Probabilistic Contracts for Component-based Design

Gregor Gössler, Dana N. Xu, Alain Girault

Probabilistic Contracts for Component-based Design

Gregor Gössler, Dana N. Xu, Alain Girault

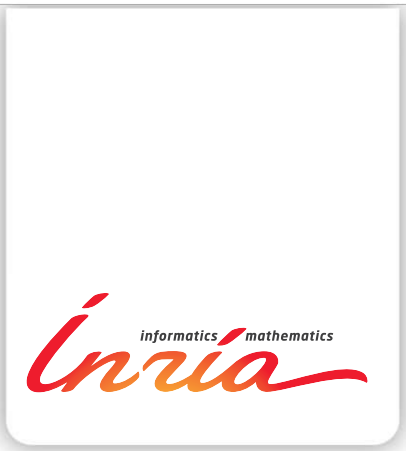
RESEARCH REPORT

N° 7328

July 2010

Project-Teams Pop Art, Gallium

ISSN 0249-6399 ISRN INRIA/RR--7328--FR+ENG



Probabilistic Contracts for Component-based Design*†

Gregor Gössler, Dana N. Xu, Alain Girault

Project-Teams Pop Art, Gallium

Research Report n° 7328 — version 2‡ — initial version July 2010 — revised version June 2012 — 49 pages

Abstract: We define a probabilistic contract framework for describing and analysing component-based embedded systems, based on the theory of Interactive Markov Chains (IMC). A contract specifies the assumptions a component makes on its context and the guarantees it provides. Probabilistic transitions allow for uncertainty in the component behavior, e.g., to model observed black-box behavior (internal choice) or reliability. An interaction model specifies how components interact.

We provide the ingredients for a component-based design flow, including (1) contract satisfaction and refinement, (2) parallel composition of contracts over disjoint, interacting components, and (3) conjunction of contracts describing different requirements over the same component. Compositional design is enabled by congruence of refinement.

Key-words: component, probabilistic contract, refinement, composition

* supported by the European project COMBEST no. 215543
† The final publication is available at springerlink.com
‡ Changes include an improvement of the framework and corrections of errors.

RESEARCH CENTRE
GRENOBLE – RHÔNE-ALPES

Inovallée
655 avenue de l'Europe Montbonnot
38334 Saint Ismier Cedex

Contrats probabilistes pour la conception à base de compostants

Résumé : Nous définissons un cadre formel de contrats probabilistes pour décrire et analyser des systèmes embarqués à base de composants. Ce cadre formel est fondé sur la théorie des chaînes de Markov interactives (IMC). Un contrat spécifie les hypothèses qu'un composant fait quant à son contexte et les garanties qu'il fournit. Des transitions probabilistes permettent de raisonner sur les incertitudes dans le comportement d'un composant, par exemple pour modéliser un comportement de type boîte noire (choix interne) ou sa fiabilité. Un modèle d'interaction spécifie la faqn dont des composants interagissent.

Nous fournissons tous les ingrédients pour le flot de conception à base de composants, incluant (1) la satisfaction et le raffinement de contrat, (2) la composition parallèle de contrats portant sur des composants disjoints qui interagissent, et (3) la conjonction de contrats décrivant des comportements différents d'un même composant. Notre cadre formel permet de faire de la conception compositionnelle grâce à la congruence de l'opération de raffinement.

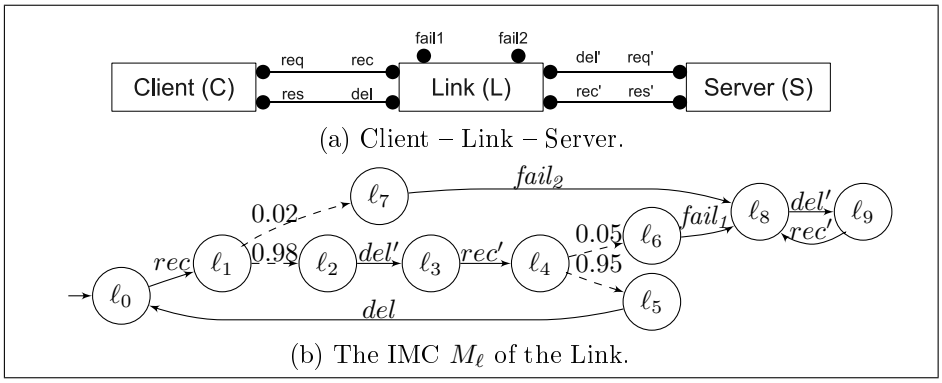
Mots-clés : composant, contrat probabiliste, raffinement, composition

Contents

1 Introduction

Embedded and distributed systems often encompass unreliable software or hardware components, as it may be technically or economically impossible to make a system entirely reliable. As a result, system designers have to deal with probabilistic specifications such as "the probability that this component fails at this point of its behavior is less than or equal to 10^{-6}". More generally, uncertainty in the observed behavior is introduced by abstraction of black-box behavior of components, the environment, or the execution platform. In this paper, we introduce a framework for the design of correct systems from probabilistic, interacting components.

Figure 1(a) shows a Link system that transmits data between a Client and a Server. The Link receives a request from the Client and encodes the request before sending it to the Server. The encoding process fails with probability 0.02. After receiving a response from the Server, it decodes the data before delivering it to the Client. To model components, we use a variant of Interactive Markov Chain (IMC) framework [9] with discrete time semantics, which combines labeled transition systems (LTS) and Markov chains. Figure 1(b) shows an IMC



(a) Client – Link – Server.

(b) The IMC M_ℓ of the Link.

Figure 1: An example of IMC: a Client-Link-Server.

describing the Link component of Figure 1(a). From its initial state ℓ_0, the Link goes to state ℓ_1 as soon as it receives (rec) a request from a Client; the probability that it delivers (del') this request to the Server is 0.98 and the probability that it fails to deliver it to the Server is 0.02. The Link goes to state ℓ_4 immediately after receiving a response (rec') from the Server; the probability that it delivers (del) the response to the Client is 0.95 and the probability of failing to do so is 0.05. In state ℓ_8, the Link may still communicate with the Server regarding other services, but will not deliver any response to the Client.

Components communicate through interactions, that is, synchronized action transitions. Interactions are essential in component frameworks because they allow the modeling of how components cooperate and communicate. We use the BIP framework [8] to model interactions between components.

Since the deploying context of a component is not known at design time, we use *probabilistic contracts* to specify and reason about the correct behaviors of a component. Contracts were first introduced in [13]. They allow the designer to specify what a component can expect from its context, what it must guarantee, and explicitly limit the responsibilities of both.

The framework we propose here allows us to model components, their interactions, and the uncertainty in their observed behavior (§2). It supports the different steps classically found in a design flow: refinement, satisfaction, and projection (§3), parallel composition (§4.1), and conjunction (shared refinement) (§4.2). We prove that these operations satisfy the desired properties of *independent implementability* and *congruence* for parallel composition, and *soundness* for conjunction. The features of our framework are thus the following:

- refinement is compositional, that is, contracts over different components can be refined and implemented independently;
- the parallel composition of two contracts is satisfied by the parallel composition of any two implementations of the contracts; and
- several contracts C_i over the same component may be used to independently specify different requirements, possibly over different subsets of the component interactions. The conjunction is a common refinement of all C_i.

As pointed out in [2], the conjunction of probabilistic specifications is non trivial, since a straight-forward approach would introduce spurious behaviors.

2 Components and Contracts

We use Interactive Markov Chains [9] with discrete-time semantics to model the behavior of components.

Definition 1 (Probability distribution). *A* probability distribution *over a finite set X is a function $f : X \to [0,1]$ such that $\sum_{x \in X} f(x) = 1$.*

Definition 2 (Interactive Markov Chain (IMC)). *An IMC is a tuple $(\mathcal{Q}, \mathcal{A}, \to, \pi, s_0)$ where:*

- *$\mathcal{Q}$ is a nonempty finite set of states, partitioned into $\mathcal{Q}^p$, the set of probabilistic states, and $\mathcal{Q}^a$, the set of action states;*
- *A is a finite alphabet of actions;*
- *$\to \subseteq \mathcal{Q}^a \times \mathcal{A} \times \mathcal{Q}$ is an action transition relation;*
- *$\pi : \mathcal{Q}^p \to (\mathcal{Q} \to [0,1])$ is a transition probability function such that, for each $s \in \mathcal{Q}^p$, $\pi(s)$ is a probability distribution over $\mathcal{Q}$;*
- *s_0 is the initial state.*

Each action state in $\mathcal{Q}^a$ may have outgoing action transitions — also called *non-deterministic transitions* in the literature — like those in a labeled transition system (LTS). Each probabilistic state in $\mathcal{Q}^p$ has outgoing probabilistic transitions like those in a Markov chain. Probability distributions on states are memoryless, i.e., the future of an IMC depends only on the current state, not on past choices. For example, in Figure 1(b), the probabilistic choice that the Link delivers the response to the Client (i.e., $\pi(\ell_4)(\ell_5) = 0.95$) is independent from the probabilistic choice of delivering a request to the Server (i.e., $\pi(\ell_1)(\ell_2) = 0.98$).

Notation: For convenience, we sometimes write the transition probability function π as a transition relation $\dashrightarrow \subseteq \mathcal{Q}^p \times [0,1] \times \mathcal{Q}$ such that:

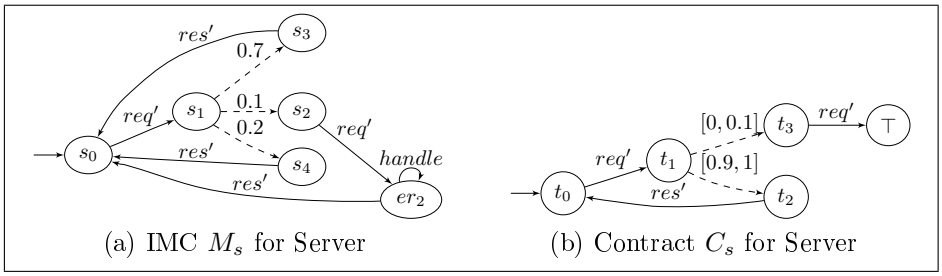
$$\dashrightarrow = \{(s, p, s') \mid s \in \mathcal{Q}^p \wedge s' \in \mathcal{Q} \wedge p = \pi(s)(s')\}$$

Graphically, we only depict the $\dashrightarrow$ transitions labeled with a non null probability (see Figure 2(a)).

We introduce *contracts* as a finite specification for a possibly infinite number of components modeled by IMCs. In contrast to IMCs, the probabilistic transitions of a contract are labeled with probability *intervals*, similar to the formalism of [10, 17]. Moreover, two distinct states $\top$ and $\bot$ are used to distinguish the assumptions on the use of the component from the guarantees it provides.

Definition 3 (Contract). *A contract is a tuple $(\mathcal{Q}, \mathcal{A}, \to, \sigma, t_0)$ where:*

- *$\mathcal{Q}$ is a nonempty finite set of states, partitioned into $\mathcal{Q} = \mathcal{Q}^p \cup \mathcal{Q}^a \cup \{\top, \bot\}$, where $\mathcal{Q}^p$ is the set of probabilistic states, $\mathcal{Q}^a$ is the set of action states, and $\top$ and $\bot$ are distinct states without any outgoing transitions;*
- *A is a finite alphabet of actions;*



(a) IMC M_s for Server (b) Contract C_s for Server

Figure 2: Contract Examples

- $\rightarrow \subseteq \mathcal{Q}^a \times \mathcal{A} \times \mathcal{Q}$ *is the action transition relation;*
- $\sigma : \mathcal{Q}^p \rightarrow (\mathcal{Q} \rightarrow 2^{[0,1]})$ *is a transition probability predicate, associating with each pair of states in* $\mathcal{Q}^p \times \mathcal{Q}$ *an interval of probabilities;*
- t_0 *is the initial state.*

Let $C_\perp = (\{\perp\}, \emptyset, \emptyset, \emptyset, \perp)$ *be the* inconsistent contract.

Notations: We also write σ as a transition relation $\dashrightarrow \subseteq \mathcal{Q}^p \times 2^{[0,1]} \times \mathcal{Q}$ such that $\dashrightarrow = \{(s, P, s') \mid s \in \mathcal{Q}^p \wedge s' \in \mathcal{Q} \wedge P = \sigma(s)(s')\}$. We write $q \overset{>0}{\dashrightarrow} q'$ if $\exists p > 0 : p \in \sigma(q, q')$ and denote by $\overset{>0}{\dashrightarrow}^+$ the transitive closure of $\overset{>0}{\dashrightarrow}$. Graphically, we only depict the $\overset{>0}{\dashrightarrow}$ transitions (see Figure 2(b)). Let $\rightsquigarrow = \rightarrow \cup \overset{>0}{\dashrightarrow}$, and let $\rightsquigarrow^*$ be the reflexive and transitive closure of $\rightsquigarrow$. A state $q \in \mathcal{Q}$ is *reachable* if and only if $t_0 \rightsquigarrow^* q$. A contract is *consistent* if $\perp$ is not reachable.

The meaning of a contract C over a component M is the following:

- a transition $s \xrightarrow{a} \top$ specifies the *assumption* of the component M that an interaction involving action a does not occur in state s;
- in an action state s, an action a labeling a transition not leading to $\top$ specifies the *guarantee* of the component M that a is enabled in s; conversely, the absence of any outgoing transition labeled with a specifies the *guarantee* that an interaction involving a will not occur;
- the $\top$ state represents the fact that the *assumption* has been violated, and henceforth, the component M can behave arbitrarily;
- the $\perp$ state stands for "inconsistent" and means that M cannot satisfy the contract C any more;
- a transition $s \overset{[a,b]}{\dashrightarrow} t$ specifies an interval of allowed transition probabilities, i.e., the component M has a transition $s \overset{p}{\dashrightarrow} t$ with any $p \in [a, b]$.

Hypothesis 1. *We require that the target states of probabilistic transitions are action or probabilistic states: if* $q \overset{>0}{\dashrightarrow} q'$ *then* $q' \notin \{\top, \perp\}$.

Example 1. *The contract* C_s *in Figure 2(b) specifies that, after the Server receives a request* req'*, the probability that it reaches state* t_3 *is within* $[0, 0.1]$*; in state* t_3*, it* assumes *that the environment does not provide* req'*; if this occurs,*

its implementation is not bound by C_s any more; the probability that it reaches t_2 from t_1 is within $[0.9, 1]$*; in state t_2, it* guarantees *to send a response (res′). In §3, we show how to check that the IMC M_s (in Figure 2(a)) satisfies the contract C_s.*

$$\begin{array}{rrcl} \forall \alpha \in \mathcal{A}, & \lfloor s_1 \xrightarrow{\alpha} s_2 \rfloor & = & s_1 \xrightarrow{\alpha} s_2 \\ \forall p \in [0,1], & \lfloor s_1 \overset{p}{\dashrightarrow} s_2 \rfloor & = & s_1 \overset{[p,p]}{\dashrightarrow} s_2 \end{array}$$

Figure 3: Rules for lifting an IMC to a contract.

From the definitions of IMC and contract, we can see that an IMC can be trivially converted into a contract. For this, we define a lifting operator $\lfloor . \rfloor$ (Figure 3). We use the same notation $\dashrightarrow$ to represent both kinds of probabilistic transitions (i.e., those in an IMC and in a contract).

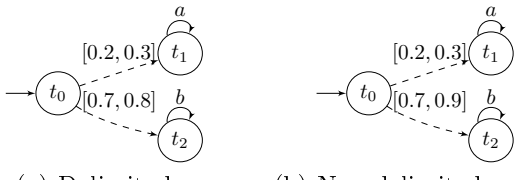
$$\begin{array}{rcll} \lceil n \rceil & = & \text{if } n > 1 \text{ then } 1 \text{ else } n & \\ [\ell_1, u_1] + [\ell_2, u_2] & = & [\ell_1 + \ell_2, \lceil u_1 + u_2 \rceil] & \text{[F1]} \\ [\ell_1, u_1] * [\ell_2, u_2] & = & [\ell_1 * \ell_2, u_1 * u_2] & \text{[F2]} \\ k * [\ell, u] & = & [k * \ell, k * u] \quad \text{for } k \in [0,1] & \text{[F3]} \end{array}$$

Figure 4: Operations on probability intervals.

In Figure 4, we define some useful operations related to probability intervals. When summing up the upper bounds, the ceiling for a probability value is 1, so if the summation is greater than 1, we let the result be 1 (operator $\lceil . \rceil$).

Definition 4 (Delimited contract)**.** *A contract $C = (\mathcal{Q}, \mathcal{A}, \rightarrow, \sigma, t_0)$ is delimited [6] iff $\forall s \in \mathcal{Q}^p$, $\forall s' \in \mathcal{Q}$, and $\forall p \in \sigma(s)(s')$: $1 - p \in \sum_{s'' \in \mathcal{Q} \setminus \{s'\}} \sigma(s)(s'')$.*

Definition 4, borrowed from [6], states that, for any probability chosen in any probabilistic transition's interval, it is always possible to choose probabilities in the intervals of all the remaining transitions outgoing from the same state such that the sum is 1.



(a) Delimited. (b) Non-delimited.

Figure 5: Delimited contract and non-delimited contract.

Example 2. *Figure 5(a) shows a delimited contract: for all $p \in [0, 2, 0.3]$, we can find $p' \in [0.7, 0.8]$ such that $p + p' = 1$ and vice versa. Figure 5(b) shows a contract that is not delimited. However, we can* cut *[6] the redundant sub-interval [0.8,0.9] from the interval [0.7,0.9] to obtain the delimited contract of Figure 5(a).*

3 Contract Refinement

System synthesis involves refining a contract until an implementation is obtained. We therefore define formally the notion of contract refinement.

3.1 Refinement and Satisfaction

We first define contract refinement, and give thereafter some explanations.

