that $x'_{u''} \neq 0$ and $y'_{v''} \neq 0$. Thus $\sum_{j=1}^{k_1} \Delta_{1u''j} = 1$ and $\sum_{j=1}^{k_2} \Delta_{2v''j} = 1$.

$$\sum_{(r,s)\in\{1,\dots,k_1\}\times\{1,\dots,k_2\}} \Delta_{(u'',v'')(r,s)} = \sum_{(r,s)\in\{1,\dots,k_1\}\times\{1,\dots,k_2\}} \Delta_{1u''r}\cdot\Delta_{2v''s}$$
$$= \sum_{r=1}^{k_1}\sum_{s=1}^{k_2} \Delta_{1u''r}\cdot\Delta_{2v''s}$$
$$= (\sum_{r=1}^{k_1}\Delta_{1u''r})\cdot(\sum_{s=1}^{k_2}\Delta_{2v''s}) = 1.$$

(b) Let $z = z' \times \Delta \in [0,1]^{1\times k_1\cdot k_2}$. Remark that $z = (x'\times\Delta_1)\otimes(y'\times\Delta_2)$. Let $x = x'\times\Delta_1$ and $y = y'\times\Delta_2$. Since $u'\,\mathcal{R}_1\,u$ and $v'\,\mathcal{R}_2\,v$, we have $\varphi_1(u)(x)$ and $\varphi_2(v)(y)$. Thus $\varphi(u,v)(z'\times\Delta)$.

(c) Let $u'', v'', u'''v'''$ such that $\Delta_{(u'',v'')(u''',v''')} \neq 0$.By definition, it implies that $\Delta_{1u''u'''} \neq 0$ and $\Delta_{2v''v'''} \neq 0$, and as a consequence $(u'',v'')\,\mathcal{R}(u''',v''')$.

From (a),(b),(c), we conclude that $\mathcal{R}$ is a refinement relation. Since $(o_1',o_2')\,\mathcal{R}(o_1,o_2)$, we have $S' \preceq S$.

□

The proof of the second part of the theorem is similar, and left to the reader.

A.5 Proof of Theorem 4

Let S_1, S_2 and S_3 be three CMCs with disjoint sets of atomic propositions A_1, A_2 and A_3. Let $\mathsf{Sync}_{123} = \langle\{1\},1,"\lambda x.x=1", A_1\cup A_2\cup A_3, V_{\mathsf{Sync}}\rangle$ be a synchronizer between A_1, A_2 and A_3. Consider $\mathsf{Sync}_{12} = \langle\{1\},1,"\lambda x.x=1", A_1\cup A_2, V_{\mathsf{Sync}}{\downarrow_{A_1\cup A_2}}\rangle$. We want to prove that $[\![[((S_1 \parallel S_2)\wedge\mathsf{Sync}_{12}) \parallel S_3]\wedge\mathsf{Sync}_{123}]\!] = [\![[S_1\parallel S_2\parallel S_3]\wedge\mathsf{Sync}_{123}]\!]$.

Proof :

We first prove the following statement. Let S_1 and S_2 be two CMCs with disjoint sets of atomic propositions A_1 and A_2. Let Sync_1 be a synchronizing vector on A_1. We have $(S_1\parallel S_2)\wedge\mathsf{Sync}_1 = (S_1\wedge\mathsf{Sync}_1)\parallel S_2$.

First, remember that synchronizers are single state CMCs, with a single transition taken with probability 1. As a consequence, computing the conjunction with a synchronizer preserves the structure of any CMC. The only change lies in the sets of valuations.

Let p be a state of S_1 and q be a state of S_2. We have $(V_1(p)\cup V_2(q))\cap V_{\mathsf{Sync}_1}{\uparrow^{A_1\cup A_2}} = (V_1(p)\cap V_{\mathsf{Sync}_1})\cup V_2(q)$. As a consequence, the valuations of $(S_1\wedge\mathsf{Sync}_1)\parallel S_2$ are the same as the valuations of $(S_1\parallel S_2)\wedge\mathsf{Sync}_1$. □

By monotony of conjunction, we have $(S_1\parallel S_2)\wedge\mathsf{Sync}_{12}\preceq(S_1\parallel S_2)$. By Theorem 3, it implies that $[((S_1\parallel S_2)\wedge\mathsf{Sync}_{12})\parallel S_3]\wedge\mathsf{Sync}_{123}\preceq[S_1\parallel S_2\parallel S_3]\wedge\mathsf{Sync}_{123}$, and finally $[\![[((S_1\parallel S_2)\wedge\mathsf{Sync}_{12})\parallel S_3]\wedge\mathsf{Sync}_{123}]\!]\subseteq[\![[S_1\parallel S_2\parallel S_3]\wedge\mathsf{S}_{123}]\!]$.