Definition 5 (Contract refinement)**.** *Let* $C_1 = (\mathcal{Q}_1, \mathcal{A}, \rightarrow_1, \sigma_1, s_0)$ *and* $C_2 = (\mathcal{Q}_2, \mathcal{A}, \rightarrow_2, \sigma_2, t_0)$ *be two contracts. A relation* $\preceq \subseteq \mathcal{Q}_1 \times \mathcal{Q}_2$ *is a* simulation *if for all* $s \preceq t$ *we have:*

1. $s = \top \implies t = \top$.
2. $t = \bot \implies s = \bot$.
3. *If* $(s,t) \in \mathcal{Q}_1^a \times (\mathcal{Q}_2^a \cup \{\top\})$ *then*
   (a) $\forall t' \neq \top \in \mathcal{Q}_2,\ (t \xrightarrow{\alpha}_2 t') \implies (\exists s' \in \mathcal{Q}_1,\ s \xrightarrow{\alpha}_1 s' \wedge s' \preceq t')$;
   (b) $\forall s' \in \mathcal{Q}_1,\ (s \xrightarrow{\alpha}_1 s') \implies (t = \top \vee \exists t' \in \mathcal{Q}_2,\ t \xrightarrow{\alpha}_2 t' \wedge s' \preceq t')$.
4. *If* $(s,t) \in \mathcal{Q}_1^p \times \mathcal{Q}_2^p$ *then there exists a function* $\delta : \mathcal{Q}_1 \times \mathcal{Q}_2 \rightarrow [0,1]$*, which, for each* $s' \in \mathcal{Q}_1$*, gives a probability distribution* $\delta(s')$ *over* $\mathcal{Q}_2$*, such that for every probability distribution* f *over* $\mathcal{Q}_1$ *with* $f(s') \in \sigma_1(s)(s')$ *and* $\forall t' \in \mathcal{Q}_2$*,*
$$\sum_{s' \in \mathcal{Q}_1} f(s') * \delta(s')(t') \in \sigma_2(t)(t') \text{ and } \forall s' \in \mathcal{Q}_1 : \big(\delta(s')(t') > 0 \implies s' \preceq t'\big)$$
5. *If* $(s,t) \in \mathcal{Q}_1^a \times \mathcal{Q}_2^p$ *then* $\exists t^a \in \mathcal{Q}_2^a : t \xrightarrow{>0}{}^{+}_2 t^a \wedge s \preceq t^a$ *and* $\forall t' \in \mathcal{Q}_2$, $\big(t \xrightarrow{>0}_2 t' \implies s \preceq t'\big)$.
6. *If* $(s,t) \in \mathcal{Q}_1^p \times \mathcal{Q}_2^a$ *then* $\exists s^a \in \mathcal{Q}_1^a : s \xrightarrow{>0}{}^{+}_1 s^a \wedge s^a \preceq t$ *and* $\forall s' \in \mathcal{Q}_1$, $\big(s \xrightarrow{>0}_1 s' \implies s' \preceq t\big)$.

It can be shown that a greatest simulation relation, called refinement and noted $\leq$*, exists.* C_1 *refines* C_2 *(written* $C_1 \leq C_2$*) iff* $s_0 \leq t_0$.

In Definition 5, conditions (1) and (2) ensure that C_1 makes no stronger assumptions on the context than C_2, and that the inconsistent state $\bot$ is only refined by itself. Since Definition 5 defines $\leq$ as the greatest relation, this implies that for any state s, $\bot \leq s$ and $s \leq \top$.

Condition (3a) says that any action transition accepted by C_2 must also be accepted by C_1. In contrast, action transitions leading to $\top$ (i.e., violating the assumption) do not need to be present in the refinement C_1. This is why we have $\forall t' \neq \top$ in condition (3a). On the other hand, condition (3b) says that each action transition of C_1 must also be enabled in C_2, unless C_2 is in the $\top$ state. Condition (4), adapted from [10], deals with refinement among probabilistic states. Intuitively, $s \preceq t$ if there exists a function δ that distributes the

probabilities of transitions from s to all successor states s' onto the transitions from t to its successors t', such that the sum of the probability fractions (i.e., $f(s') * \delta(s')(t')$) is in the range $\sigma_2(t)(t')$; this is illustrated in Example 4.

Condition (5) says that an action state s refines a probabilistic state t if it refines all action states reachable with a path of positive probabilities from t. Finally, condition (6) is symmetrical to condition (5).

In Section 2, we gave an intuitive explanation of contracts: transitions leading to $\top$ model the violation of the assumption, whereas action transitions not leading to $\top$ model the guarantee that the transition has to be offered. The following example shows that Definition 5 is consistent with the usual contravariant notion of contract refinement requiring that the refining contract has a weaker assumption and a stronger guarantee.

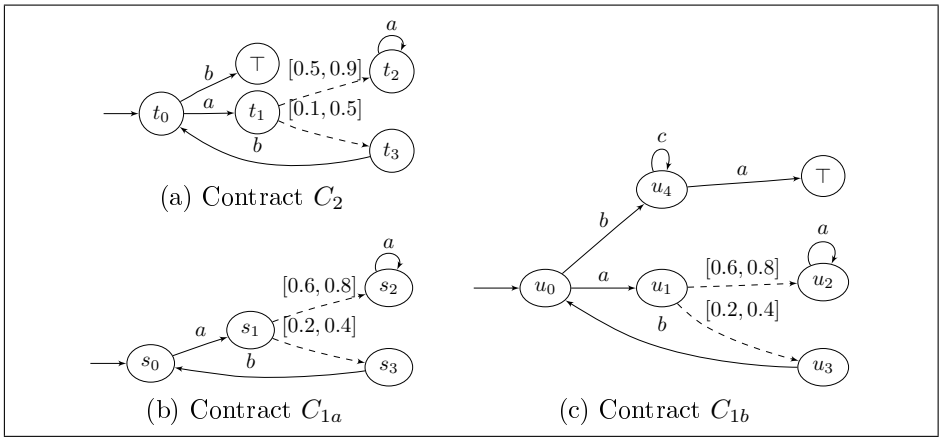


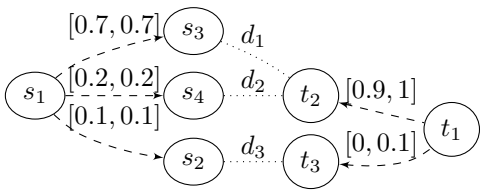
Figure 6: Stronger guarantee and weaker assumption

Example 3. *In Figure 6(a), the contract C_2 says that, in the state t_0, the action b is assumed not to occur; if an interaction involving b occurs (and the environment violates the assumption of C_2), then a component implementing C_2 is no longer bound by C_2; i.e., it can do anything after the action b is synchronized. The contract C_2 also says that, in the state t_0, the action a is guaranteed to be offered. It follows that a contract can refine C_2 in different ways, as shown in Figure 6:*

(1) $C_{1a} \leq C_2$: the contract C_{1a} does not offer action b in state s_0.

(2) $C_{1b} \leq C_2$: the contract C_{1b} offers action b in state u_0. If the b is synchronized with its environment, it reaches state u_4, from which C_{1b} can perform any action.

Both in C_{1a} and C_{1b}, the action a is guaranteed in state s_0 and u_0 respectively. It is also easy to check that $s_1 \leq t_1$ as the probabilistic transition leading to s_2 has a tighter *interval and $s_2 \leq t_2$, and similarly for the transition leading to s_3. This means that both C_{1a} and C_{1b} have stronger guarantees than C_2. At the same time, the transition labeled by b leading from state t_0 to $\top$ has been removed in C_{1a} and replaced with a transition leading to a state different from $\top$ in C_{1b}, thus weakening the assumption of C_2. For instance, contract C_2*



(1) $p_2 \in [0.1, 0.1]$
(2) $p_3 \in [0.7, 0.7]$
(3) $p_4 \in [0.2, 0.2]$
(4) $p_2 + p_3 + p_4 = 1$
(5) $p_3 * d_1 + p_4 * d_2 \in [0.9, 1]$
(6) $p_2 * d_3 \in [0, 0.1]$

Figure 7: Left: Contract refinement $s_1 \leq t_1$. Right: Constraints to be checked.

assumes action b not to occur, whereas C_{1a} guarantees not to offer b in state s_0. On the other hand, u_0 accepts more behaviors by the environment than t_0 without reaching $\top$.

We define the satisfaction of a contract by an IMC as the refinement of the contract by the lifted IMC (i.e., written in the form of a contract).

Definition 6 (Contract satisfaction)**.** *An IMC M satisfies a contract C (written $M \models C$) iff $\lfloor M \rfloor \leq C$.*

Example 4. *We illustrate in Figure 7 how to check that the contracts of Figure 2 are such that $\lfloor M_s \rfloor \leq C_s$, in particular, $s_1 \leq t_1$. It is easy to check that $s_3 \leq t_2$, $s_4 \leq t_2$, and $s_2 \leq t_3$. According to Condition (4) in Definition 5, we must find for each $s_i \in \{s_2, s_3, s_4\}$ a probability distribution $\delta(s_i)$ over $\{t_2, t_3\}$ such that $\sum_{i \in \{2,3,4\}, j \in \{2,3\}} f(s_i) * \delta(s_i)(t_j) \in \sigma_2(t_1)(t_j)$ — where f is the probability distribution over $\{s_2, s_3, s_4\}$ with $f(s_2) = 0.1$, $f(s_3) = 0.7$, and $f(s_4) = 0.2$ —, and $\delta(s_i)(t_j) = 0$ if $s_i \not\leq t_j$. In Figure 7, $\delta(s_3)(t_2) = d_1$, $\delta(s_4)(t_2) = d_2$, $\delta(s_2)(t_3) = d_3$ (all three represented by dotted lines), and $\delta(s_i)(t_j) = 0$ for all other pairs of states. We must thus check that for each tuple (p_2, p_3, p_4) satisfying the constraints (1) to (4) in Figure 7, the constraints (5) and (6) are implied. As each $\delta(s_i)$ is a probability distribution, we obtain for our example $d_1 = d_2 = d_3 = 1$. (Note that if we had $s_2 \leq t_2$ as well with weight d_4 from s_2 to t_2, we would have another constraint $d_3 + d_4 = 1$, and (5) would become $p_3 * d_1 + p_4 * d_2 + p_2 * d_4 \in [0.9, 1]$.) Condition (4) can be checked efficiently by requiring the set inclusion to hold for the bounds of interval $\sigma(s)(s')$, using a linear programming solver.*

Definition 7 (Models of contracts)**.** *The set of models of a contract C (written $\mathcal{M}(C)$) is the set of IMCs that satisfy C: $\mathcal{M}(C) = \{M \mid M \models C\}$.*

It can be checked that the inconsistent contract $C_\perp$, consisting only of the state $\perp$, does not have any model.

Definition 8 (Semantical equivalence)**.** *Contracts C_1 and C_2 are semantically equivalent (written $C_1 \equiv C_2$) iff $\mathcal{M}(C_1) = \mathcal{M}(C_2)$.*

Lemma 1 (Reflexivity of refinement)**.** *For all contracts $C = (\mathcal{Q}, \mathcal{A}, \rightarrow, \sigma, s_0)$, we have $C \leq C$, and for any state $s \in \mathcal{Q}$, we have $s \leq s$.*

Proof. Definition 5 (1)–(3) are trivially satisfied for $\{(s,t) \mid s = t\}$. Definition 5 (4) is satisfied with $\delta(s)(s) = 1$ and $\delta(s)(t) = 0$ for $s \neq t$. Finally, Definition 5 (5)–(6) are irrelevant for $\{(s,t) \mid s = t\}$. □

Lemma 2 (Transitivity of refinement)**.** *For all contracts C_1, C_2 and C_3, if $C_1 \leq C_2$ and $C_2 \leq C_3$, then $C_1 \leq C_3$.*

Proof. See appendix A.1. □

Corollary 1. *For all IMC M and contracts C_1 and C_2, we have:*

1. *if $M \models C_1$ and $C_1 \leq C_2$, then $M \models C_2$;*
2. *if $C_1 \leq C_2$, then $\mathcal{M}(C_1) \subseteq \mathcal{M}(C_2)$;*
3. *if $C_1 \leq C_2$ and $C_2 \leq C_1$, then $C_1 \equiv C_2$.*

3.2 Bisimulation

We adapt the usual notion of bisimulation to contracts, and define reduction of a contract with respect to bisimulation.

Definition 9 (Bisimulation $\simeq$)**.** *Given two contracts $C_1 = (\mathcal{Q}_1, \mathcal{A}, \rightarrow_1, \sigma_1, s_0)$ and $C_2 = (\mathcal{Q}_2, \mathcal{A}, \rightarrow_2, \sigma_2, t_0)$, a relation $\simeq \subseteq \mathcal{Q}_1 \times \mathcal{Q}_2$ is a* bisimulation *if both $\simeq$ and $\simeq^{-1} = \{(t, s) \mid s \simeq t\}$ are simulations.*

C_1 and C_2 are bisimilar (written $C_1 \simeq C_2$) iff $s_0 \simeq t_0$, where $\simeq$ is the greatest bisimulation.

Definition 10 (Reduction modulo $\simeq$ and reduced contract $\overline{C}$)**.** *Let $C = (\mathcal{Q}, \mathcal{A}, \rightarrow, \sigma, s_0)$ be a contract and $\simeq$ be a bisimulation over $\mathcal{Q}$. For all $s \in \mathcal{Q}$, let $\mathcal{C}_s = \{q \in \mathcal{Q} \mid s \simeq q\}$ be the equivalence class of s. Let $\mathcal{C} = \{\mathcal{C}_s \mid s \in \mathcal{Q}\}$. The reduced contract, written $C_{/\simeq}$, is $(\mathcal{C}, \mathcal{A}, \rightarrow_\simeq, \sigma_\simeq, \mathcal{C}_{s_0})$ with $\mathcal{C}^p = \{c \in \mathcal{C} \mid \forall s \in c : s \in \mathcal{Q}^p\}$ and $\mathcal{C}^a = \mathcal{C} \setminus (\mathcal{C}^p \cup \{\top, \bot\})$ such that, $\forall s = \{s_1, \ldots, s_m\}, t = \{t_1, \ldots, t_n\} \in \mathcal{C}$, we have:*

(a) $s \xrightarrow{\alpha}_\simeq t$ iff $\exists i, j : s_i \xrightarrow{\alpha} t_j$, and

(b) $\sigma_\simeq(s, t) = \sum_{1 \leq j \leq n} \sigma(s_1, t_j)$ iff $s \in \mathcal{C}^p$.

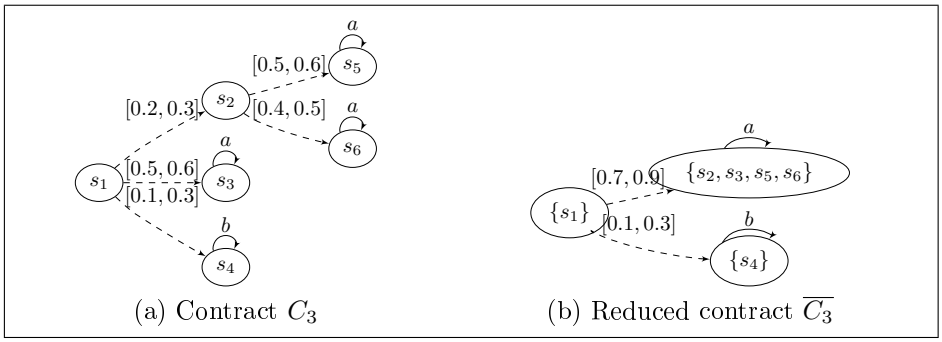
If $\simeq$ is the greatest bisimulation then we write $\overline{C}$ for $C_{/\simeq}$.

Notice that an equivalence class may contain both action and probabilistic states. For each probabilistic state $s_i \in s$, the probabilities of transitions to states $t_j \in t$ are summed up (it does not matter which of the transitions is taken since all the successors t_j are equivalent). This sum is the transition probability from s_i to some state in t. By definition of $\simeq$, the sum is the same for all $s_i \in s$, thus we pick $\sigma(s_1, t_j)$.

Example 5. *By Definition 10, we can reduce the contract C_3 of Figure 8(a) to $\overline{C_3}$ of Figure 8(b). There are 3 equivalence classes: $\{s_1\}$, $\{s_4\}$ and $\{s_2, s_3, s_5, s_6\}$. By Definition 10(b), we sum up the (lower bound and upper bound of) transitions from s_1 to s_2 and from s_1 to s_3.*

Lemma 3 (Bisimilarity of reduction)**.** *For any contract C, we have $\overline{C} \simeq C$.*

Proof. Let $C = (\mathcal{Q}, \mathcal{A}, \rightarrow, \sigma, s_0)$ and $C_{/\simeq} = (\mathcal{C}, \mathcal{A}, \rightarrow_\simeq, \sigma_\simeq, \mathcal{C}_{s_0})$. By Definition 10 we have $s_0 \in \mathcal{C}_{s_0}$ and thus $s_0 \simeq \mathcal{C}_{s_0}$ and $\overline{C} \simeq C$. □



(a) Contract C_3 (b) Reduced contract $\overline{C_3}$

Figure 8: A reduced contract.

Definition 11 (Deadend freedom)**.** *A delimited contract $C = (\mathcal{Q}, \mathcal{A}, \rightarrow, \sigma, s_0)$ is deadend-free if any reachable state has an outgoing transition in $(\mathcal{Q} \setminus \{\top\}, \mathcal{A}, \rightarrow', \sigma, s_0)$ where $\rightarrow' = \{(q, a, q') \in \rightarrow \mid q' \neq \top\}$.*

In other words, C is deadend-free if all reachable action states have a successor state other than $\top$. In particular, $\bot$ is unreachable in any deadend-free contract since $\bot$ has no successor at all.

Theorem 1 (Refinement preserves deadend-freedom)**.** *Let $C = (\mathcal{Q}, \mathcal{A}, \rightarrow, \sigma, s_0)$ and $C' = (\mathcal{Q}', \mathcal{A}, \rightarrow', \sigma', s_0')$ be two contracts such that $C' \leq C$, and C' is delimited and consistent. If C is deadend-free then so is C'.*

Proof. Since C' is delimited, every reachable probabilistic state has an outgoing transition with a non-empty probability interval. For each action state in $q \in \mathcal{Q}^a$ that has a transition $q \xrightarrow{a} q_1$ with $q_1 \neq \top$, all action states $q' \in \mathcal{Q}'$ refining q have an outgoing transition $q' \xrightarrow{a}{}' q_2$ with $q_2 \neq \top$. On the other hand, all reachable action states in $\mathcal{Q}'$ must refine some reachable action state in $\mathcal{Q}$. The claim follows. □

3.3 Contract Projection

The need of projection arises naturally in contract frameworks. $\mathcal{A}$ and $\mathcal{B}$ being two alphabets of actions such that $\mathcal{B} \subseteq \mathcal{A}$, we abstract from actions in $\mathcal{A} \setminus \mathcal{B}$ that are not relevant by renaming them into internal τ actions. The contract over the alphabet $\mathcal{B} \cup \{\tau\}$ is then projected on the sub-alphabet $\mathcal{B}$ by using the standard determinization algorithm (see e.g. [1]).

Definition 12 (Projection)**.** *Let $C = (\mathcal{Q}, \mathcal{A}, \rightarrow_1, \sigma, s_0)$ be a contract and $\mathcal{B} \subseteq \mathcal{A}$ such that for any $q \in \mathcal{Q}^a$ and $\alpha \in \mathcal{A}$, if $q \xrightarrow{\alpha}_1 \top$ or $q \xrightarrow{\alpha}_1 \bot$ then $\alpha \in \mathcal{B}$. Let $C' = (\mathcal{Q}, \mathcal{B} \cup \{\tau\}, \rightarrow_2, \sigma, s_0)$ be the contract where all transition labels in $\mathcal{A} \setminus \mathcal{B}$ are replaced with a new label τ. We require that C is such that $act \cap prob = \emptyset$ where*

$$act = \big\{q \in \mathcal{Q} \mid \exists q' \in \mathcal{Q} : q \xrightarrow{\tau^*}_2 q' \wedge \big((\exists \alpha \in \mathcal{B}\ \exists q'' \in \mathcal{Q} : q' \xrightarrow{a}_2 q'') \vee (\forall q'' : q' \xrightarrow{\tau^*}_2 q'' \implies q'' \in \mathcal{Q}^a)\big)\big\}$$

$$prob = \{q \in \mathcal{Q} \mid \exists q' \in \mathcal{Q}^p : q \xrightarrow{\tau^*}_2 q'\}$$

and $\xrightarrow{\tau^*}_2$ is the transitive and reflexive closure of $\xrightarrow{\tau}_2$.

The projection of C on $\mathcal{B}$ (written $\pi_{\mathcal{B}}(C)$) is obtained by τ-elimination (determinization) of C'.

The requirement that action transitions immediately leading to $\top$ or $\bot$ be kept in the projection ensures that Hypothesis 1 is preserved. The second requirement ensures that the states of $\pi_{\mathcal{B}}(C)$ are partitioned into action states, probabilistic states, $\{\top\}$, and $\{\bot\}$. More precisely, *act* is the set of states q from which a state q' is reachable by taking only τ transitions, such that either a transition with an action label in $\mathcal{B}$ is enabled in q', or no more probabilistic state is reachable. Conversely, *prob* is the set of states from where a probabilistic state can be reached. Disjointness of both sets ensures that every state of $\pi_{\mathcal{B}}(C)$ is uniquely typed, such that $\pi_{\mathcal{B}}(C)$ is a contract again.

Lemma 4 (Projection and refinement)**.** *For all contracts $C_1 = (\mathcal{Q}_1, \mathcal{A}, \rightarrow_1, \dashrightarrow_1, s_0)$ and $C_2 = (\mathcal{Q}_2, \mathcal{A}, \rightarrow_2, \dashrightarrow_2, t_0)$ and for all $\mathcal{B} \subseteq \mathcal{A}$ such that $\pi_{\mathcal{B}}(C_1)$ and $\pi_{\mathcal{B}}(C_2)$ are defined, if $C_1 \leq C_2$ then $\pi_{\mathcal{B}}(C_1) \leq \pi_{\mathcal{B}}(C_2)$.*

Proof. See appendix A.2. □

Example 6. *In Figure 2, if we do not care how the implementation handles failure cases, we can check that $\pi_{\mathcal{A}_s \setminus \{handle\}}(M_s) \models C_s$, where $\mathcal{A}_s$ is the action alphabet of C_s.*

4 Contract Composition

We introduce two composition operations for contracts: parallel composition $||$ parametrized with an interaction set $\mathcal{I}$, and conjunction $\wedge$ (also called shared refinement).

4.1 Parallel Composition of Contracts

Parallel composition allows the designer to build complex models from simpler components in a stepwise and hierarchical manner. In order to reason about the composition of components at the contract level, we define the parallel composition of contracts. As in the BIP component framework [8], parallel composition is parametrized with a set of interactions, where each interaction is a set of component actions occurring simultaneously. For instance, an interaction set $\big\{\{a\}, \{a, b\}, \{c\}\big\}$ says that action a can interleave or synchronize with b; action b must synchronize with a; action c is a singleton interaction that always interleaves. Whenever there is no ambiguity we simply write a (resp. $a|b$) for the singleton interaction $\{a\}$ (resp. for the interaction $\{a, b\}$), therefore the symbol "|" is commutative.

Definition 13 (Parallel composition of contracts)**.** *Let $C_1 = (\mathcal{Q}_1, \mathcal{A}_1, \rightarrow_1, \dashrightarrow_1, s_0)$ and $C_2 = (\mathcal{Q}_2, \mathcal{A}_2, \rightarrow_2, \dashrightarrow_2, t_0)$ be two contracts. The parallel composition of C_1 and C_2 with respect to an interaction set $\mathcal{I} \subseteq 2^{\mathcal{A}_1 \cup \mathcal{A}_2}$ (written $C_1 || _{\mathcal{I}} C_2$) is the contract $\big(\mathcal{Q}, \mathcal{I}, \rightarrow', \dashrightarrow, (s_0, t_0)\big)$ where:*

1. *$\mathcal{Q} = (\mathcal{Q}'_1 \times \mathcal{Q}'_2) \cup \{\top, \bot\}$ with $Q'_1 = Q_1 \setminus \{\top_1, \bot_1\}$, $Q'_2 = Q_2 \setminus \{\top_2, \bot_2\}$, $\mathcal{Q}^a = \mathcal{Q}^a_1 \times \mathcal{Q}^a_2$, and $\mathcal{Q}^p = \mathcal{Q} \setminus (\mathcal{Q}^a \cup \{\top, \bot\})$;*

2.

$$\begin{aligned}\rightarrow' = \{(q,a,q') \in \rightarrow \mid q' \notin \mathcal{Q}^\top \cup \mathcal{Q}^\bot\} \cup \\ \{(q,a,\top) \mid \exists q' \in \mathcal{Q}^\top : (q,a,q') \in \rightarrow\} \cup \\ \{(q,a,\bot) \mid \exists q' \in \mathcal{Q}^\bot : (q,a,q') \in \rightarrow\}\end{aligned}$$

where $\rightarrow$ is the least relation satisfying the rules [R1]–[R3] *in Figure 9; and*

3. $\dashrightarrow$ is the least relation satisfying the rules [R4]–[R6] *in Figure 9*

where $\mathcal{Q}^\top = (\mathcal{Q}_1 \times \{\top_2\}) \cup (\{\top_1\} \times \mathcal{Q}_2)$ *and* $\mathcal{Q}^\bot = (\mathcal{Q}_1 \times \{\bot_2\}) \cup (\{\bot_1\} \times \mathcal{Q}_2)$.

In other words, $\top$ (resp. $\bot$) is reached in $C_1||_\mathcal{I} C_2$ as soon as one of C_1 or C_2 reaches its $\top_i$ (resp. $\bot_i$) state.

$$\frac{q_1 \xrightarrow{\alpha}_1 q_1' \quad \alpha \in \mathcal{I} \quad q_2 \in \mathcal{Q}_2^a}{(q_1,q_2) \xrightarrow{\alpha} (q_1',q_2)}\ [R1] \qquad \frac{q_2 \xrightarrow{\alpha}_2 q_2' \quad \alpha \in \mathcal{I} \quad q_1 \in \mathcal{Q}_1^a}{(q_1,q_2) \xrightarrow{\alpha} (q_1,q_2')}\ [R2]$$

$$\frac{q_1 \xrightarrow{\alpha}_1 q_1' \quad q_2 \xrightarrow{\beta}_2 q_2' \quad \alpha|\beta \in \mathcal{I}}{(q_1,q_2) \xrightarrow{\alpha|\beta} (q_1',q_2')}\ [R3] \qquad \frac{q_1 \overset{[p_1,p_2]}{\dashrightarrow}_1 q_1' \quad q_2 \overset{[p_3,p_4]}{\dashrightarrow}_2 q_2'}{(q_1,q_2) \overset{[p_1*p_3,p_2*p_4]}{\dashrightarrow} (q_1',q_2')}\ [R4]$$

$$\frac{q_1 \overset{P}{\dashrightarrow}_1 q_1' \quad q_2 \in \mathcal{Q}_2^a}{(q_1,q_2) \overset{P}{\dashrightarrow} (q_1',q_2)}\ [R5] \qquad \frac{q_2 \overset{P}{\dashrightarrow}_2 q_2' \quad q_1 \in \mathcal{Q}_1^a}{(q_1,q_2) \overset{P}{\dashrightarrow} (q_1,q_2')}\ [R6]$$

Figure 9: Rules for the parallel composition of contracts.

Rules [R1] to [R3] are the usual parallel composition rules for LTS, while Rule [R4] is similar to the typical parallel composition for Markov chains but on probability intervals. Finally, Rules [R5] and [R6] state that probabilistic transitions, usually modeling hidden internal behavior, have priority over action transitions. Parallel composition is commutative since the rules are symmetrically defined.

Example 7. *Figure 10 illustrates the parallel composition of contracts C_s (from Figure 2(b)) and $C_\ell = \lfloor M_\ell \rfloor$ (where M_ℓ is given in Figure 1(b)), with $\mathcal{I} = \{rec, del, req'|del', res'|rec', fail_1, fail_2\}$. The composed contract $C_s \,||_\mathcal{I}\, C_\ell$ states that a failure in the Link component does not prevent it from continuing to deliver the request req' to the Server, and receiving the response res' from the Server, but the failure prevents it from delivering the response res' back to the Client.*

We end the section on parallel composition with several useful theorems.

Theorem 2 (Congruence of refinement for $||_\mathcal{I}$)**.** *For all contracts C_1, C_2, C_3, C_4 and an interaction set $\mathcal{I}$, if $C_1 \leq C_2$ and $C_3 \leq C_4$, then $C_1||_\mathcal{I}\, C_3 \;\leq\; C_2||_\mathcal{I}\, C_4$.*

Proof. See appendix B.1. □

Theorem 3 (Independent implementability)**.** *For all IMCs M, N, contracts C_1, C_2, and interaction set $\mathcal{I}$, if $M \models C_1$ and $N \models C_2$, then $M||_\mathcal{I} N \;\models\; C_1||_\mathcal{I} C_2$.*

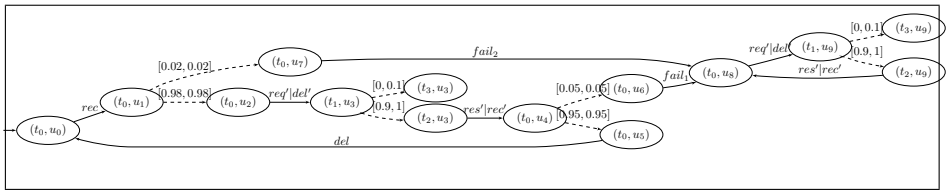


Figure 10: Parallel composition of C_s and C_ℓ.

Proof.

$$
\begin{array}{ll}
 & M \models C_1 \text{ and } N \models C_2 \\
\iff & \text{(By definition of } \models\text{)} \\
 & \lfloor M \rfloor \leq C_1 \text{ and } \lfloor N \rfloor \leq C_2 \\
\Rightarrow & \text{(By Theorem 2 (Congruence of refinement for } ||_\mathcal{I}\text{))} \\
 & \lfloor M \rfloor ||_\mathcal{I} \lfloor N \rfloor \leq C_1 ||_\mathcal{I} C_2 \\
\iff & \text{(By definition of } \lfloor . \rfloor \text{ (Figure 3))} \\
 & \lfloor M ||_\mathcal{I} N \rfloor \leq C_1 ||_\mathcal{I} C_2 \\
\iff & \text{(By Definition 6 } (\models)\text{)} \\
 & M ||_\mathcal{I} N \models C_1 ||_\mathcal{I} C_2
\end{array}
$$

□

Theorem 4 (Reduction and parallel composition)**.** *For all contracts* C_1 *and* C_2, $\overline{C_1} \,||_\mathcal{I}\, \overline{C_2} \equiv C_1 \,||_\mathcal{I}\, C_2$.

Proof.

$$
\begin{array}{ll}
 & \text{(By Lemma 3 (Bisimilarity of reduction))} \\
 & \overline{C_1} \leq C_1 \text{ and } \overline{C_2} \leq C_2 \text{ and } C_1 \leq \overline{C_1} \text{ and } C_2 \leq \overline{C_2} \\
\Rightarrow & \text{(By Theorem 2 (Congruence of refinement for } ||_\mathcal{I}\text{))} \\
 & \overline{C_1} ||_\mathcal{I} \overline{C_2} \leq C_1 ||_\mathcal{I} C_2 \text{ and } C_1 ||_\mathcal{I} C_2 \leq \overline{C_1} ||_\mathcal{I} \overline{C_2} \\
\Rightarrow & \text{(By Corollary 1)} \\
 & \overline{C_1} ||_\mathcal{I} \overline{C_2} \equiv C_1 ||_\mathcal{I} C_2
\end{array}
$$

□

4.2 Conjunction of contracts

A single component may have to satisfy several contracts that are specified independently, each of them specifying different requirements on the component, such as safety, reliability, or quality of service. Therefore, the contracts may use different, possibly overlapping, sub-alphabets of the component. The *conjunction* of contracts computes a common refinement of all contracts. Prior to conjunction, we define *similarity* of contracts as a test whether a common refinement exists.

Definition 14 (Similarity ($\sim$))**.** *Let* $C_1 = (\mathcal{Q}_1, \mathcal{A}_1, \rightarrow_1, \dashrightarrow_1, s_0)$ *and* $C_2 = (\mathcal{Q}_2, \mathcal{A}_2, \rightarrow_2, \dashrightarrow_2, t_0)$ *be two contracts.* $\sim \subseteq (\mathcal{Q}_1 \setminus \{\bot\}) \times (\mathcal{Q}_2 \setminus \{\bot\})$ *is the largest relation such that* $\forall (s,t) \in (\mathcal{Q}_1 \setminus \{\bot\}) \times (\mathcal{Q}_2 \setminus \{\bot\})$, $s \sim t$ *iff* $(s = \top \vee t = \top)$ *or conditions (1) to (4) below hold:*

1. *If* $(s,t) \in \mathcal{Q}_1^a \times \mathcal{Q}_2^a$ *then*

(a) *for all* $s' \in \mathcal{Q}_1$, *if* $s \xrightarrow{\alpha}_1 s'$, *then either*
   i. $\alpha \notin \mathcal{A}_2$, *or*
   ii. $\alpha \in \mathcal{A}_2$ *and* $\exists m \geq 0,\ \exists \beta_1, ..., \beta_m \in \mathcal{A}_2 \setminus \mathcal{A}_1,\ \exists t_1, ..., t_m, t' \in \mathcal{Q}_2$: $t \xrightarrow{\beta_1}_2 t_1 \xrightarrow{\beta_2}_2 \ldots \xrightarrow{\beta_m}_2 t_m \xrightarrow{\alpha}_2 t' \wedge \forall i = 1, ..., m$: $s \sim t_i$;

(b) *for all* $t' \in \mathcal{Q}_2$, *if* $t \xrightarrow{\alpha}_2 t'$, *then either*
   i. $\alpha \notin \mathcal{A}_1$, *or*
   ii. $\alpha \in \mathcal{A}_1$ *and* $\exists m \geq 0,\ \exists \beta_1, ..., \beta_m \in \mathcal{A}_1 \setminus \mathcal{A}_2,\ \exists s_1, ..., s_m, s' \in \mathcal{Q}_1$: $s \xrightarrow{\beta_1}_1 s_1 \xrightarrow{\beta_2}_1 \ldots \xrightarrow{\beta_m}_1 s_m \xrightarrow{\alpha}_1 s' \wedge \forall i = 1, ..., m$: $s_i \sim t$;

2. *If* $(s, t) \in \mathcal{Q}_1^p \times \mathcal{Q}_2^p$ *then*

   (a) *for all* $s' \in \mathcal{Q}_1$, *if* $s \overset{P_1}{\dashrightarrow} s'$, *then* $t \overset{P_2}{\dashrightarrow} t'$ *for some* $t' \in \mathcal{Q}_2$ *with* $P_1 \cap P_2 \neq \emptyset$ *and* $s' \sim t'$; *and*

   (b) *for all* $t' \in \mathcal{Q}_2$, *if* $t \overset{P_2}{\dashrightarrow} t'$, *then* $s \overset{P_1}{\dashrightarrow} s'$ *for some* $s' \in \mathcal{Q}_1$ *with* $P_1 \cap P_2 \neq \emptyset$ *and* $s' \sim t'$;

3. *If* $(s, t) \in \mathcal{Q}_1^a \times \mathcal{Q}_2^p$ *then for all* $t' \in \mathcal{Q}_2$ *with* $t \overset{P}{\dashrightarrow}_2 t'$, $s \sim t'$;

4. *If* $(s, t) \in \mathcal{Q}_1^p \times \mathcal{Q}_2^a$ *then for all* $s' \in \mathcal{Q}_1$ *with* $s \overset{P}{\dashrightarrow}_1 s'$, $s' \sim t$.

Finally, C_1 *and* C_2 *are similar, written* $C_1 \sim C_2$, *iff* $s_0 \sim t_0$.

Each P_i in Definition 14 refers to a probabilistic interval in the form of $[\ell_i, u_i]$. Any state is similar to a top state $\top_i$ (where the contract does not constrain the implementation in any way). The bottom states $\bot_i$ are not similar to any state. Two action states are similar if they agree on the enabled actions in the shared alphabet $\mathcal{A}_1 \cap \mathcal{A}_2$. The successor states are not required to be similar again, as they may be made unreachable in a subsequent parallel composition. Two probabilistic states are similar if the probabilistic transitions can be matched such that the intervals overlap ($P_1 \cap P_2 = \emptyset$) and the successor states are similar. Overall, two states are similar if they agree on the behavior up to and including the next reachable action transition in the shared alphabet.