We now prove that $[S_1\parallel S_2\parallel S_3]\wedge\mathsf{Sync}_{123}\preceq[((S_1\parallel S_2)\wedge\mathsf{Sync}_{12})\parallel S_3]\wedge\mathsf{Sync}_{123}$. By monotony of conjunction, we have $[S_1\parallel S_2\parallel S_3]\wedge\mathsf{Sync}_{123}\preceq[S_1\parallel$

$S_2 \parallel S_3] \wedge \mathsf{Sync}_{12} \wedge \mathsf{Sync}_{123}$. *Moreover, by the statement proved above, we have* $[S_1 \parallel S_2 \parallel S_3] \wedge \mathsf{Sync}_{12} \preceq ((S_1 \parallel S_2) \wedge \mathsf{Sync}_{12}) \parallel S_3$. *As a consequence, we have* $[S_1 \parallel S_2 \parallel S_3] \wedge \mathsf{Sync}_{123} \preceq [((S_1 \parallel S_2) \wedge \mathsf{Sync}_{12}) \parallel S_3] \wedge \mathsf{Sync}_{123}$, *and thus* $[\![[S_1 \parallel S_2 \parallel S_3] \wedge \mathsf{Sync}_{123}]\!] \subseteq [\![[((S_1 \parallel S_2) \wedge \mathsf{Sync}_{12}) \parallel S_3] \wedge \mathsf{Sync}_{123}]\!]$.

□

A.6 Proof of Theorem 5

Proof :
Let $S = \langle\{1,\dots,k\}, o, \varphi, A, V\rangle$ *be a CMC in single valuation normal form. Let* $\rho(S) = \langle\{1,\dots,m\}, o', \varphi', A, V'\rangle$ *be a determinisation of* S *and* $h : \{1,\dots,k\} \to \{1,\dots,m\}$ *the associated projection.*

Define $\mathcal{R} \subseteq \{1,\dots,k\} \times \{1,\dots,m\}$ *such that* $u \,\mathcal{R}\, v \iff h(u) = v$. *We will show that* $\mathcal{R}$ *is a strong refinement relation. Let* u, v *such that* $u \,\mathcal{R}\, v$.

1. *By definition, we have* $h(u) = v$, *thus* $V'(v) = V(u)$.
2. *Let* $\Delta \in [0,1]^{k\times m}$ *such that* $\Delta_{i,j} = 1$ *if* $h(i) = j$ *and* 0 *else.* Δ *is clearly a correspondance matrix.*
   (a) *Let* $x \in [0,1]^k$ *such that* $\varphi(u)(x)$. *For all* $1 \le j \le m$, *we have* $y_j = \sum_{i\in h^{-1}(j)} x_i$ *and* $\varphi(u)(x)$, *thus* $\varphi'(v)(x \times \Delta)$. *Moreover, for all* $1 \le i \le k$, $\sum_{j=1}^{m} \Delta_{i,j} = 1$ *by construction.*
   (b) *If* $\Delta_{u',v'} \neq 0$, *then* $h(u') = v'$ *and thus* $u' \,\mathcal{R}\, v'$.

Finally, $\mathcal{R}$ *is a refinement relation and* $o \,\mathcal{R}\, o'$, *thus* $S \preceq \rho(S)$.

□

A.7 Normalization

The normalization algorithm basically separates each state u with m possible valuations into m states $u_1,\dots,u_m$, each with a single admissible valuation. Then the constraint function is adjusted, by substituting sums of probabilities going to the new states in place of the old probabilities targeting u. Finally, a mutual exclusion constraint is added so that it is not allowed to have positive probability of reaching more than one of u_i states from the same source state. The transformation is local and syntax based. It can be performed in polynomial time and it only increases the size of the CMC polynomially. We will write $\mathcal{N}(S)$ for a result of normalization of S.