Definition 15 (Unambiguous contract)**.** *A contract* $C = (\mathcal{Q}, \mathcal{A}, \rightarrow, \dashrightarrow, s_0)$ *is unambiguous w.r.t* $\mathcal{B} \subseteq \mathcal{A}$ *iff for all* r, s, *and* $t \in \mathcal{Q}$ *such that:*

$$\left(r \overset{>0}{\dashrightarrow} s \ \wedge\ r \overset{>0}{\dashrightarrow} t\right) \ \vee\ \left(\exists \alpha, \beta \in (\mathcal{A} \setminus \mathcal{B}) \cup \{\emptyset\} : r \xrightarrow{\alpha} s \ \wedge\ r \xrightarrow{\beta} t\right)$$

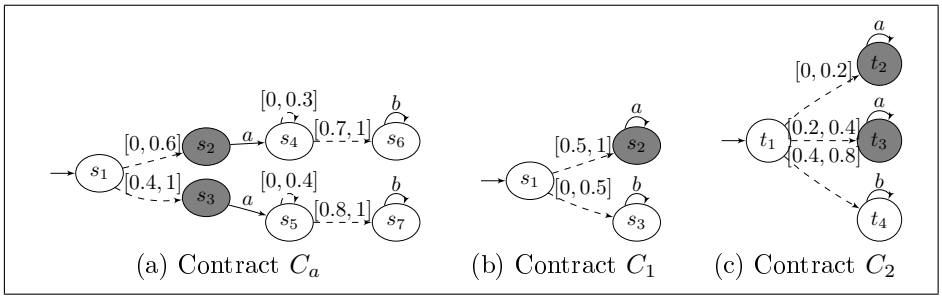
we have: if $s \sim t$ *then* $s = t$, *where* $q \xrightarrow{\emptyset} q$ *for all* $q \in \mathcal{Q}$, .

C *is* unambiguous *if it is unambiguous w.r.t* $\mathcal{A}$.

In other words, a contract is *unambiguous* if the reachable successor states of any probabilistic state are pairwise non-similar.

Example 8. *In Figure 11(a), the contract* C_a *is ambiguous because* $s_2 \sim s_3$ *(highlighted in gray) but* $s_2 \neq s_3$.

We are now ready to define the conjunction of two contracts. The two contracts may refer to different, not necessarily disjoint alphabets. Therefore, the contracts can be used to specify requirements on two (not necessarily disjoint) aspects of a component.



(a) Contract C_a (b) Contract C_1 (c) Contract C_2

Figure 11: (a) An ambiguous contract C_a; (b,c) Two non-similar contracts C_1 and C_2.

Definition 16 (Conjunction of contracts ($\wedge$))**.** *Let* $C_1 = (\mathcal{Q}_1, \mathcal{A}_1, \rightarrow_1, \dashrightarrow_1, s_0)$ *and* $C_2 = (\mathcal{Q}_2, \mathcal{A}_2, \rightarrow_2, \dashrightarrow_2, t_0)$ *be two contracts such that* C_1 *and* C_2 *are unambiguous w.r.t* $\mathcal{A}_1 \cap \mathcal{A}_2$*. The conjunction of* C_1 *and* C_2 *is the contract* $C_1 \wedge C_2 = \big(\mathcal{Q}, \mathcal{A}_1 \cup \mathcal{A}_2, \rightarrow', \dashrightarrow, (s_0, t_0)\big)$ *where:*

1. $\mathcal{Q} = \{(q_1, q_2) \in \mathcal{Q}_1 \times \mathcal{Q}_2 \mid q_1 \sim q_2 \wedge (q_1 \neq \top_1 \vee q_2 \neq \top_2)\} \cup \{\top, \bot\}$, $\mathcal{Q}^p = \mathcal{Q} \cap \big((\mathcal{Q}_1^p \times \mathcal{Q}_2) \cup (\mathcal{Q}_1 \times \mathcal{Q}_2^p)\big)$, *and* $\mathcal{Q}^a = \mathcal{Q} \setminus (\mathcal{Q}^p \cup \{\top, \bot\})$*;*

2. $$\begin{aligned}\rightarrow' = \{(q, a, q') \in \rightarrow \mid q' \in \mathcal{Q}\} \cup \\ \{(q, a, \top) \mid \big(q, a, (\top_1, \top_2)\big) \in \rightarrow\} \cup \\ \{(q, a, \bot) \mid \exists q' = (q_1', q_2') \in \mathcal{Q}_1 \times \mathcal{Q}_2 : \neg(q_1' \sim q_2') \wedge (q, a, q') \in \rightarrow\}\end{aligned}$$

   where $\rightarrow$ *is the least relation satisfying the rules* [C1] – [LiftR] *in Figure 12, and*

3. $\dashrightarrow$ *is the least relation satisfying the rules* [C3] – [C4R] *in Figure 12 (where for all other probabilistic transitions* $(q_1, q_2) \overset{P}{\dashrightarrow} (q_1', q_2')$*,* $P = [0, 0]$*).*

The $\bot$ state is entered in the contract $C_1 \wedge C_2$ as soon as a pair of non-similar states (including, by definition, pairs with at least one $\bot$ state) is reached.

Rule [C1] requires the contracts to agree on action transitions over their common alphabet. According to rule [C2L] (resp. [C2R]), the conjunction behaves like the first (resp. second) contract as soon as the other contract is in $\top$. Rules [LiftL] and [LiftR] allow the interleaving of action transitions that are not in the common alphabet. Rules [C3] – [C4R] define probabilistic transitions whose successor states are similar.

Example 9. *Figure 13 shows three contracts for the Link component:* $C_{\ell 1}$ *specifies that the implementation should receive a request (rec) from the Client and deliver it to the Server (del′);* $C_{\ell 2}$ *specifies that the implementation should receive a response (rec′) from the Server and deliver it to the Client (del);* $C_{\ell 3}$ *requires the response (rec′) received from the Server to occur after the request (del′) delivered to the Server. We can verify that* $M_\ell \models (C_{\ell 1} \wedge C_{\ell 3}) \wedge (C_{\ell 2} \wedge C_{\ell 3})$ *(where* M_ℓ *is in Figure 1(b)).*

$$\frac{q_1 \xrightarrow{\alpha}_1 q_1' \quad q_2 \xrightarrow{\alpha}_2 q_2'}{(q_1,q_2) \xrightarrow{\alpha} (q_1',q_2')} \quad [\text{C1}]$$

$$\frac{q_1 \xrightarrow{\alpha}_1 q_1'}{(q_1,\top_2) \xrightarrow{\alpha} (q_1',\top_2)} \quad [\text{C2L}] \qquad \frac{q_2 \xrightarrow{\alpha}_2 q_2'}{(\top_1,q_2) \xrightarrow{\alpha} (\top_1,q_2')} \quad [\text{C2R}]$$

$$\frac{q_1 \xrightarrow{\alpha}_1 q_1' \quad q_2 \in \mathcal{Q}_2^a \quad \alpha \notin \mathcal{A}_2}{(q_1,q_2) \xrightarrow{\alpha} (q_1',q_2)} \quad [\text{LiftL}]$$

$$\frac{q_2 \xrightarrow{\alpha}_2 q_2' \quad q_1 \in \mathcal{Q}_1^a \quad \alpha \notin \mathcal{A}_1}{(q_1,q_2) \xrightarrow{\alpha} (q_1,q_2')} \quad [\text{LiftR}]$$

$$\frac{q_1 \overset{P_1}{\dashrightarrow}_1 q_1' \quad q_2 \overset{P_2}{\dashrightarrow}_2 q_2' \quad q_1' \sim q_2'}{(q_1,q_2) \overset{P_1 \cap P_2}{\dashrightarrow} (q_1',q_2')} \quad [\text{C3}]$$

$$\frac{q_1 \overset{P}{\dashrightarrow}_1 q_1' \quad q_2 \in \mathcal{Q}_2^a \cup \{\top_2\} \quad q_1' \sim q_2}{(q_1,q_2) \overset{P}{\dashrightarrow} (q_1',q_2)} \quad [\text{C4L}]$$

$$\frac{q_2 \overset{P}{\dashrightarrow}_2 q_2' \quad q_1 \in \mathcal{Q}_1^a \cup \{\top_1\} \quad q_1 \sim q_2'}{(q_1,q_2) \overset{P}{\dashrightarrow} (q_1,q_2')} \quad [\text{C4R}]$$

Figure 12: Rules for conjunction of contracts.

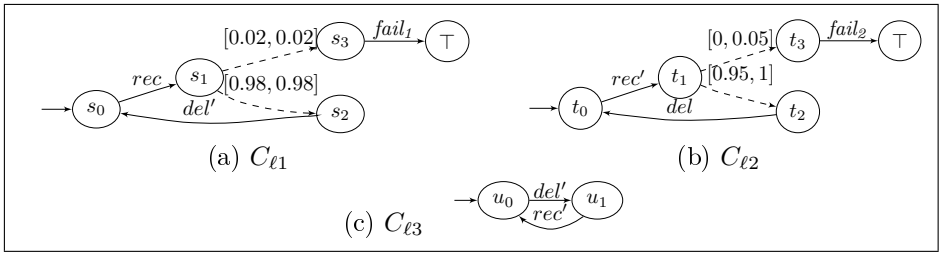


Figure 13: Example: Conjunction of Contracts

Example 10. *Since a contract that is not in reduced form may be ambiguous, contracts should be reduced before performing conjunction. In Figure 11(c), contract C_2 is ambiguous, but $t_2 \simeq t_3$. If we reduce C_2 by applying Definition 10, we get $t_1 \overset{[0.2,0.6]}{\dashrightarrow} \{t_2,t_3\} \xrightarrow{a} \{t_2,t_3\}$. The reduced contract is unambiguous and $s_1 \sim t_1$, hence conjunction yields a common refinement of C_1 and C_2.*

Theorem 5 (Associativity of conjunction over the same alphabet)**.** *For all unambiguous contracts $C_1 = (\mathcal{Q}_1, \mathcal{A}, \rightarrow_1, \sigma_1, s_0)$, $C_2 = (\mathcal{Q}_2, \mathcal{A}, \rightarrow_2, \sigma_2, t_0)$, and $C_3 = (\mathcal{Q}_3, \mathcal{A}, \rightarrow_3, \sigma_3, u_0)$, $(C_1 \wedge C_2) \wedge C_3 = C_1 \wedge (C_2 \wedge C_3)$.*

Proof. See appendix B.5. □

Theorem 6 (Soundness of conjunction)**.** *For all unambiguous contracts C_1 and C_2, if $\pi_{\mathcal{A}_i}(C_1 \wedge C_2)$ is defined then $\pi_{\mathcal{A}_i}(C_1 \wedge C_2) \leq C_i$ for $i = 1, 2$.*

Proof. See appendix B.2. □

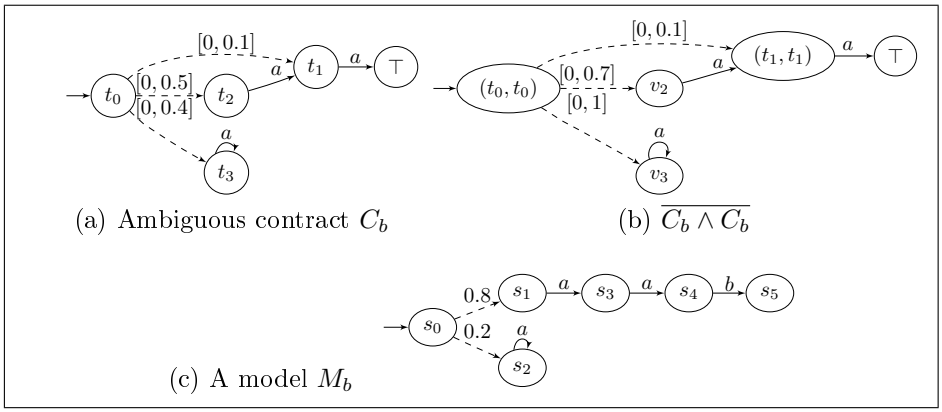


Figure 14: Example where $M_b \models C_b \wedge C_b$ but $M_b \not\models C_b$.

Example 11. *Figure 14 motivates the requirement of conjunction (Definition 16) for* unambiguous *contracts. The resulting contract $C_b \wedge C_b$ is reduced such that the model relation can be seen easily. In Figure 14(b), v_2 denotes the equivalent class $\{(t_1, t_2), (t_2, t_1), (t_2, t_2)\}$ while v_3 denotes the equivalent class $\{(t_1, t_3), (t_2, t_3), (t_3, t_1), (t_3, t_2), (t_3, t_3)\}$. Since $t_1 \sim t_2 \sim t_3$, duplicated intervals lead to an unsound result.*

Theorem 7 (Completeness of conjunction over the same alphabet)**.** *For all delimited unambiguous contracts C_1, C_2, C_3, if $C_1 \leq C_2$ and $C_1 \leq C_3$, then $C_1 \leq C_2 \wedge C_3$.*

Proof. See appendix B.4. □

Theorem 8 (Congruence of refinement for $\wedge$ over the same alphabet)**.** *For all delimited unambiguous contracts C_1, C_2, C_3, and C_4 over the same alphabet, if $C_1 \leq C_2$ and $C_3 \leq C_4$, then $C_1 \wedge C_3 \leq C_2 \wedge C_4$.*

Proof. See appendix B.4. □

5 Case Study

We study a dependable computing system with time redundancy. The system specification is expressed by the contract C_S of Figure 15 (top left), which specifies that the computation *comp* should have a success probability of at least 0.999. If the computation fails, then nothing is specified (state $\top$). All the contracts in this section are delimited.

The processor P the system is running on is specified by the contract C_P of Figure 15 (top right). Following an execution request *exe*, either the processor succeeds and replies with *ok* (with a probability at least p), or fails and replies with *nok* (with a probability at most $1 - p$). The failure rates for successive executions are independent. The probability p is a *parameter* of the contract.

We place ourselves in a setting where the reliability level guaranteed by C_P alone (as expressed by p) cannot fulfill the requirement of C_S (that is, 0.999), and hence some form of redundancy must be used. We propose to use time redundancy, as expressed by the contract C_R of Figure 15 (bottom). Each

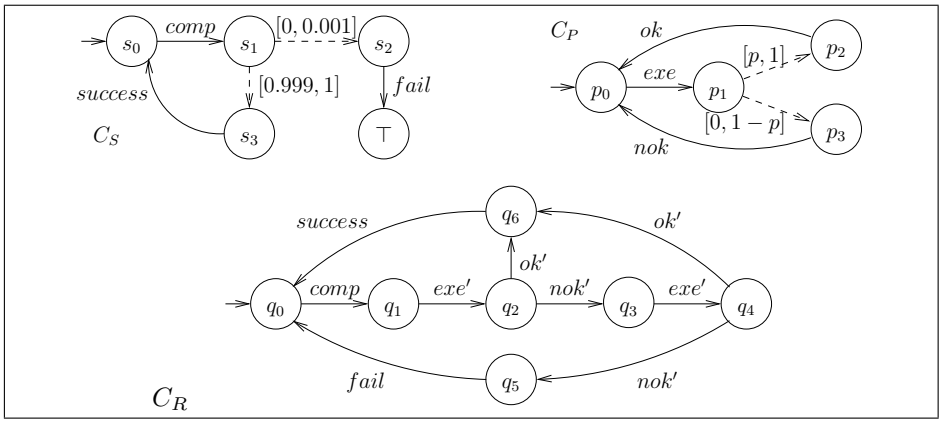


Figure 15: (Top left) Specification C_S; (top right) Processor contract C_P; (bottom) Time redundancy contract C_R.

computation *comp* is first launched on the processor P (exe'), either followed by a positive (ok') or negative (nok') answer from P. In the latter case, the execution is launched a second time, therefore implementing time redundancy. The contract C_R finally answers with *success* if *either* execution is followed by ok', or with $fail$ is *both* executions are followed by nok'.

In terms of component-based design for reliability, we want to determine the minimum value of p that guarantees the reliability level of C_S. To compute this minimum value, we first compute the parallel composition $C_R||_{\mathcal{I}}C_P$, with the interaction set $\mathcal{I} = \{comp, exe|exe', ok|ok', nok|nok', success, fail\}$. The reduction modulo bisimulation of this parallel composition is shown in Figure 16 (top), where the interactions $exe|exe'$, $ok|ok'$, and $nok|nok'$ have been replaced for conciseness by **exe**, **ok**, and **nok**, respectively. We call this new contract $C_{R||P}$. We then compute the projection of $C_{R||P}$ onto the set $\mathcal{B} = \{comp, success, fail\}$. The result $C_\pi = \pi_{\mathcal{B}}(C_{R||P})$ is shown in Figure 16 (bottom left).

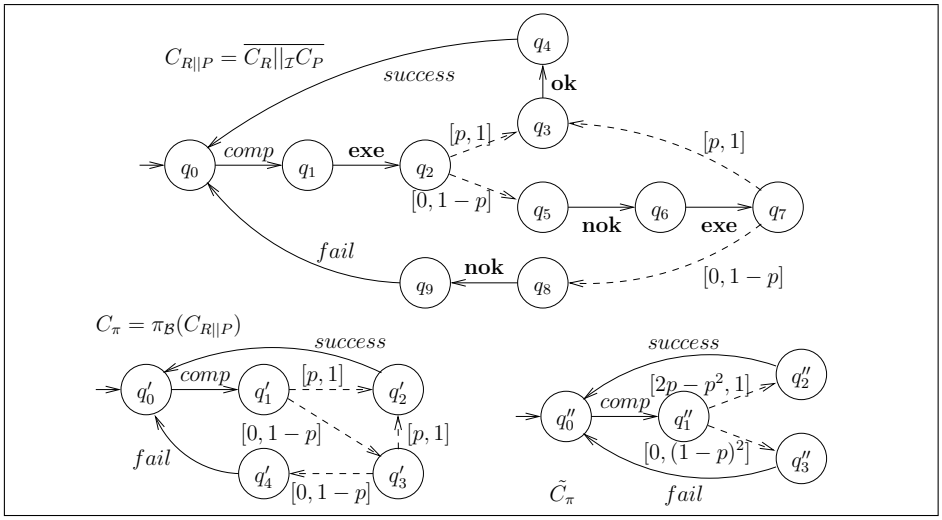


Figure 16: Parallel composition $C_{T||P}$; Projection C_π; Transitive closure $\tilde{C}_\pi$.

We are thus faced with a contract C_π having *sequences* of probabilistic transitions; more precisely, since some probabilistic states have several outgoing transitions, we have DAGs of probabilistic transitions. We therefore compute the transitive closure for each such DAG: that is, for each sequence of probabilistic transitions from the initial state of the DAG (e.g., q'_1 in C_π) to one of its final states (e.g., q'_2 and q'_4 in C_π), we compute the equivalent probabilistic transition. Starting from q'_1, the probability interval of reaching q'_2 (resp. q'_4) is given by $\{p' + (1-p')p' \mid p' \in [p,1]\}$ (resp. $\{(1-p')^2 \mid p' \in [p,1]\}$), that is, $[2p-p^2, 1]$ (resp. $[0,(1-p)^2]$). The resulting contract $\tilde{C}_\pi$ is shown in Figure 16 (bottom right).

The last step involves checking under which condition on p the contract $\tilde{C}_\pi$ refines the specification C_S. We have $\tilde{C}_\pi \leq C_S \Leftrightarrow (1-p)^2 \leq 0.001 \Leftrightarrow p \geq 0.968$. This means that, with time redundancy and a processor with a reliability level of at least 0.969, we are able to ensure an overall reliability level of 0.999.

To demonstrate the versatility of our contract framework, we show in Figure 17 the alternative contract C'_R for *spatial* redundancy. This time, the execution is launched both on processor 1 (exe_1) and on processor 2 (exe_2). We call C_{P1} the contract of processor 1, which is identical to C_P in Figure 15 (top right). We call C_{P2} the contract of processor 2, which is identical to C_{P1} upto a renaming of the index. The contract C'_R answers with *success* if *either* ok_1 or ok_2 is received, or with $fail$ is *both* nok_1 and nok_2 are received, in any order.

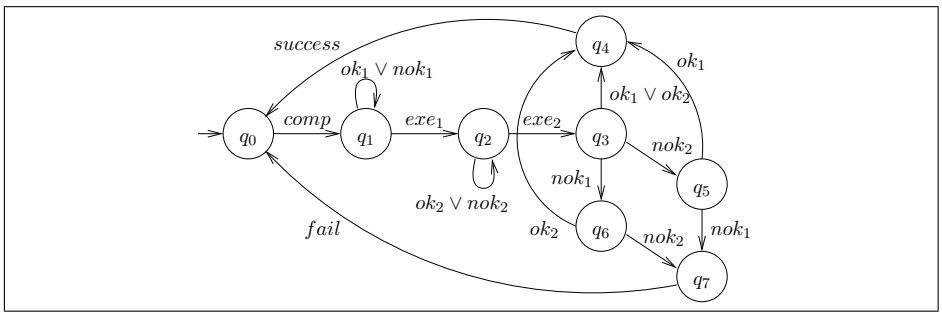


Figure 17: Spatial redundancy: the contract C'_R.

We leave the intermediate computations as exercises for the reader. These are:

- $C_A = C_{P1} ||_{\mathcal{I}} C_{P2}$ with $\mathcal{I} = \{exe'_1, ok'_1, nok'_1, exe'_2, ok'_2, nok'_2\}$.
- $C_B = C_A ||_{\mathcal{I}'} C'_R$ with $\mathcal{I}' = \{comp, success, fail, exe_1|exe'_1, ok_1|ok'_1, nok_1|nok'_1, exe_2|exe'_2, ok_2|ok'_2, nok_2|nok'_2\}$.

We then compute the projection $\pi_{\mathcal{B}}(\overline{C_B})$ onto the set $\mathcal{B} = \{comp, success, fail\}$. The reduction modulo bisimulation of the result, called C'_π, is shown in Figure 18 (left). Like with the time redundancy contract, we compute the transitive closure for each DAG of probabilistic transitions. The result $\tilde{C}'_\pi$ is shown in Figure 18 (right).

The last step involves checking under which condition on p_1 and p_2 the contract $\tilde{C}'_\pi$ refines the specification C_S. We have $\tilde{C}'_\pi \leq C_S \Leftrightarrow (1-p_1)(1-p_2) \leq 0.001$. This condition is to be compared with the $(1-p)^2 \leq 0.001$ condition obtained with time redundancy.

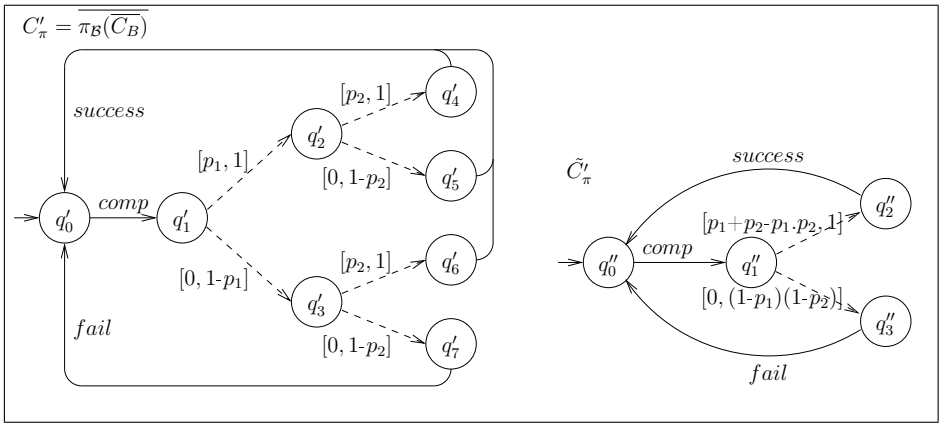


Figure 18: Projection $C'_\pi = \overline{\pi_{\mathcal{B}}(\overline{C_B})}$ onto the set $\mathcal{B} = \{comp, success, fail\}$; Transitive closure $\tilde{C}'_\pi$.

6 Discussion

We have introduced a design framework based on probabilistic contracts and proved essential properties for its use in component-based design. Our definition of contracts adapts ideas from [10, 17, 6], although the frameworks in [10, 6] do not support interactions between contracts. This article extends the preliminary work of [16] with several new results. In particular, the definition of similarity has been weakened, so as to provide a less pessimistic definition of conjunction. This enables us to provide a new result on completeness of conjunction if both arguments share the same alphabet (Theorem 7).

6.1 Design choices

A fundamental syntactic choice in defining a symbolic contract framework is to define a contract either as a pair (assumption, guarantee) as in [7] — call them *assume/guarantee contracts* — or as a single *implicit* transition system where the distinction of assumption and guarantee is made by means of a specific $\top$ state, as in the present article. Whereas assume/guarantee contracts have the benefit of making explicit the assumptions of how a component is used and the guarantees provided by the component in this case, they come at the price of introducing some redundancy whenever the assumptions and the guarantees refer to the same sub-alphabet of the component. From a more technical point of view, another downside of assume/guarantee contracts is that parallel composition and conjunction of symbolic representations usually require the computation of an equivalent implicit form of the contract, whose definition is far from being obvious for probabilistic contracts.

A further choice is where to represent the probabilistic behavior: in the model of a component (i.e., the implementation), in the contract (i.e., the specification), or both. We have chosen the last option, as it allows us to model both the *expected* probabilistic behavior and the behavior *offered* by existing components, and reason about how the specification can be realized.

Moreover, probability distributions can be *local* to contract states or *global*. In this work we have adopted the first option, as state-dependent distributions

occur naturally in models of physical behavior: e.g., the failure rate of a microprocessor increases as the processor ages. The price of distinguishing local distributions are more involved definitions of refinement and conjunction.

A final parameter of the contract framework is the definition of parallel composition. We have chosen to support the BIP interaction model [8] for its expressiveness. In this framework, the direction of communications is not represented; it would be quite straight-forward, however, to add this information by typing ports as input or output ports.

6.2 Related work

Several authors have proposed probabilistic extensions of Hoare triples and Dijkstra's *wp*-calculus, see e.g. [14]. A trace-based theory of probabilistic system with compositional semantics and refinement is introduced in [3]. Later on, shared refinement of interfaces and conjunction of modal specifications over possibly different alphabets have been defined in [5, 15]. A framework of modal assume/ guarantee contracts is introduced in [7], for which both parallel composition and conjunction are defined. [11] introduces a compositional framework based on continuous time IMCs, adopting a similar interaction model as done in this paper. [11] supports projection, parallel and symmetric composition, but not conjunction.

A trace-based theory of probabilistic contracts has been introduced in [4], where a contract consists of an assumption A and a guarantee G, both being sets of traces. A trace is a sequence of valuations of global variables, a subset of which is probabilistic. The probabilistic variables are supposed to obey a distribution that is independent of the state. Two types of satisfaction of a contract C by a (non-probabilistic) model S are defined: R-satisfaction (for reliability) is the probability that S satisfies C; A-satisfaction (for availability) measures the expected time ratio during which S satisfies C. Conjunction and refinement are defined for both types of satisfaction. In contrast to our framework, probability distributions are defined globally.

Assume/guarantee verification of probabilistic models is studied in [12]. Probabilistic automata are used to model probabilistic and non-deterministic behavior. Several assume/guarantee rules are introduced using pairs (A, G) of probabilistic safety properties, where a probabilistic safety property is itself a pair of a (non-probabilistic) regular safety property and a probability.

The recently introduced Constraint Markov Chains (CMC) [2] generalize Markov chains by introducing constraints on state valuations and transition probability distributions, aiming at a similar goal of providing a probabilistic component-based design framework. Whereas CMCs do not support explicit interactions among components, they allow the designer to expressively specify constraints on probability distributions. In this framework, conjunction is shown to be sound and complete.

References

[1] A.V. Aho, R. Sethi, and J.D. Ullman. *Compilers – Principles, Techniques, and Tools*. Addison Wesley, 1986.

[2] B. Caillaud, B. Delahaye, K.G. Larsen, A. Legay, M.L. Pedersen, and A. Wasowski. Compositional design methodology with Constraint Markov Chains. In *International Conference on the Quantitative Evaluation of Systems, QEST'10*, pages 123–132, 2010.

[3] L. de Alfaro, T.A. Henzinger, and R. Jhala. Compositional methods for probabilistic systems. In K.G. Larsen and M. Nielsen, editors, *Proc. CONCUR 2001 – Concurrency Theory, 12th International Conference*, volume 2154 of *LNCS*, pages 351–365. Springer, 2001.

[4] B. Delahaye, B. Caillaud, and A. Legay. Probabilistic contracts: a compositional reasoning methodology for the design of systems with stochastic and/or non-deterministic aspects. *Formal Methods in System Design*, 38(1):1–32, 2011.

[5] L. Doyen and T. Petrov T.A. Henzinger, B. Jobstmann. Interface theories with component reuse. In *International conference on Embedded software, EMSOFT'08*, pages 79–88. ACM, 2008.

[6] H. Fecher, M. Leucker, and V. Wolf. Don't know in probabilistic systems. In *International Workshop on Model Checking Software, SPIN'06*, volume 3925 of *LNCS*, pages 71–88. Springer, 2006.

[7] G. Gössler and J.-B. Raclet. Modal contracts for component-based design. In *International Conference on Software Engineering and Formal Methods, SEFM'09*, pages 295–303. IEEE, 2009.

[8] G. Gössler and J. Sifakis. Composition for component-based modeling. *Science of Computer Programming*, 55(1-3):161–183, 3 2005.

[9] H. Hermanns. *Interactive Markov Chains: The Quest for Quantified Quality*, volume 2428 of *LNCS*. Springer, 2002.

[10] B. Jonsson and K.G. Larsen. Specification and refinement of probabilistic processes. In *Symposium on Logic in Computer Science, LICS'91*, pages 266–277. IEEE Computer Society, 1991.

[11] J.-P. Katoen, D. Klink, and M.R. Neuhäußer. Compositional abstraction for stochastic systems. In *International Conference on Formal Modeling and Analysis of Timed Systems, FORMATS'09*, volume 5813 of *LNCS*, pages 195–211. Springer, 2009.

[12] M.Z. Kwiatkowska, G. Norman, D. Parker, and H. Qu. Assume-guarantee verification for probabilistic systems. In *International Conference on Tools and Algorithms for the Construction and Analysis of Systems, TACAS'10*, volume 6015 of *LNCS*, pages 23–37. Springer, 2010.

[13] B. Meyer. *Advances in Object-Oriented Software Engineering*, chapter Design by Contract, pages 1–50. Prentice Hall, 1991.

[14] C. Morgan, A. McIver, and K. Seidel. Probabilistic predicate transformers. *ACM Trans. Program. Lang. Syst.*, 18(3):325–353, 1996.

[15] J.-B. Raclet, E. Badouel, A. Benveniste, B. Caillaud, and R. Passerone. Why modalities are good for interface theories? In *International Conference on Application of Concurrency to System Design, ACSD'09*, pages 119–127. IEEE, 2009.

[16] D.N. Xu, G. Gössler, and A. Girault. Probabilistic contracts for component-based design. In *International Symposium on Automated Technology for Verification and Analysis, ATVA'10*, volume 6252 of *LNCS*, pages 325–340. Springer, 2010.

[17] W. Yi. Algebraic reasoning for real-time probabilistic processes with uncertain information. In *Third International Symposium on Formal Techniques in Real-Time and Fault-Tolerant Systems, FTRTFT'94*, volume 863 of *LNCS*, pages 680–693. Springer, 1994.

A Contract Refinement

A.1 Transitivity of Refinement

Lemma 2 [Transitivity of $\leq$] For all contracts C_1, C_2, and C_3, if $C_1 \leq C_2$ and $C_2 \leq C_3$, then $C_1 \leq C_3$.

Proof. Let

$$\begin{array}{rcl} C_1 & = & (\mathcal{Q}_1, \mathcal{A}_1, \rightarrow_1, \sigma_1, r_0) \\ C_2 & = & (\mathcal{Q}_2, \mathcal{A}_2, \rightarrow_2, \sigma_2, s_0) \\ C_3 & = & (\mathcal{Q}_3, \mathcal{A}_3, \rightarrow_3, \sigma_3, t_0) \end{array}$$

To show $C_1 \leq C_2$ and $C_2 \leq C_3$ implies $C_1 \leq C_3$, by Definition 5 [Contract Refinement], we must show $r_0 \leq s_0$ and $s_0 \leq t_0$ implies $r_0 \leq t_0$. That is, for all $r \in \mathcal{Q}_1, s \in \mathcal{Q}_2, t \in \mathcal{Q}_3$, we must show that:

$$r \leq s \wedge s \leq t \Rightarrow r \leq t$$

We have the following induction hypothesis: for all r', t' which are next states of r and t respectively,

$$(\exists s' \in \mathcal{Q}_2, r' \leq s' \wedge s' \leq t') \Rightarrow r' \leq t' \qquad [\text{H1}]$$

To show $r \leq t$, we check conditions in Definition 5 one by one as follows.

(1)

$$\begin{array}{rl} & r = \top \\ \Rightarrow & (r \leq s, \text{by Definition 5 (1)}) \\ & s = \top \\ \Rightarrow & (s \leq t, \text{by Definition 5 (1)}) \\ & t = \top \end{array}$$

(2)

$$\begin{array}{rl} & t = \bot \\ \Rightarrow & (s \leq t, \text{by Definition 5 (2)}) \\ & s = \bot \\ \Rightarrow & (r \leq s, \text{by Definition 5 (2)}) \\ & r = \bot \end{array}$$

(3) If $(r, t) \in \mathcal{Q}_1^a \times (\mathcal{Q}_3^{\cup}\{\top\})$, then
(a) for all $t' \neq \top \in \mathcal{Q}_3$,

$$\begin{array}{rl} & t \xrightarrow{\alpha}_3 t' \\ \Rightarrow & (s \leq t, \text{by Definition 5 (3a)}) \\ & \exists s' \in \mathcal{Q}_2, s \xrightarrow{\alpha}_2 s' \text{ and } s' \leq t' \\ \Rightarrow & (t' \neq \top \text{ and } s' \leq t' \text{ implies } s' \neq \top, \text{so by Definition 5 (3a)}) \\ & \exists s' \in \mathcal{Q}_2, \exists r' \in \mathcal{Q}_1, r \xrightarrow{\alpha}_1 r' \text{ and } r' \leq s' \text{ and } s' \leq t' \\ \Rightarrow & (\text{Since } r' \leq s' \text{ and } s' \leq t', \text{by induction hypothesis [H1]}) \\ & \exists r' \in \mathcal{Q}_1, r \xrightarrow{\alpha}_1 r' \text{ and } r' \leq t' \end{array}$$

(b) for all $r \in \mathcal{Q}_1$,

$$\begin{array}{rl} & r \xrightarrow{a}_1 r' \\ \Rightarrow & (\text{By Definition 5 (3b)}) \\ & s = \top \text{ or } \exists s' \in \mathcal{Q}_2, s \xrightarrow{\alpha}_2 s' \text{ and } r' \leq s' \end{array}$$

There are two cases to consider:

- Case $s = \top$.

$$\begin{array}{ll} & s = \top \\ \Rightarrow & \text{(By Definition 5 (1))} \\ & t = \top \end{array}$$

  Since any state refines $\top$, we have $r \leq \top$.