Definition 13 (Normalization) *Let* $S = \langle\{1,\dots,k\}, o, \varphi, A, V\rangle$ *be a CMC. If there exists a function* $\mathcal{N} : \{1,\dots,k\} \to 2^{\{1,\dots,m\}}$ *such that*

1. $\{1,\dots,m\} = \cup_{i\in\{1\dots,k\}} \mathcal{N}(i)$;
2. *For all* $1 \le i \neq j \le k$, $\mathcal{N}(i) \cap \mathcal{N}(j) = \emptyset$;
3. $\forall 1 \le i \le k$, $|\mathcal{N}(i)| = |V(i)|$;

If, moreover, $|V(o)| = 1$, *the normalization of* S *is the CMC* $\mathcal{N}(S) = \langle\{1,\dots,m\}, o', \varphi', A, V'\rangle$ *such that* $\mathcal{N}(o) = o'$ *and*

1. $\forall 1 \le j \le m$, $|V'(j)| = 1$;

2. $\forall 1 \leq i \leq k, V(i) = \cup_{u \in \mathcal{N}(i)} V'(u)$;
3. $\forall 1 \leq i \leq k, \forall u, v \in \mathcal{N}(i), u \neq v \iff V'(u) \neq V'(v)$;
4. $\forall 1 \leq j \leq m$,

$$\varphi'(j)(x_1, \dots x_m) = \varphi(\mathcal{N}^{-1}(j))(\sum_{u \in \mathcal{N}(1)} x_u, \dots \sum_{u \in \mathcal{N}(k)} x_u).$$

By construction, $\mathcal{N}(S)$ is in single valuation normal form. Moreover, if S is consistent, then a function $\mathcal{N}$ satisfying the conditions above exists.

Theorem 7 *Let $S = \langle \{1, \dots k\}, o, \varphi, A, V \rangle$ be a consistent CMC. If $|V(o)| = 1$, then for all MC P, we have $P \models S \iff P \models \mathcal{N}(S)$.*

Proof :
Let $S = \langle \{1, \dots, k\}, o, \varphi, A, V \rangle$ be a consistent CMC such that $|V(o)| = 1$. Let $S' = \mathcal{N}(S) = \langle \{1, \dots, m\}, o', \varphi', A, V' \rangle$ and $\mathcal{N} : \{1, \dots, k\} \to 2^{\{1, \dots, m\}}$ the associated function.

$\Rightarrow$ *Let $P = \langle \{1, \dots, n\}, o_P, M, A_P, V_P \rangle$ be a MC such that $P \models S$. Let $\mathcal{R}$ be the associated satisfaction relation. Let $\mathcal{R}' \subseteq \{1, \dots, n\} \times \{1, \dots, m\}$ such that $p \mathcal{R} u \iff V_P(p) \in V'(u)$ and $p \mathcal{R} \mathcal{N}^{-1}(u)$. We will show that $\mathcal{R}'$ is a satisfaction relation. Let p, u such that $p \mathcal{R}' u$.*

1. *By definition, we have $V_P(p) \in V'(u)$.*
2. *We have $p \mathcal{R} \mathcal{N}^{-1}(u)$. Let $\Delta \in [0,1]^{n \times k}$ be the associated correspondance matrix. Define $\Delta' \in [0,1]^{n \times m}$ such that $\Delta'_{q,v} = \Delta_{q, \mathcal{N}^{-1}(v)}$ if $V_p(q) \in V'(v)$ and 0 else. As every coefficient of Δ appears once and only once in the same row of Δ', it is clear that Δ' is a correspondance matrix. Moreover,*
   (a) *If q is such that $M_{pq} \neq 0$, then $\sum_{j=1}^{m} \Delta'_{q,j} = \sum_{i=1}^{k} \Delta_{q,i} = 1$;*
   (b) *For all $1 \leq i \leq k$, $\sum_{j \in \mathcal{N}(i)} ([M_p \times \Delta']_j) = [M_p \times \Delta]_i$. As a consequence, $\varphi'(u)(M_p \times \Delta') = \varphi(\mathcal{N}^{-1}(u))(M_p \times \Delta)$ holds.*
   (c) *If q, v are such that $\Delta'_{q,v} \neq 0$, then $\Delta_{q, \mathcal{N}^{-1}(v)} \neq 0$ and $V_P(q) \in V'(v)$, thus $q \mathcal{R}' v$.*

Finally, $\mathcal{R}'$ is a satisfaction relation. It is easy to see that $o_p \mathcal{R}' o'$. As a consequence, we have $P \models \mathcal{N}(S)$.

$\Leftarrow$ *Let $P = \langle \{1, \dots, n\}, o_P, M, A_P, V_P \rangle$ be a MC such that $P \models \mathcal{N}(S)$. Let $\mathcal{R}$ be the associated satisfaction relation. Let $\mathcal{R}' \subseteq \{1, \dots, n\} \times \{1, \dots, k\}$ such that $p \mathcal{R}' u \iff \exists j \in \mathcal{N}(u)$ s.t. $p \mathcal{R} j$. We will show that $\mathcal{R}'$ is a satisfaction relation. Let p, u such that $p \mathcal{R}' u$.*

1. *We have $V_P(p) \in V(u) = \cup_{j \in \mathcal{N}(u)} V'(j)$.*
2. *Let $j \in \mathcal{N}(u)$ such that $p \mathcal{R} j$, and let $\Delta \in [0,1]^{n \times m}$ be the associated correspondance matrix. Define $\Delta' \in [0,1]^{n \times k}$ such that $\Delta'_{q,v} = \sum_{i \in \mathcal{N}(v)} \Delta_{q,i}$. It is clear that for all q, $\sum_{v=1}^{k} \Delta'_{q,v} = \sum_{r=1}^{m} \Delta_{qr}$. Thus Δ' is a correspondance matrix. Moreover,*

(a) If q is such that $M_{pq} \neq 0$, then $\sum_{i=1}^{k} \Delta'_{q,i} = \sum_{r=1}^{m} \Delta_{q,r} = 1$;
(b) For all $1 \leq i \leq k$, $[M_p \times \Delta']_i = \sum_{r \in \mathcal{N}(i)}([M_p \times \Delta]_r)$. As a consequence, $\varphi(u)(M_p \times \Delta) = \varphi'(j)(M_p \times \Delta')$ holds.
(c) If q, v are such that $\Delta'_{q,v} \neq 0$, then there exists $r \in \mathcal{N}(v)$ such that $\Delta_{q,r} \neq 0$, thus $q \mathcal{R}' v$.

Finally, $\mathcal{R}'$ is a satisfaction relation. It is esay to see that $o_P \mathcal{R}' o$. As a consequence, we have $P \models S$.

□

It is easy to see that normalization preserves determinism.

A.8 Completeness of weak refinement

A.8.1 Soundness of weak refinement

Let $S_1 = \langle \{1, \ldots, k_1\}, o_1, \varphi_1, A_1, V_1 \rangle$ and $S_2 \langle \{1, \ldots, k_2\}, o_2, \varphi_2, A_2, V_2 \rangle$ be two CMCs. Assume $S_1 \preceq S_2$, we prove that $[\![S_1]\!] \subseteq [\![S_2]\!]$.

Proof :

Since $S_1 \preceq S_2$, there exists a refinement relation $\mathcal{R} \subseteq \{1, \ldots, k_1\} \times \{1, \ldots, k_2\}$ such that $o_1 \mathcal{R} o_2$. Consider $P = \langle \{1, \ldots n\}, o_P, M, A_P, V_P \rangle$ such that $P \models S_1$. By definition, we have $o_P \models o_1$ and there exists a satisfaction relation $\mathcal{R}' \subseteq \{1, \ldots, n\} \times \{1, \ldots, k_1\}$ such that $o_P \mathcal{R}' o_1$.
Let $\mathcal{R}'' \subseteq \{1, \ldots, n\} \times \{1, \ldots, k_2\}$ such that $p \mathcal{R}'' u \iff \exists v \in \{1, \ldots, k_1\}$ with $p \mathcal{R}' v$ and $v \mathcal{R} u$. Let's show that $\mathcal{R}''$ is a satisfaction relation. First, it is clear that $A_2 \subseteq A_1 \subseteq A_P$.
Now, consider p, u such that $p \mathcal{R}'' u$. By definition, there exists v such that $p \mathcal{R}' v$ and $v \mathcal{R} u$. Since $V_P(p)\downarrow_{A_1} \in V_1(v)$ and $V_1(v)\downarrow_{A_2} \in V_2(u)$, we have $V_P(p)\downarrow_{A_2} \in V_2(u)$.

We now build a correspondance matrix Δ'' that satisfies the axioms of Definition 4. Let $x = M_p \in [0,1]^{1 \times n}$ and $\Delta' \in [0,1]^{n \times k_1}$ be a correspondance matrix witnessing $p \models v$. Let $y = x \times \Delta' \in [0,1]^{1 \times k_1}$. By definition of Δ', we have $\varphi_1(v)(y)$. Let $\Delta \in [0,1]^{k_1 \times k_2}$ be the correspondance matrix witnessing $v \preceq u$ and define $\Delta'' = \Delta' \times \Delta \in [0,1]^{n \times k_2}$. By Lemma 1, Δ'' is also a correspondance matrix. We prove that Δ'' satisfies the axioms of Definition 4.