- Case $s \neq \top$.

$$\begin{array}{ll} & \exists s' \in \mathcal{Q}_2, s \xrightarrow{\alpha}_2 s' \text{ and } r' \leq s' \\ \Rightarrow & (s \leq t, \text{by Definition 5 (3b)}) \\ & \exists s' \in \mathcal{Q}_2, (t = \top \text{ or } \exists t' \in \mathcal{Q}_3, t \xrightarrow{\alpha}_3 t' \text{ and } s' \leq t') \text{ and } r' \leq s' \end{array}$$

  There are two subcases to consider:

  * Subcase $t = \top$. Since any state refines $\top$, we have $r \leq \top$.
  * Subcase $t \neq \top$.

$$\begin{array}{ll} & \exists s' \in \mathcal{Q}_2, (\exists t' \in \mathcal{Q}_3, t \xrightarrow{\alpha}_3 t' \text{ and } s' \leq t') \text{ and } r' \leq s' \\ \Rightarrow & \text{(Since } r' \leq s' \text{ and } s' \leq t', \text{ by the induction hypothesis [H1])} \\ & \exists t' \in \mathcal{Q}_3, t \xrightarrow{a}_3 t' \text{ and } r' \leq t' \end{array}$$

(4) Now, let us consider Definition 5 (4). Given $C_1 \leq C_2$, by Definition 5 (4), we know there is a probability distribution $\delta_{12} \subset \mathcal{Q}_1 \times \mathcal{Q}_2 \times [0,1]$, such that, $\forall f_1(r') \in \sigma_1(r)(r'), s' \in \mathcal{Q}_2$,

$$(A) \quad \sum_{r' \in \mathcal{Q}_1} (f_1(r') * \delta_{12}(r')(s')) \in \sigma_2(s)(s'), \\ \text{and } \forall r' \in \mathcal{Q}_1, \delta_{12}(r')(s') > 0 \Rightarrow r' \leq s'$$

Given $C_2 \leq C_3$, by Definition 5 (4), we know there is a probability distribution $\delta_{23} \subset \mathcal{Q}_2 \times \mathcal{Q}_3 \times [0,1]$, such that, $\forall f_2(s') \in \sigma_2(s)(s'), t' \in \mathcal{Q}_3$,

$$(B) \quad \sum_{s' \in \mathcal{Q}_1} (f_2(s') * \delta_{23}(s')(t')) \in \sigma_3(t)(t'), \\ \text{and } \forall s' \in \mathcal{Q}_2, \delta_{23}(s')(t') > 0 \Rightarrow s' \leq t'$$

We want to establish a $\delta_{13} \subset \mathcal{Q}_1 \times \mathcal{Q}_3 \times [0,1]$ such that Definition 5 (4) holds. Let δ_{13} be

$$\delta_{13}(r')(t') = \sum_{s' \in \mathcal{Q}_2} \delta_{12}(r')(s') * \delta_{23}(s')(t')$$

We want to check that δ_{13} satisfies the condition Definition 5 (4) for all

$f_1(r') \in \delta_1(r)(r'), t' \in \mathcal{Q}_3$.

$$
\begin{array}{ll}
 & \sum_{r' \in \mathcal{Q}_1} \big(f_1(r') * \delta_{13}(r')(t)\big) \\
= & \text{(By definition of } \delta_{13}) \\
 & \sum_{r' \in \mathcal{Q}_1} \big(f_1(r') * \sum_{s' \in \mathcal{Q}_2} \delta_{12}(r')(s') * \delta_{23}(s')(t')\big) \\
= & \text{(By distribution of } * \text{ over } +) \\
 & \sum_{r' \in \mathcal{Q}_1} \sum_{s' \in \mathcal{Q}_2} f_1(r') * \delta_{12}(r')(s') * \delta_{23}(s')(t') \\
= & \text{(By commutativity and associativity of } +) \\
 & \sum_{s' \in \mathcal{Q}_2} \sum_{r' \in \mathcal{Q}_1} f_1(r') * \delta_{12}(r')(s') * \delta_{23}(s')(t') \\
= & \text{(By (A), } \exists f_2 \in \sigma_2(s), f_2(s') = \sum_{r' \in \mathcal{Q}_1} f_1(r') * \delta_{12}(r')(s')) \\
 & \sum_{s' \in \mathcal{Q}_2} f_2(s') * \delta_{23}(s')(t') \\
\in & \text{(By (B), which holds for all } f_2 \in \sigma_2(s)) \\
 & \sigma_3(t)(t')
\end{array}
$$

So we have the desired result $\sum_{r' \in \mathcal{Q}_1} \big(f_1(r') * \delta_{13}(r')(t)\big) \in \sigma_3(t)(t')$.

(5) If $r \in \mathcal{Q}_1^a$ and $t \in \mathcal{Q}_3^p$ and $r \leq s$ and $s \leq t$, then there are two subcases to consider: $s \in \mathcal{Q}_2^a$ and $s \in \mathcal{Q}_2^p$.

– Subcase $s \in \mathcal{Q}_2^a$.

$$
\begin{array}{ll}
 & r \leq s \text{ and } s \leq t \\
\iff & \text{(By Definition 5 [Contract refinement] (5))} \\
 & r \leq s \text{ and } \exists t^a \in \mathcal{Q}_3^a : t \overset{>0}{\dashrightarrow}_3{}^{+} t^a \wedge s \leq t^a \text{ and} \\
 & \forall t' \in \mathcal{Q}_3, \big(t \overset{>0}{\dashrightarrow}_3 t' \implies s \leq t'\big) \\
\Rightarrow & \text{(Since } r \leq s \text{ and } s \leq t^a \text{, by induction hypothesis [H1]} \\
 & \text{where } r' = r, s' = s, t' = t^a) \\
 & r \leq s \text{ and } \exists t^a \in \mathcal{Q}_3^a : t \overset{>0}{\dashrightarrow}_3{}^{+} t^a \wedge r \leq t^a \text{ and} \\
 & \forall t' \in \mathcal{Q}_3, \big(t \overset{>0}{\dashrightarrow}_3 t' \implies s \leq t'\big) \\
\Rightarrow & \text{(Since } r \leq s \text{ and } s \leq t' \text{, by induction hypothesis [H1]} \\
 & \text{where } r' = r, s' = s, t' = t') \\
 & \exists t^a \in \mathcal{Q}_3^a : t \overset{>0}{\dashrightarrow}_3{}^{+} t^a \wedge r \leq t^a \text{ and} \\
 & \forall t' \in \mathcal{Q}_3, \big(t \overset{>0}{\dashrightarrow}_3 t' \implies r \leq t'\big) \\
\iff & \text{(By Definition 5 [Contract refinement] (5))} \\
 & r \leq t
\end{array}
$$

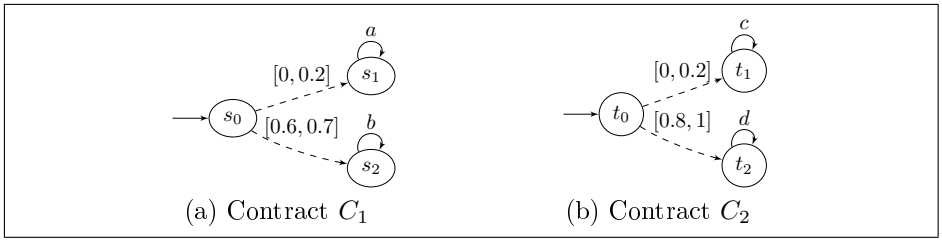
– Subcase $s \in \mathcal{Q}_2^p$.

$r \leq s$ and $s \leq t$
$\iff$ (By Definition 5 [Contract refinement] (5))
$\exists s^a \in \mathcal{Q}_2^a : s \overset{>0}{\dashrightarrow}_2^+ s^a \wedge r \leq s^a$ and
$\forall s' \in \mathcal{Q}_2, \left(s \overset{>0}{\dashrightarrow}_2 s' \implies r \leq s'\right)$ and $s \leq t$
$\iff$ (By Definition 5 [Contract refinement] (4))
(1) $\exists s^a \in \mathcal{Q}_2^a : s \overset{>0}{\dashrightarrow}_2^+ s^a \wedge r \leq s^a$ and
(2) $\forall s' \in \mathcal{Q}_2, \left(s \overset{>0}{\dashrightarrow}_2 s' \implies r \leq s'\right)$ and
(3) $\exists \delta : \mathcal{Q}_2 \times \mathcal{Q}_3 \to [0,1], \forall f(s') \in \sigma_3(s)(s')$ and
$\forall t' \in \mathcal{Q}_3, \sum_{s' \in \mathcal{Q}_2} (f(s') * \delta(s')(t')) \subseteq \sigma_3(t)(t')$ and
$\forall s' \in \mathcal{Q}_2 : \left(\delta(s')(t') > 0 \implies s' \leq t'\right)$
$\Rightarrow$ (By (1), $s \leq t$ and Definition 5 (4,5), we have (4);
from (2) and (3), we know $\forall s', t', r \leq s'$ and $s' \leq t'$,
thus we apply induction hypothesis [H1] where
$r' = r, s' = s', t' = t'$, we have (5))
(1) $\exists s^a \in \mathcal{Q}_2^a : s \overset{>0}{\dashrightarrow}_2^+ s^a \wedge r \leq s^a$ and
(4) $\exists t^a \in \mathcal{Q}_3^a : t \overset{>0}{\dashrightarrow}_3^+ t^a \wedge s^a \leq t^a$ and
(5) $\forall t' \in \mathcal{Q}_3, \left(t \overset{>0}{\dashrightarrow}_3 t' \implies r \leq t'\right)$
$\Rightarrow$ (From (1) and (4), we know $r \leq s^a$ and $s^a \leq t^a$,
thus we can apply the induction hypothesis [H1] where
$r' = r, s' = s^a, t' = t^a$)
$\exists t^a \in \mathcal{Q}_3^a : t \overset{>0}{\dashrightarrow}_3^+ t^a \wedge r \leq t^a$ and
$\forall t' \in \mathcal{Q}_3, \left(t \overset{>0}{\dashrightarrow}_3 t' \implies r \leq t'\right)$
$\iff$ (By Definition 5 [Contract refinement] (5))
$r \leq t$

(6) Similar to the proof in (5).

□

Remark: The converse of Corollary 1, item 2 does not hold, as shown by the counter example in Figure 19. There is no model for C_1, i.e., $\mathcal{M}(C_1) = \emptyset$, while there are models for C_2. Thus, we have $\mathcal{M}(C_1) \subset \mathcal{M}(C_2)$ and $C_1 \not\leq C_2$.



(a) Contract C_1 (b) Contract C_2

Figure 19: Counter example for the converse of Corollary 1, item 2.

A.2 Contract Projection

Lemma 4 [Projection and refinement] For all contracts $C_1 = (\mathcal{Q}_1, \mathcal{A}, \rightarrow_1, \dashrightarrow_1, s_0)$ and $C_2 = (\mathcal{Q}_2, \mathcal{A}, \rightarrow_2, \dashrightarrow_2, t_0)$ and for all $\mathcal{B} \subseteq \mathcal{A}$ such that $\pi_{\mathcal{B}}(C_1)$ and $\pi_{\mathcal{B}}(C_2)$ are defined, if $C_1 \leq C_2$ then $\pi_{\mathcal{B}}(C_1) \leq \pi_{\mathcal{B}}(C_2)$.

Proof. Let $\pi_{\mathcal{B}}(C_1) = (\mathcal{Q}_3, \mathcal{A}, \rightarrow_3, \sigma_3, \mathbf{s_0})$ and $\pi_{\mathcal{B}}(C_2) = (\mathcal{Q}_4, \mathcal{A}, \rightarrow_4, \sigma_4, \mathbf{t_0})$.

Given states s and t in $\mathcal{Q}_1$ and in $\mathcal{Q}_2$, respectively, let $\mathbf{s} \in Q_3$ and $\mathbf{t} \in Q_4$ be states with $s \in \mathbf{s}$ and $t \in \mathbf{t}$. Notice that the states of $\mathcal{Q}_3$ and $\mathcal{Q}_4$ are not equivalence classes of the states in $\mathcal{Q}_1$ and $\mathcal{Q}_2$: s may be part of several states of $\mathcal{Q}_3$. To show that $s_0 \leq t_0 \Rightarrow \mathbf{s_0} \leq \mathbf{t_0}$, we show the general case: for all $s \in \mathcal{Q}_1, t \in \mathcal{Q}_2$, if $s \leq t$, then $\mathbf{s} \leq \mathbf{t}$. We prove this lemma by structural induction. We have the following induction hypothesis: for all $s' \in \mathcal{Q}_1, t' \in \mathcal{Q}_2, \mathbf{s}' \in \mathcal{Q}_3, \mathbf{t}' \in \mathcal{Q}_4$, such that $s' \in \mathbf{s}'$ and $t' \in \mathbf{t}'$,

$$s' \leq t' \implies \mathbf{s}' \leq \mathbf{t}' \qquad \text{[H]}$$

We have the following cases to consider:

- Case $s = \top$. Actions leading to a $\top$ state are kept in the projection. There is no state in the projection containing other states than $\top$. Therefore, both $\mathbf{s}$ and $\mathbf{t}$ are $\top$.

- Case $t = \bot$. Actions leading to a $\bot$ state are kept in the projection. There is no state in the projection containing other states than $\bot$. Therefore, in both cases, $\mathbf{s}$ and $\mathbf{t}$ are $\bot$.

- Case $s \in \mathcal{Q}_1^a, t \in \mathcal{Q}_2^a \cup \{\top\}$. There are two cases to consider. The case that $\exists \alpha \in \mathcal{Q}_1, s \xrightarrow{\alpha}_1 \top$ is taken care in case (b).

  (a) $\forall t' \neq \top \in \mathcal{Q}_2,\ (t \xrightarrow{\alpha}_2 t') \implies (\exists s' \in \mathcal{Q}_1,\ s \xrightarrow{\alpha}_1 s' \wedge s' \leq t')$.
  If $\alpha \in \mathcal{B}$, this action transition is kept in $\pi_{\mathcal{B}}(C_1)$ and $\pi_{\mathcal{B}}(C_2)$. So we have $\mathbf{s} \xrightarrow{\alpha}_3 \mathbf{s}'$ and $\mathbf{t} \xrightarrow{\alpha}_4 \mathbf{t}'$. From $s' \leq t'$, by induction hypothesis [H], we have $\mathbf{s}' \leq \mathbf{t}'$. So we have $\forall \mathbf{t}' \neq \top \in \mathcal{Q}_4,\ (\mathbf{t} \xrightarrow{\alpha}_4 \mathbf{t}') \implies (\exists \mathbf{s}' \in \mathcal{Q}_3,\ \mathbf{s} \xrightarrow{\alpha}_3 \mathbf{s}' \wedge \mathbf{s}' \leq \mathbf{t}')$ which meets Definition 5 ($\leq$) (3a).
  If $\alpha \notin \mathcal{B}$, this action transition does not appear in $\pi_{\mathcal{B}}(C_1)$ and $\pi_{\mathcal{B}}(C_2)$. We have $\{s, s'\} \subseteq \mathbf{s}$ and $\{t, t'\} \subseteq \mathbf{t}$. By induction hypothesis [H], we have $\mathbf{s} \leq \mathbf{t}$.

  (b) $\forall s' \in \mathcal{Q}_1,\ (s \xrightarrow{\alpha}_1 s') \implies (t = \top \vee \exists t' \in \mathcal{Q}_2,\ t \xrightarrow{\alpha}_2 t' \wedge s' \leq t')$.
  For the case $t = \top$, since actions leading to a $\top$ state are kept in the projection, there is no state in the projection containing other states than $\top$. Therefore, $\mathbf{t}$ is $\top$. By Definition 5, any state refines $\top$, so we have $\mathbf{s} \leq \mathbf{t}$.
  For the case $\exists t' \in \mathcal{Q}_2,\ t \xrightarrow{\alpha}_2 t' \wedge s' \leq t'$, we have two subcases to consider:

  * If $\alpha \in \mathcal{B}$, this action transition is kept in $\pi_{\mathcal{B}}(C_1)$ and $\pi_{\mathcal{B}}(C_1)$. So we have $\mathbf{s} \xrightarrow{\alpha}_3 \mathbf{s}'$ and $\mathbf{t} \xrightarrow{\alpha}_4 \mathbf{t}'$. From $s' \leq t'$, by induction hypothesis [H], we have $\mathbf{s}' \leq \mathbf{t}'$. So we have $\forall \mathbf{s}' \in \mathcal{Q}_3,\ (\mathbf{s} \xrightarrow{\alpha}_3 \mathbf{s}') \implies \exists \mathbf{t}' \in \mathcal{Q}_4,\ \mathbf{t} \xrightarrow{\alpha}_2 \mathbf{t}' \wedge \mathbf{s}' \leq \mathbf{t}'$, which meets Definition 5 ($\leq$) (3b).

  - If $\alpha \notin \mathcal{B}$, this action transition does not appear in $\pi_{\mathcal{B}}(C_1)$ and $\pi_{\mathcal{B}}(C_2)$. We have $\{s, s'\} \subseteq \mathbf{s}$ and $\{t, t'\} \subseteq \mathbf{t}$. By induction hypothesis [H], we have $\mathbf{s} \leq \mathbf{t}$.

- Case $s \in \mathcal{Q}_1^p, t \in \mathcal{Q}_2^p$. By Definition 5 (4), we know $s \overset{P_1}{\dashrightarrow}_1 s'$, $t \overset{P_2}{\dashrightarrow}_2 t'$ and $s' \leq t'$. Projection only has effect on action states, the probabilistic transitions remain the same (up to their target states). That is, we have (1) $\mathbf{s} \overset{P_3}{\dashrightarrow}_3 \mathbf{s}'$ and (2) $\mathbf{t} \overset{P_4}{\dashrightarrow}_4 \mathbf{t}'$. From $s' \leq t'$, by induction hypothesis [H], we have (3) $\mathbf{s}' \leq \mathbf{t}'$. From (1), (2), (3), by Definition 5 (4), we have $\mathbf{s} \leq \mathbf{t}$.

- Case $s \in \mathcal{Q}_1^a, t \in \mathcal{Q}_2^p$. By Definition 5 (5), $\exists t^a \in \mathcal{Q}_2^a : t \overset{>0}{\dashrightarrow}_2{}^{+} t^a \wedge s \leq t^a$ and $\forall t' \in \mathcal{Q}_2$, $\left(t \overset{>0}{\dashrightarrow}_2 t' \implies s \leq t'\right)$. If we have $t' \in \mathcal{Q}_2^p$, we have $s \leq t'$. Projection does not have effect on probabilistic transitions, by induction hypothesis [H], we are done. If $t' \in \mathcal{Q}_2^a$, then we have $s \leq t^a$. Since $s \in \mathcal{Q}_1^a$, this falls into the case $s \in \mathcal{Q}_1^a, t \in \mathcal{Q}_2^a$, which has been proved above.

- Case $s \in \mathcal{Q}_1^p, t \in \mathcal{Q}_2^a$. Similar reasoning as the case $s \in \mathcal{Q}_1^a, t \in \mathcal{Q}_2^p$.