1. *Let $1 \leq p' \leq n$ such that $M_{pp'} \neq 0$. As a consequence, $\sum_{j=1}^{k_1} \Delta'_{p'j} = 1$. We want to prove that $\sum_{j=1}^{k_2} \Delta''_{p'j} = 1$.*

$$\begin{aligned} \sum_{j=1}^{k_2} \Delta''_{p'j} &= \sum_{j=1}^{k_2} (\sum_{q=1}^{k_1} \Delta'_{p'q} \cdot \Delta_{qj}) \\ &= \sum_{q=1}^{k_1} \Delta'_{p'q} \cdot (\sum_{j=1}^{k_2} \Delta_{qj}) \end{aligned}$$

Let q such that $\Delta'_{p'q} \neq 0$. It is then clear that $y_q \geq M_{pp'} \cdot \Delta'_{p'q} > 0$. As Δ is a witness of $v \preceq u$, we have $\sum_{j=1}^{k_2} \Delta_{qj} = 1$. Finally, this implies that $\sum_{j=1}^{k_2} \Delta''_{p'j} = 1$.

2. *By construction,* $\varphi_2(u)(M_p \times \Delta'')$ *holds.*

3. *Let* p', u' *such that* $\Delta''_{p'u'} \neq 0$*. By construction, it is clear that there exists* v' *such that* $\Delta'_{p'v'} \neq 0$ *and* $\Delta_{v'u'} \neq 0$*. By definition of* Δ' *and* Δ*, this implies that* $p' \mathcal{R}' v'$ *and* $v' \mathcal{R} u'$*, thus* $p' \mathcal{R}'' u'$*.*

From 1-3, we can conclude that $\mathcal{R}''$ *is a satisfaction relation. Since* $o_P \mathcal{R}'' o_2$*, we have* $P \in [\![S_2]\!]$ *and* $[\![S_1]\!] \subseteq [\![S_2]\!]$*.*

□

A.8.2 Proof of Theorem 6

We suppose that the CMCs we consider in this proof are pruned. Moreover we only consider CMCs in single valuation normal form. Given two CMCs S_1 and S_2 such that $[\![S_1]\!] \subseteq [\![S_2]\!]$, we prove that $S_1 \preceq S_2$. The proof is structured as following.

1. • We define the relation $\mathcal{R}$ between S_1 and S_2.

$$R = \{(v, u) \mid \forall I, \forall p \in I,\ p \models v \Rightarrow p \models u\}$$

   We consider u and v such that $v \mathcal{R} u$ and prove that $\mathcal{R}$ satisfies Axiom (1) of the refinement relations.

   • Axiom (2) of the refinement relations : Given a distribution X on the outgoing transitions of v, we must find a correspondance matrix Δ satisfying Axioms $2(a)$, $2(b)$ and $2(c)$ of the refinement relation :

   – We consider a distribution X on the outgoing transitions from v and we build a MC I satisfying S_1 such that the outgoing probabilities of the state v_I are exactly X.
   – This leads to $v_I \models u$ and gives a correspondance matrix Δ_2, which we will take as our correspondance matrix Δ.
   – By definition, Δ satisfies the axioms $2(a)$ and $2(b)$ of the refinement relation.

2. As Δ comes from a satisfaction relation, the axiom $2(c)$ of the refinement relation is not so immediate. It tells us that if a coefficient $\Delta_{v'u'}$ is not 0, then there exists an implementation I and a state v'_I such that $v'_I \models v'$ and $v'_I \models u'$. What we need is that for all implementations I' and state p' such that $p' \models v'$, we have $p' \models u'$. **The rest of the proof is dedicated to proving that this statement being false leads to a contradiction**.

   Assuming there exists I' and p' such that $p' \models v'$ and $p' \not\models u'$, we build an implementation $\hat{I}$ from I and I' such that the state v' of $\hat{I}$ is syntactically equivalent to the state p'. We then prove that this state v' of $\hat{I}$ still satisfies the state u' of S_2 because it is a successor of v and S_2 is deterministic. As the state v' of $\hat{I}$ is syntactically equivalent to the state p' of I', this means that $p' \models u'$, which is a contradiction.

We now go through the mathematical foundations of this proof.

Proof :

Let $S_1 = \langle\{1,\dots,k_1\}, o_1, \varphi_1, A_1, V_1\rangle$ and $S_2 = \langle\{1,\dots,k_2\}, o_2, \varphi_2, A_2, V_2\rangle$ be two consistent and deterministic CMCs in single valuation normal form such that $A_2 \subseteq A_1$ and $[\![S_1]\!] \subseteq [\![S_2]\!]$.
First, remark that $S_1 \preceq S_2 \iff S_1' = \langle\{1,\dots,k_1\}, o_1, \varphi_1, A_2, V_1{\downarrow_{A_2}}\rangle \preceq S_2$. It is thus safe to suppose that $A_1 = A_2$. Similarly, if $I = \langle\dots,,A_I,V_I\rangle$ is a MC, we have $I \models S_1 \iff I' = \langle\dots,,A_1,V_I{\downarrow_{A_1}}\rangle \models S_1$. As a consequence, it is also safe to suppose that implementations have the same set of atomic propositions as S_1 and S_2.

1. *Let $\mathcal{R} \subseteq \{1,\dots,k_1\}\times\{1,\dots,k_2\}$ such that $v\,\mathcal{R}\,u$ iff for all MC I and state p of I, $p \models v \Rightarrow p \models u$. As we consider pruned CMCs, there exist implementations for all states.*

   Consider v and u such that $v\,\mathcal{R}\,u$.

   (a) *By definition of $\mathcal{R}$, there exists a MC I and a state p of I such that $p \models v$ and $p \models u$. Thus $V_I(p) \in V_1(v)$ and $V_I(p) \in V_2(u)$. As S_1 and S_2 are in single valuation normal form, $V_1(v)$ and $V_2(u)$ are singletons, so $V_1(v) = V_2(u)$.*

   (b) *Consider $x \in [0,1]^{1\times k_1}$ such that $\varphi_1(v)(x)$ and build the MC $I = \langle\{1,\dots,k_1\}, o_1, M,$ $A_1, V_1'\rangle$ such that for all $1 \le w \le k_1$,*
   - *$V_1'(w)$ is the only valuation T such that $V_1(w) = \{T\}$;*
   - *If $w \neq v$, the line M_w is any solution of $\varphi_1(w)$. One exists because S_1 is pruned;*
   - *$M_v = x$.*

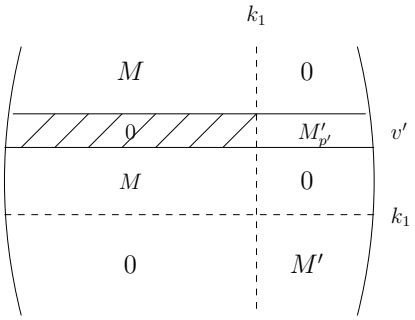
   When necessary, we will adress state w of I as w_I to differentiate it from state w of S_1. We will now build the correspondance matrix Δ.
   I clearly satisfies S_1 with a satisfaction relation $\mathcal{R}_1 = \mathsf{Identity}$, and $v_I \models v$. By hypothesis, we thus have $v_I \models u$. Consider $\mathcal{R}_2$ the satisfaction relation such that $v_I\,\mathcal{R}_2\,u$ and Δ_2 the corresponding correspondance matrix. Let $\Delta = \Delta_2$.

   (c) *As a consequence,*
   - *i. $\forall 1 \le i \le k_1, x_i \neq 0 \Rightarrow \sum_{j=1}^{k_2} \Delta_{ij} = 1$;*
   - *ii. $\varphi_2(u)(x \times \Delta)$ holds;*

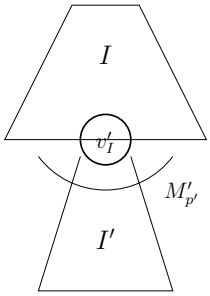
2. *Let v' be a state of S_1 such that If $x_{v'} \neq 0$ and $\Delta_{v'u'} \neq 0$. By definition of I and Δ, we have $v_I' \models v'$ and $v_I' \models u'$. We want to prove that for all implementations I' and state p' in I', $p' \models v'$ implies $p' \models u'$.*

   Suppose this is not the case. *There exists an implementation $I' = \langle\{1,\dots,n\}, o', M', A_1, V'\rangle$ and a state p' of I' such that $p' \models v'$ and $p' \not\models u'$. Let $\mathcal{R}'$ be the correspondance matrix witnessing $p' \models v'$.*

   Consider the MC $\hat{I} = \langle\{1,\dots,k_1,k_1+1,\dots,k_1+n\}, o_I, \hat{M}, A_1, \hat{V}\rangle$. Intuitively, the first k_1 states correspond to I and the next n states to I'. The state v_I'



(a) The transition matrix $\hat{M}$



(b) The MC $\hat{I}$

will be the link between the two and its outgoing transitions will be the ones of p'*. Define*