□

B Contract Composition

B.1 Congruence of Refinement for Parallel Composition

Lemma 5 (Congruence of refinement for $||_{\mathcal{I}}$)**.** *For all contracts C_1, C_2, and C_3, and for all interaction set $\mathcal{I}$, if $C_1 \leq C_2$, then $C_1||_{\mathcal{I}}C_3 \leq C_2||_{\mathcal{I}}C_3$.*

Proof. Let

$$\begin{array}{rcl} C_1 & = & (\mathcal{Q}_1, \mathcal{A}_1, \rightarrow_1, \sigma_1, s_0) \\ C_2 & = & (\mathcal{Q}_2, \mathcal{A}_2, \rightarrow_2, \sigma_2, t_0) \\ C_3 & = & (\mathcal{Q}_3, \mathcal{A}_3, \rightarrow_3, \sigma_3, u_0) \\ C_1||_{\mathcal{I}}\, C_3 & = & (\mathcal{Q}_{13}, \mathcal{A}_{13}, \rightarrow_{13}, \sigma_{13}, (s_0, u_0)) \\ C_2||_{\mathcal{I}}\, C_3 & = & (\mathcal{Q}_{23}, \mathcal{A}_{23}, \rightarrow_{23}, \sigma_{23}, (t_0, u_0)) \end{array}$$

Let $\theta \subseteq \mathcal{Q}_1 \times \mathcal{Q}_2$ be the refinement relation stating that $s \leq t$. Let $\theta' \subseteq \mathcal{Q}_{13} \times \mathcal{Q}_{23}$ be a binary relation such that $((s, u), (t, u)) \in \theta'$ if $(s, t) \in \theta$. We now prove that θ' allows us to establish that $(s, u) \leq (t, u)$.

Notation: For all interval σ, let $\underline{\sigma}$ and $\overline{\sigma}$ denote respectively the lower bound and the upper bound of σ.

First, we consider the 3 cases involving the state $\top_i$.

(a) Case $s = \top_1$. Since $s \leq t$, by Definition 5 ($\leq$) (1), $t = \top_2$. By Definition 13 (Parallel composition), both composed states are $\top$. Since $\top \leq \top$, we have the desired result.

(b) Case $t = \top_2$. By Definition 13 [Parallel composition], the composed state (t, u) is replaced by $\top$. Since any state refines $\top$, we have the desired result.

(c) Case $u = \top_3$. By Definition 13 [Parallel composition], both composed states are $\top$. Since $\top \leq \top$, we have the desired result.

Second, we consider the 3 cases involving the state $\bot_i$:

(a) Case $s = \bot_1$. By Definition 13 [Parallel composition], the composed state (s, u) is replaced by $\bot$. Since $\bot$ refines any state, we have the desired result.

(b) Case $t = \bot_2$. Since $s \leq t$, by Definition 5 ($\leq$) (2), s is $\bot_1$. By Definition 13 [Parallel composition], both composed states are $\bot$. Since $\bot \leq \bot$, we have the desired result.

(c) Case $u = \bot_3$. By Definition 13 [Parallel composition], both composed states are $\bot$. Since $\bot \leq \bot$, we have the desired result.

Now, we consider cases where states s, t, u are neither $\top_i$ nor $\bot_i$. We have the following co-induction hypothesis: for all s', t', u' such that s', t', u' are the next states of s, t and u respectively, and $((s', u'), (t', u')) \in \theta'$,

$$s' \leq t' \Rightarrow (s', u') \leq (t', u') \qquad \text{[H]}$$

Given $((s, u), (t, u)) \in \theta'$, we have the following cases to consider.

- Case $s \in \mathcal{Q}_1^a, t \in \mathcal{Q}_2^a, u \in \mathcal{Q}_3^a$. Since $s \leq t$, we have (1) $s \xrightarrow{\alpha}_1 s'$; (2) $t \xrightarrow{\alpha}_2 t'$; (3) $u \xrightarrow{\beta}_3 u'$; (4) $s' \leq t'$. There are three subcases to consider:

  (a) Subcase $\alpha|\beta \in \mathcal{I}$.
  By (1), (3) and rule [R3], we have (5) $(s, u) \xrightarrow{\alpha|\beta}_{12} (s', u')$.
  By (2), (3) and rule [R3], we have (6) $(t, u) \xrightarrow{\alpha|\beta}_{23} (t', u')$.
  From (4), by co-induction hypothesis [H], we have (7) $(s', u') \leq (t', u')$. By Definition 5 (3), we thus have $(s, u) \leq (t, u)$.

  (b) Subcase $\alpha \in \mathcal{I}$.
  By (1), (3) and rule [R1], we have (5) $(s, u) \xrightarrow{\alpha}_{12} (s', u)$.
  By (2), (3) and rule [R1], we have (6) $(t, u) \xrightarrow{\alpha}_{23} (t', u)$.
  From (4), by co-induction hypothesis [H], we have (7) $(s', u) \leq (t', u)$.
  By Definition 5 (3), we thus have $(s, u) \leq (t, u)$.

  (c) Subcase $\beta \in \mathcal{I}$.
  By (1), (3) and rule [R2], we have (5) $(s, u) \xrightarrow{\beta}_{12} (s, u')$.
  By (2), (3) and rule [R2], we have (6) $(t, u) \xrightarrow{\beta}_{23} (t, u')$.
  From (4), by co-induction hypothesis [H], we thus have (7) $(s, u') \leq (t, u')$.

  For each subcase, from (5), (6), (7), and Definition 5 (3), we have $(s, u) \leq (t, u)$.

- Case $s \in \mathcal{Q}_1^a, t \in \mathcal{Q}_2^a, u \in \mathcal{Q}_3^p$. Since $s \leq t$, we have (1) $s \xrightarrow{\alpha}_1 s'$; (2) $t \xrightarrow{\alpha}_2 t'$; (3) $u \overset{P_3}{\dashrightarrow}_3 u'$; (4) $s' \leq t'$.
  By (1), (3) and rule [R6], we have (5) $(s, u) \overset{P_3}{\dashrightarrow}_{12} (s, u')$.
  By (2), (3) and rule [R6], we have (6) $(t, u) \overset{P_3}{\dashrightarrow}_{23} (t, u')$.
  From (4), by co-induction hypothesis [H], we have $(s, u') \leq (t, u')$. Let $\delta(s, u')(t, u') = 1$. By Definition 5 (4), we thus have $(s, u) \leq (t, u)$.

- Case $s \in \mathcal{Q}_1^a, t \in \mathcal{Q}_2^p, u \in \mathcal{Q}_3^a$. Since $s \leq t$, we have (1) $s \xrightarrow{\alpha}_1 s'$; (2) $t \xrightarrow{P_2}_2 t'$; (3) $u \xrightarrow{\beta}_3 u'$. (4) $\exists t^a \in \mathcal{Q}_2^a : t \xrightarrow{>0}{}_2^+ t^a \wedge s \leq t^a$; $\forall t' \in \mathcal{Q}_2$, $\left(t \xrightarrow{>0}_2 t' \implies s \leq t'\right)$. By (2), (3) and rule [R6], we have $(t,u) \xrightarrow{P_2}_{23} (t',u)$. From (4), by co-induction hypothesis [H], we have $(s,u) \leq (t',u)$. By Definition 5 (5), we have $(s,u) \leq (t,u)$.

- Case $s \in \mathcal{Q}_1^a, t \in \mathcal{Q}_2^p, u \in \mathcal{Q}_3^p$. Since $s \leq t$, we have (1) $s \xrightarrow{\alpha}_1 s'$; (2) $t \xrightarrow{[p_1,p_2]}_2 t'$; (3) $u \xrightarrow{[p_3,p_4]}_3 u'$. (4) $\exists t^a \in \mathcal{Q}_2^a : t \xrightarrow{>0}{}_2^+ t^a \wedge s \leq t^a$; $\forall t' \in \mathcal{Q}_2$, $\left(t \xrightarrow{>0}_2 t' \implies s \leq t'\right)$.

  By (1), (3) and rule [R6], we have $(s,u) \xrightarrow{[p_3,p_4]}_{12} (s,u')$.

  By (2), (3) and rule [R4], we have $(t,u) \xrightarrow{[p_1 * p_3, p_2 * p_4]}_{12} (t',u')$.
  This yields:

$$
\begin{array}{lll}
(\dagger_1) & & \sigma_{23}(t,u)(t',u') \\
& = & [\underline{\sigma_{23}}(t,u)(t',u'), \overline{\sigma_{23}}(t,u)(t',u')] \\
& = & [\underline{\sigma_2}(t)(t') * \underline{\sigma_3}(u)(u'), \overline{\sigma_2}(t)(t') * \overline{\sigma_3}(u)(u')]
\end{array}
$$

  By Lemma 1 [Reflexivity of refinement], $u \leq u$. This means that there exists a probability distribution δ_3 that satisfies the condition (4) of Definition 5 for all $f_3(u') \in \sigma_3(u)(u')$ and $u' \in \mathcal{Q}_3$. By definition of f_3, we have:

$$
\begin{array}{lll}
(\dagger_2) & \displaystyle\sum_{u' \in \mathcal{Q}_3} f_3(u') * \delta_3(u')(u') \in \sigma_3(u)(u') \\
\iff & \displaystyle\sum_{u' \in \mathcal{Q}_3} \sigma_3(u)(u') * \delta_3(u')(u') \subseteq \sigma_3(u)(u')
\end{array}
$$

  We want to check that there exists a δ that satisfies the condition Definition 5 (4) for all $f(s,u') \in \sigma_{13}(s,u)(s,u')$ and $(t',u') \in \mathcal{Q}_{23}$. Let

$\delta((s,u'))((t',u')) \in \sigma_2(t)(t') * \delta_3(u')(u')$

(By definition [F2] in Figure 4: $[a,b]*[c,d] = [a*c, b*d]$)
$\sigma_2(t)(t') * \sigma_3(u)(u') \subseteq [\underline{\sigma_2}(t)(t') * \underline{\sigma_3}(u)(u'), \overline{\sigma_2}(t)(t') * \overline{\sigma_3}(u)(u')]$

$\Rightarrow$ (By $\dagger_2$ and by set theory
$[a,b]*[c,d] \subseteq [e,f] \wedge [c_1,d_1] \subseteq [c,d] \implies [a,b]*[c_1,d_1] \subseteq [e,f]$)
$\sum_{u' \in \mathcal{Q}_3} \sigma_2(t)(t') * \sigma_3(u)(u') * \delta_3(u')(u')$
$\subseteq [\underline{\sigma_2}(t)(t') * \underline{\sigma_3}(u)(u'), \overline{\sigma_2}(t)(t') * \overline{\sigma_3}(u)(u')]$

$\Rightarrow$ (By definition of δ and commutativity of $*$)
$\sum_{u' \in \mathcal{Q}_3} (\sigma_3(u)(u') * \delta(s,u')(t',u'))$
$\subseteq [\underline{\sigma_2}(t)(t') * \underline{\sigma_3}(u)(u'), \overline{\sigma_2}(t)(t') * \overline{\sigma_3}(u)(u')]$

$\iff$ (By (1), (3), rule [R6], $\sum_{(s,u') \in \mathcal{Q}_{13}} \sigma_{13}(s,u)(s,u') = \sum_{u' \in \mathcal{Q}_3} \sigma_3(u)(u')$)
$\sum_{(s,u') \in \mathcal{Q}_{13}} (\sigma_{13}(s,u)(s,u') * \delta(s,u')(t',u'))$
$\subseteq [\underline{\sigma_2}(t)(t') * \underline{\sigma_3}(u)(u'), \overline{\sigma_2}(t)(t') * \overline{\sigma_3}(u)(u')]$

$\iff$ (By $(\dagger_1)$)
$\sum_{(s,u') \in \mathcal{Q}_{13}} (\sigma_{13}(s,u)(s,u') * \delta(s,u')(t',u')) \subseteq \sigma_{23}(t,u)(t',u')$,

$\iff$ (By definition of f)
$\sum_{(s,u') \in \mathcal{Q}_{13}} (f(s,u') * \delta(s,u')(t',u')) \in \sigma_{23}(t,u)(t',u')$

So we have the desired result $(s,u) \leq (t,u)$.

- Case $s \in \mathcal{Q}_1^p, t \in \mathcal{Q}_2^a, u \in \mathcal{Q}_3^a$. Similar to the case $s \in \mathcal{Q}_1^a, t \in \mathcal{Q}_2^p, u \in \mathcal{Q}_3^a$.
- Case $s \in \mathcal{Q}_1^p, t \in \mathcal{Q}_2^a, u \in \mathcal{Q}_3^p$. Similar to the case $s \in \mathcal{Q}_1^a, t \in \mathcal{Q}_2^p, u \in \mathcal{Q}_3^p$.
- Case $s \in \mathcal{Q}_1^p, t \in \mathcal{Q}_2^p, u \in \mathcal{Q}_3^a$. We have (1) $s \overset{P_1}{\dashrightarrow}_1 s'$; (2) $t \overset{P_2}{\dashrightarrow}_2 t'$; (3) $u \overset{\alpha}{\rightarrow}_3 u'$. By (1), (3) and rule [R5], we have (5) $(s,u) \overset{P_1}{\dashrightarrow}_{12} (s',u)$. By (2), (3) and rule [R5], we have (6) $(s,u) \overset{P_1}{\dashrightarrow}_{12} (s',u)$. We know that there is a probability distribution $\delta \subset \mathcal{Q}_1 \times \mathcal{Q}_2 \times [0,1]$, such that, $\forall f(s') \in \sigma_1(s)(s'), t' \in \mathcal{Q}_2$,

  $(\dagger)$ $\sum_{s' \in \mathcal{Q}_1} (f(s') * \delta(s')(t')) \in \sigma_2(t)(t')$ and $\forall s' \in \mathcal{Q}_1, \delta(s')(t') > 0 \Rightarrow s' \leq t'$

  Let $\delta' = \delta$. We want to check that δ' satisfies the condition Definition 5 (4)

for all $f(s',u) \in \sigma_{13}(s,u)(s',u)$ and $(t',u) \in \mathcal{Q}_{23}$.

$$\begin{array}{ll} & \text{(By definition of } \delta') \\ & \sum_{(s',u)\in\mathcal{Q}_{13}} (f(s',u) * \delta(s')(t')) \\ = & \text{(By (3) and rule [R5], } \sum_{(s',u)\in\mathcal{Q}_{13}} f(s',u) = \sum_{s'\in\mathcal{Q}_1} f(s')) \\ & \sum_{(s',u)\in\mathcal{Q}_{13}} (f(s') * \delta(s')(t')) \\ \in & \text{(By (†))} \\ & \sigma_2(t)(t') \\ = & \text{(By (3) and rule [R5], } \sigma_{23}(t,u)(t',u) = \sigma_2(t)(t')) \\ & \sigma_{23}(t,u)(t',u), \end{array}$$

So we have the desired result $(s,u) \leq (t,u)$.

- Case $s \in \mathcal{Q}_1^p, t \in \mathcal{Q}_2^p, u \in \mathcal{Q}_3^p$. We have (1) $s \overset{[p_1,p_2]}{\dashrightarrow}_1 s'$ and (2) $u \overset{[p_3,p_4]}{\dashrightarrow}_3 u'$. From (1), (2), by rule [R4], we have $(s,u) \overset{[p_1*p_3,p_2*p_4]}{\dashrightarrow}_{13} (s',u')$. This yields:

$$(\dagger_1) \quad \sigma_{13}(s,u)(s',u') = \sigma_1(s)(s') * \sigma_3(u)(u')$$

Since $s \leq t$, by Definition 5 [Contract Refinement] (4), we know $t \overset{[p_5,p_6]}{\dashrightarrow}_2 t'$ for some t', p_5, p_6 and $s' \leq t'$. By $u \overset{[p_3,p_4]}{\dashrightarrow}_3 u'$ and rule [R4], we know $(t,u) \overset{[p_5*p_3,p_6*p_4]}{\dashrightarrow}_{23} (t',u')$. This yields:

$$(\dagger_2) \quad \sigma_{23}(t,u)(t',u') = \sigma_2(t)(t') * \sigma_3(u)(u')$$

By Definition 5 (4), we know there is a probability distribution $\delta \subset \mathcal{Q}_1 \times \mathcal{Q}_2 \times [0,1]$, s.t.,

$$(\dagger_3) \quad \forall f(s') \in \sigma_1(s)(s'), t' \in \mathcal{Q}_2, \sum_{s'\in\mathcal{Q}_1} (f(s') * \delta(s')(t')) \in \sigma_2(t)(t'), \\ \text{and } s' \leq t' \text{ if } \delta(s')(t') > 0$$

We want to show that there is a probability distribution $\delta' \subset \mathcal{Q}_{13} \times \mathcal{Q}_{23} \times [0,1]$, such that Definition 5 (4) holds. Let δ' be

$$\delta'(s',u'')(t',u') = \begin{cases} \delta(s')(t'), & \text{if } u'' = u' \\ 0, & \text{otherwise} \end{cases}$$

We want to check that δ' satisfies the condition Definition 5 (4) for all $f' \in \sigma_{13}(s,u))$ and $(t',u') \in \mathcal{Q}_{23}$. We prove it for all $t' \in \mathcal{Q}_2$ as follows.

$$
\begin{array}{ll}
 & (\text{By } (\dagger_3), f(s') \in \delta_1(s)(s')) \\
 & \sum_{s' \in \mathcal{Q}_1} \sigma_1(s)(s') * \delta(s')(t') \subseteq \sigma_2(t)(t') \\
\iff & (\text{By arithmetic, if } [a,b],[c,d],[e,f] \subseteq [0,1], \text{ then} \\
 & [a,b] \subseteq [c,d] \iff [a,b] * [e,f] \subseteq [c,d] * [e,f]. \\
 & \text{We also know that } \sigma_3(u)(u') \subseteq [0,1]) \\
 & \forall u' \in \mathcal{Q}_3, \sum_{s' \in \mathcal{Q}_1} \sigma_1(s)(s') * \sigma_3(u)(u') * \delta(s')(t'), \subseteq \sigma_2(t)(t') * \sigma_3(u)(u') \\
\iff & (\text{By } (\dagger_1) \text{ and } (\dagger_2)) \\
 & \forall u' \in \mathcal{Q}_3, \sum_{s' \in \mathcal{Q}_1} \sigma_{13}(s,u)(s',u') * \delta'(s')(t') \subseteq \sigma_{23}(t,u)(t',u') \\
\iff & (\text{For } u'' \neq u', \sum_{(s',u'') \in \mathcal{Q}_{13}} \text{ does not add any non-zero term.} \\
 & \text{Also by definition of } \delta'.) \\
 & \forall u' \in \mathcal{Q}_3, \sum_{(s',u'') \in \mathcal{Q}_{13}} \sigma_{13}(s,u)(s',u'') * \delta'(s',u'')(t',u') \subseteq \sigma_{23}(t,u)(t',u') \\
\iff & (\text{By definition of } f') \\
 & \forall u' \in \mathcal{Q}_3, \sum_{(s',u'') \in \mathcal{Q}_{13}} (f'(s',u'') * \delta'(s',u'')(t',u')) \in \sigma_{23}(t,u)(t',u')
\end{array}
$$

We have the desired result $(s,u) \leq (t,u)$.