- $\hat{M}_{ij} = M_{i,j}$ *if* $1 \leq i, j \leq k_1$ *and* $i \neq v'$
- $\hat{M}_{v'j} = 0$ *if* $1 \leq j \leq k_1$
- $\hat{M}_{ij} = 0$ *if* $1 \leq i \leq k_1$ *and* $i \neq v'$ *and* $j > k_1$
- $\hat{M}_{v'j} = m'_{p',j-k_1}$ *if* $j > k_1$
- $\hat{M}_{ij} = 0$ *if* $i > k_1$ *and* $1 \leq j \leq k_1$
- $\hat{M}_{ij} = m'_{i-k_1,j-k_1}$ *if* $i > k_1$ *and* $j > k_1$.
- $\hat{V}(i) = V'_1(i)$ *if* $i \leq k_1$
- $\hat{V}(i) = V'(i - k_1)$ *if* $i > k_1$

We want to prove that $v'_{\hat{I}}$ *satisfies* u'*. This should imply that* $p'_{I'}$ *also satisfies* u'*, which is absurd.*

Consider the relation $\hat{\mathcal{R}}$ *between the states of* $\hat{I}$ *and the states of* S_1 *defined as follows :*

$$\hat{\mathcal{R}} = \{(q, w) \in R_1 \mid q \neq v'\} \cup \{(q, w) \mid (q - k_1)\, \mathcal{R}'\, w\} \cup \{(v', w) \mid p'\, \mathcal{R}'\, w\}$$

Intuitively, $\hat{\mathcal{R}}$ *is equal to* $\mathcal{R}_1$ *for the states* $q \leq k_1$*, except* v'*, and equal to* $\mathcal{R}'$ *for the states* $q > k_1$*. The states related to* $v'_{\hat{I}}$ *are the ones that were related to* p' *with* $\mathcal{R}'$*.*

We will show that $\hat{\mathcal{R}}$ is a satisfaction relation between $\hat{I}$ and S_1.

Let q, w such that $q\hat{\mathcal{R}}w$. For all the pairs where $q \neq v'_{\hat{I}}$, the conditions of the satisfaction relation obviously still hold because they held for $\mathcal{R}_1$ if $q \leq k_1$ and for $\mathcal{R}'$ otherwise. It remains to check the conditions for the pairs where $q = v'_{\hat{I}}$.

Consider w such that $v'_{\hat{I}}\hat{\mathcal{R}}w$.

- *(a) Because (v'_I) and $(p'_{I'})$ are both implementations of v', it is clear that $\hat{V}(v'_{\hat{I}}) = \hat{V}(p')$. As $p'\,\mathcal{R}'\,w$, we know that $V'(p') \in V_1(w)$. Thus, $\hat{V}(v'_{\hat{I}}) \in V_1(w)$.*
- *(b) Consider the correspondance matrix Δ' given by $p'\,\mathcal{R}'\,w$. Let $\hat{\Delta} \in [0,1]^{(k_1+n)\times k_1}$ such that $\hat{\Delta}_{ij} = 0$ if $i \leq k_1$, and $\hat{\Delta}_{ij} = \Delta'_{(i-k_1)j}$ otherwise.*
  - *i. We want to show that if $\hat{M}_{(v'_{\hat{I}})(w')} \neq 0$, then $\sum_{j=1}^{k_1} \hat{\Delta}_{w'j} = 1$. We know that $\hat{M}_{(v'_{\hat{I}})(w')} = 0$ if $w' \leq k_1$. Take $w' > k_1$ such that $\hat{M}_{(v'_{\hat{I}})(w')} \neq 0$. Then we know that $\hat{M}_{(v'_{\hat{I}})(w')} = M'_{p'(w'-k_1)}$. Because $\mathcal{R}'$ is a satisfaction relation, it implies that $\sum_{j=1}^{k_1} \Delta'_{(w'-k_1)j} = 1$. Thus, $\sum_{j=1}^{k_1} \hat{\Delta}_{w'j} = \sum_{j=1}^{k_1} \Delta'_{(w'-k_1)j} = 1$.*
  - *ii. We want to show now that $\varphi_1(w)(\hat{M}_{v'_{\hat{I}}} \times \hat{\Delta})$ holds. Let $1 \leq j \leq k_1$. We have*

$$[\hat{M}_{v'_{\hat{I}}} \times \hat{\Delta}]_j = \sum_{l=1}^{k_1+n} \hat{M}_{(v'_{\hat{I}})l} \cdot \hat{\Delta}_{lj} = 0 + \sum_{l=k_1+1}^{k_1+n} \hat{M}_{(v'_{\hat{I}})l} \cdot \hat{\Delta}_{lj}$$

$$= \sum_{l=1}^{n} M'_{p'l} \cdot \Delta'_{lj} = [M'_{p'} \times \Delta']_j$$

  As a consequence, $\hat{M}_{v'_{\hat{I}}} \times \hat{\Delta} = M'_{p'} \times \Delta'$. Since Δ' is a witness of $p'\,\mathcal{R}'\,w$, $\varphi_1(w)(M'_{p'} \times \Delta')$ holds. So does $\varphi_1(w)(\hat{M}_{v'_{\hat{I}}} \times \hat{\Delta})$.
  - *iii. We want to show that if $\hat{M}_{(v'_{\hat{I}})q} \neq 0$ and $\hat{\Delta}_{qw'} \neq 0$, then $q\hat{\mathcal{R}}w'$. We only need to consider $q > k_1$ (since otherwise $\hat{M}_{(v'_{\hat{I}})q} = 0$) and w' such that $\hat{\Delta}_{qw'} \neq 0$. In this case, $\hat{M}_{(v'_{\hat{I}})q} = M'_{p'(q-k_1)} \neq 0$ and $\Delta'_{(q-k_1)w'} \neq 0$. As Δ' is a witness of $p'\,\mathcal{R}'\,w$, it has to be that $(q-k_1)\,\mathcal{R}'\,w'$, which implies, by definition of $\hat{\mathcal{R}}$, that $q\hat{\mathcal{R}}w'$.*

Finally $\hat{I}$ satisfies S_1, and in particular, $v_{\hat{I}} \models v$. As $v\,\mathcal{R}\,u$, it implies that $v_{\hat{I}} \models u$. As a consequence, there exists $\Delta'' \in [0,1]^{(k_1+n)\times k_2}$ such that $\varphi_2(u)(\hat{M}_{v_{\hat{I}}} \times \Delta'')$.

- *(A) Consider $u'' \neq u'$ such that $V_2(u'') = V_2(u')$. Due to determinism of S_2, and to the fact that u' is accessible from u, we have $[\hat{M}_{v_{\hat{I}}} \times \Delta'']_{u''} = 0$. Since $\hat{M}_{(v_{\hat{I}})(v'_{\hat{I}})} \neq 0$ and $\hat{M}_{(v_{\hat{I}})(v'_{\hat{I}})} \cdot \Delta''_{(v'_{\hat{I}})u''}$ is part of $[\hat{M}_{v_{\hat{I}}} \times \Delta'']_{u''}$, we must have $\Delta''_{(v'_{\hat{I}})u''} = 0$.*

(B) Consider u''' such that $V(u''') \neq V(u')$. It is clear that $\Delta''_{(v'_{\hat{I}})u'''} = 0$ since Δ'' is witnessing satisfaction between $\hat{I}$ and S_2.

(C) Moreover, we know that $\hat{M}_{(v_{\hat{I}})(v'_{\hat{I}})} \neq 0$. Thus, $\sum_{j=1}^{k_2} \Delta''_{v'_{\hat{I}}j} = 1$.

According to (A) and (B), the only non-zero value in the sum in (C) must be $\Delta''_{(v'_{\hat{I}})u'}$. Since Δ'' is witnessing $\hat{I} \models S_2$, this means that $v'_{\hat{I}} \models u'$.

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

Finally, we have by hypothesis that $[\![S_1]\!] \subseteq [\![S_2]\!]$, which implies that $o_1 \mathcal{R} o_2$. □

Centre de recherche INRIA Rennes – Bretagne Atlantique
IRISA, Campus universitaire de Beaulieu - 35042 Rennes Cedex (France)

Centre de recherche INRIA Bordeaux – Sud Ouest : Domaine Universitaire - 351, cours de la Libération - 33405 Talence Cedex
Centre de recherche INRIA Grenoble – Rhône-Alpes : 655, avenue de l'Europe - 38334 Montbonnot Saint-Ismier
Centre de recherche INRIA Lille – Nord Europe : Parc Scientifique de la Haute Borne - 40, avenue Halley - 59650 Villeneuve d'Ascq
Centre de recherche INRIA Nancy – Grand Est : LORIA, Technopôle de Nancy-Brabois - Campus scientifique
615, rue du Jardin Botanique - BP 101 - 54602 Villers-lès-Nancy Cedex
Centre de recherche INRIA Paris – Rocquencourt : Domaine de Voluceau - Rocquencourt - BP 105 - 78153 Le Chesnay Cedex
Centre de recherche INRIA Saclay – Île-de-France : Parc Orsay Université - ZAC des Vignes : 4, rue Jacques Monod - 91893 Orsay Cedex
Centre de recherche INRIA Sophia Antipolis – Méditerranée : 2004, route des Lucioles - BP 93 - 06902 Sophia Antipolis Cedex

Éditeur
INRIA - Domaine de Voluceau - Rocquencourt, BP 105 - 78153 Le Chesnay Cedex (France)
http://www.inria.fr
ISSN 0249-6399