□

Theorem 2 (Congruence of refinement for $||_{\mathcal{I}}$) For all contracts C_1, C_2, C_3, C_4 and an interaction set $\mathcal{I}$, if $C_1 \leq C_2$ and $C_3 \leq C_4$, then $C_1||_{\mathcal{I}} C_3 \leq C_2||_{\mathcal{I}} C_4$.

Proof.

$$
\begin{array}{ll}
 & C_1 \leq C_2 \text{ and } C_3 \leq C_4 \\
\Rightarrow & (\text{By Lemma 5 (Congruence of } \leq \text{ for } ||_{\mathcal{I}}) \text{ twice}) \\
 & C_1||_{\mathcal{I}}C_3 \leq C_2||_{\mathcal{I}}C_3 \text{ and } C_3||_{\mathcal{I}}C_2 \leq C_4||_{\mathcal{I}}C_2) \\
\Rightarrow & (\text{By commutativity of } ||_{\mathcal{I}}) \\
 & C_1||_{\mathcal{I}}C_3 \leq C_3||_{\mathcal{I}}C_2 \text{ and } C_3||_{\mathcal{I}}C_2 \leq C_4||_{\mathcal{I}}C_2) \\
\Rightarrow & (\text{By Lemma 2 (Transitivity of } \leq)) \\
 & C_1||_{\mathcal{I}}C_3 \leq C_4||_{\mathcal{I}}C_2 \\
\Rightarrow & (\text{By commutativity of } ||_{\mathcal{I}}) \\
 & C_1||_{\mathcal{I}}C_3 \leq C_2||_{\mathcal{I}}C_4
\end{array}
$$

□

B.2 Conjunction of Contracts

Theorem 6 (Soundness of conjunction) For all contracts C_1 and C_2, $\pi_{\mathcal{A}_i}(C_1 \wedge C_2) \leq C_i$ for $i = 1, 2$.

Proof. We only show the proof for $\pi_{\mathcal{A}_1}(C_1 \wedge C_2) \leq C_1$ as the proof for $\pi_{\mathcal{A}_2}(C_1 \wedge C_2) \leq C_2$ is similar. If $C_1 \wedge C_2 = C_\perp$ then $\pi_{\mathcal{A}_i}(C_1 \wedge C_2) = C_\perp$, and the claim

follows. We now consider the cases where $C_1 \wedge C_2 \neq C_\perp$. Let

$$\begin{array}{rcl} C_1 & = & (\mathcal{Q}_1, \mathcal{A}_1, \rightarrow_1, \dashrightarrow_1, s_0) \\ C_2 & = & (\mathcal{Q}_2, \mathcal{A}_2, \rightarrow_2, \dashrightarrow_2, t_0) \\ \pi_{\mathcal{A}_1}(C_1 \wedge C_2) & = & (\mathcal{Q}_{12}, \mathcal{A}_1, \rightarrow_{12}, \dashrightarrow_{12}, (s_0, t_0)) \end{array}$$

Let $\theta \subseteq \mathcal{Q}_{12} \times \mathcal{Q}_1$ be a binary relation such that $\{((s,t),s) \mid s \in \mathcal{Q}_1, t \in \mathcal{Q}_2, (s,t) \in \mathcal{Q}_{12}\}$. We want to show that $\theta \subseteq \leq$. Since projection is only done for action transitions where the action is in $\mathcal{A}_2$ and not in $\mathcal{A}_1$, it only affects the case [LiftR].

First, we consider the 2 cases involving the state $\top_i$.

- Case $s = \top_1$. As any state refines $\top_1$, we are done.
- Case $t = \top_2$. We define a mapping ρ from $\mathcal{Q}_1 \times \mathcal{Q}_2$ to $\mathcal{Q}_1$, $\rho : (s, \top_2) \mapsto s$. According to rules [C2L] and [C4L], the macro-state $(s, \top_2)$ follows the transitions of s for any state s, hence ρ is a bijection. So $(s, \top_2) \leq s$.

Now, we consider cases where states s and t are neither $\top_i$ nor $\perp_i$. We have the following induction hypothesis: for all s', t' such that s', t' are the next states of s and t respectively, and $(s', t') \in \theta$,

$$(s', t') \leq s' \qquad [H]$$

Given $((s,t),s) \in \theta$, we have the following cases to consider.

- Case $s \in \mathcal{Q}_1^a, t \in \mathcal{Q}_2^a$. We have There are 3 subcases to consider.
  - Subcase $s \xrightarrow{\alpha}_1 s'$ and $t \xrightarrow{\alpha}_2 t'$. We have the following induction hypothesis:
    $$(s', t') \leq s' \qquad [\text{HC1}]$$
    Since we have $s \xrightarrow{\alpha}_1 s'$ and $(s,t) \xrightarrow{\alpha}_{12} (s', t')$ and [HC1], it is easy to check that Definition 5 [$\leq$] (3a) and (3b) are satisfied, and since (s,t) is not $\top$, Definition 5 [$\leq$] (1) is vacuously true. So we have $(s,t) \leq s$.
  - Subcase $s \xrightarrow{\alpha}_1 s'$ and $\alpha \notin \mathcal{A}_2$. We have the following induction hypothesis:
    $$(s', t) \leq s' \qquad [\text{HLiftL}]$$
    Since we have $s \xrightarrow{\alpha}_1 s'$ and $(s,t) \xrightarrow{\alpha}_{12} (s', t)$ and [HLiftL], it is easy to check that Definition 5 [$\leq$] (3a) and (3b) are satisfied and since (s,t) is not $\top$, Definition 5 (1) is vacuously true.
  - Subcase $t \xrightarrow{\alpha}_2 t'$ and $\alpha \notin \mathcal{A}_1$. We have the following induction hypothesis:
    $$(s, t') \leq s \qquad [\text{HLiftR}]$$
    Since $s \in \mathcal{Q}_1^a$, s is not $\top_1$. We thus know (s, t') is not $\top$. After projection on $\mathcal{A}_1$, we have $(s,t) = (s,t')$. By [HLiftR], we know $(s,t) \leq s$, so we are done.
- Case $s \in \mathcal{Q}_1^p, t \in \mathcal{Q}_2^a$. We have $s \overset{P}{\dashrightarrow}_1 s', t \in \mathcal{Q}^a$ and $s' \sim t$. By rule [C4L], we have $(s,t) \overset{P}{\dashrightarrow}_{12} (s', t)$. We have the following induction hypothesis:
  $$(s', t) \leq s' \qquad [\text{HC4L}]$$

Since $\leq$ is reflexive (by Lemma 1), we have $s \leq s$. We know that there is a probability distribution $\delta \subset \mathcal{Q}_1 \times \mathcal{Q}_1 \times [0,1]$, such that, $\forall f \in \sigma(s)$ and $s' \in \mathcal{Q}_1$,

$$(\dagger_2) \quad \sum_{s' \in \mathcal{Q}_1} (f(s') * \delta(s')(s')) \in \sigma_1(s)(s'), \text{ and } \delta(s')(s') > 0 \implies s' \leq s'$$

We want to establish a δ' such that for all $f'(s',t') \in \delta_{12}(s,t)(s',t')$, Definition 5 (4) holds. Let $\delta' \subset \mathcal{Q}_{12} \times \mathcal{Q}_1 \times [0,1]$ be defined as $\delta'(s',t')(s') = \delta(s')(s')$.

$$\begin{array}{ll} & \text{(By } (\dagger_2)\text{)} \\ & \sum_{s' \in \mathcal{Q}_1} (f(s') * \delta(s')(s')) \in \sigma_1(s)(s') \\ \iff & \text{(By definition of } f\text{)} \\ & \sum_{s' \in \mathcal{Q}_1} ([\underline{\sigma_1}(s)(s'), \overline{\sigma_1}(s)(s')] * \delta(s')(s')) \subseteq \sigma_1(s)(s') \\ \iff & \text{(By rule [C4L], } [\underline{\sigma_{12}}(s',t'), \overline{\sigma_{12}}(s',t')] = [\underline{\sigma_1}(s)(s'), \overline{\sigma_1}(s)(s')]\text{)} \\ & \sum_{(s',t') \in \mathcal{Q}_{12}} ([\underline{\sigma_{12}}(s',t'), \overline{\sigma_{12}}(s',t')] * \delta(s')(s')) \subseteq \sigma_1(s)(s') \\ \iff & \text{(By definition of } \delta'\text{)} \\ & \sum_{(s',t') \in \mathcal{Q}_{12}} ([\underline{\sigma_{12}}(s',t'), \overline{\sigma_{12}}(s',t')] * \delta'(s',t')(s')) \subseteq \sigma_1(s)(s') \\ \iff & \text{(By definition of } f'\text{)} \\ & \sum_{(s',t') \in \mathcal{Q}_{12}} (f'(s',t') * \delta'(s',t')(s')) \in \sigma_1(s)(s') \end{array}$$

Together with the induction hypothesis [HC4L], we thus have the desired result.

- Case $s \in \mathcal{Q}_1^a, t \in \mathcal{Q}_2^p$. Similar to the proof in case $s \in \mathcal{Q}_1^p, t \in \mathcal{Q}_2^a$.

- Case $s \in \mathcal{Q}_1^p, t \in \mathcal{Q}_2^p$. We have $s \overset{[p_1,p_2]}{\dashrightarrow}_1 s'$ and $t \overset{[p_3,p_4]}{\dashrightarrow}_2 t'$ and $s' \sim t'$. By rule [C3], we have $(s,t) \overset{[p5,p6]}{\dashrightarrow}_{12} (s',t')$ where $p_5 = \max(p_1,p_3)$ and $p_6 = \min(p_2,p_4)$. We have We have the following induction hypothesis:

$$(s',t') \leq s' \qquad \text{[HC3]}$$

Since $\leq$ is reflexive (by Lemma 1), we have $s \leq s$. We know that there is a probability distribution $\delta \subset \mathcal{Q}_1 \times \mathcal{Q}_1 \times [0,1]$, such that, $\forall f(s') \in \sigma(s)(s'), s' \in \mathcal{Q}_1$,

$$(\dagger_1) \quad \sum_{s' \in \mathcal{Q}_1} (f(s') * \delta(s')(s')) \in \sigma_1(s)(s'), \text{ and } \delta(s')(s') > 0 \implies s' \leq s'$$

We want to establish a δ' such that for all $f'(s',t') \in \delta_{12}(s,t)(s',t')$, Definition 5 (4) holds. Let $\delta' \subset \mathcal{Q}_{12} \times \mathcal{Q}_1 \times [0,1]$ be defined as $\delta'(s',t')(s') =$

$\delta(s')(s')$.

$$
\begin{array}{ll}
 & \text{(By } (\dagger_1)\text{)} \\
 & \sum_{s' \in \mathcal{Q}_1} (f(s') * \delta(s')(s')) \in \sigma_1(s)(s') \\
\iff & \text{(By definition of } f\text{)} \\
 & \sum_{s' \in \mathcal{Q}_1} ([\underline{\sigma_1}(s)(s'), \overline{\sigma_1}(s)(s')] * \delta(s')(s')) \subseteq \sigma_1(s)(s') \\
\iff & \text{(By rule [C3], } [\underline{\sigma_{12}}(s',t'), \overline{\sigma_{12}}(s',t')] \subseteq [\underline{\sigma_1}(s)(s'), \overline{\sigma_1}(s)(s')]\text{)} \\
 & \sum_{s' \in \mathcal{Q}_1} ([\underline{\sigma_{12}}(s',t'), \overline{\sigma_{12}}(s',t')] * \delta(s')(s')) \subseteq \sigma_1(s)(s'), \\
\iff & \text{(By Definition 15 [Unambiguous contract], the similarity between} \\
 & s' \text{ and } t' \text{ is a bijection, so the number of } (s',t') \text{ states is the same} \\
 & \text{as the number of } s' \text{ states.)} \\
 & \sum_{(s',t') \in \mathcal{Q}_{12}} ([\underline{\sigma_{12}}(s',t'), \overline{\sigma_{12}}(s',t')] * \delta(s')(s')) \subseteq \sigma_1(s)(s'), \\
\iff & \text{(By definition of } \delta'\text{)} \\
 & \sum_{(s',t') \in \mathcal{Q}_{12}} ([\underline{\sigma_{12}}(s',t'), \overline{\sigma_{12}}(s',t')] * \delta'(s',t')(s')) \subseteq \sigma_1(s)(s'), \\
\iff & \text{(By definition of } f'\text{)} \\
 & \sum_{(s',t') \in \mathcal{Q}_{12}} (f'(s',t') * \delta'(s',t')(s')) \in \sigma_1(s)(s')
\end{array}
$$

Together with the induction hypothesis [HC3], we thus have the desired result.

□

B.3 Proofs for Similarity

Lemma 6 (Refinement implies similarity)**.** *For all unambiguous contracts C_1 and C_2 such that $\bot \notin C_1$, if $C_1 \leq C_2$, then $C_1 \sim C_2$.*

Proof. Let $C_1 = (\mathcal{Q}_1, \mathcal{A}_1, \rightarrow_1, \sigma_1, s_0)$ and $C_2 = (\mathcal{Q}_2, \mathcal{A}_2, \rightarrow_2, \sigma_2, t_0)$. To show $s_0 \leq t_0$ implies $s_0 \sim t_0$, we prove the general case, for all states $s \in \mathcal{Q}_1$ and $t \in \mathcal{Q}_2$, if $s \leq t$, then $s \sim t$.

Since there is no $\bot$ state in C_1 and $C_1 \leq C_2$, by Definition 5 [Refinement], there is no $\bot$ in C_2. We also know that any state is similar to the $\top$ state, so we have four cases to distinguish:

- Case $s \in \mathcal{Q}^a$ and $t \in \mathcal{Q}^a$. It is easy to check that Definition 5 (3a) implies Definition 14 (1b); Similarly, Definition 5 (3b), where t is not $\top$, implies Definition 14 (1a).
- Case $s \in \mathcal{Q}^p$ and $t \in \mathcal{Q}^p$. Since s and t are states in an unambiguous contract, by the induction hypothesis, $s' \leq t' \implies s' \sim t' \implies s' = t'$, which means that the refinement relation between s' and t' is a bijection. It follows that the δ in the Definition 5 (4) is $\delta(s')(t') = 1$ for $s' \leq t'$. Suppose $s \xrightarrow{P_1} s'$ and $t \xrightarrow{P_2} t'$ where $s' \leq t'$. To satisfy the Definition 5 (4), we must have $P_1 \subseteq P_2$, which indeed implies $P_1 \cap P_2 \neq \emptyset$, which satisfies Definition 14 (2).

- Case $s \in \mathcal{Q}^a$ and $t \in \mathcal{Q}^p$. It is easy to check Definition 5 (5) implies Definition 14 (3).
- Case $s \in \mathcal{Q}^p$ and $t \in \mathcal{Q}^a$. It is easy to check Definition 5 (6) implies Definition 14 (4)

□

Lemma 7 (Commutativity of $\sim$)**.** *For all contracts C_1, C_2, $C_1 \sim C_2$ iff $C_2 \sim C_1$.*

Proof. By inspecting Definition 14, we see that the conditions for s and t to be similar are symmetrically defined. Thus, for all states s, t, $s \sim t$ iff $t \sim s$. If states s_0 and t_0 are initial states of C_1 and C_2 respectively, we then have $s_0 \sim t_0$ iff $t_0 \sim s_0$. Thus, $C_1 \sim C_2$ iff $C_2 \sim C_1$. □

Lemma 8 (Monotonicity of similarity over the same alphabets)**.** *For all unambiguous contracts C_1, C_2, and C_3 over the same alphabet, such that $C_1 \leq C_2$, if $C_1 \sim C_3$, then $C_2 \sim C_3$.*

Proof. By logic $A \Rightarrow B \iff \neg B \Rightarrow \neg A$, we prove $C_2 \not\sim C_3 \Rightarrow C_1 \not\sim C3$. If $C_2 \not\sim C_3$, the initial states of C_2 and C_3 are not similar. Since $C_1 \leq C_2$, by Definition 5, the initial states of C_1 and C_3 are not similar either. Thus, $C_1 \not\sim C_3$ and we are done.

□

Remark: We do not have *transitivity of similarity*. That is, the following statement *does not hold*: *for all contracts C_1, C_2, and C_3, if $C_1 \sim C_2$ and $C_2 \sim C_3$, then $C_1 \sim C_2$*. Here is a counter example:

$$(a) s_0 \overset{[0,0.3]}{\dashrightarrow} s_1 \xrightarrow{a} s_1 \qquad (b) t_0 \overset{[0,1]}{\dashrightarrow} t_1 \xrightarrow{a} t_1 \qquad (c) u_0 \overset{[0.5,1]}{\dashrightarrow} u_1 \xrightarrow{a} u_1$$

Here, $s_0 \sim t_0$ and $t_0 \sim u_0$, but $s_0 \not\sim u_0$.

B.4 Completeness of conjunction

Lemma 9 (Commutativity of $\wedge$)**.** *For all contracts C_1 and C_2, $C_1 \wedge C_2 = C_2 \wedge C_1$.*

Proof. It is obvious because the rules for conjunction are symmetric. □

Lemma 10 (Idempotency of $\wedge$)**.** *For any contract C, $C \wedge C \equiv C$.*

Proof. For any contract C, C is similar to itself. As C and C share the same alphabet and the same structure and we want to establish that the initial state of C refines itself, only conjunction rules [C1] and [C3] in Figure 12 can be applied. Examining [C1], the resulting transition $(q_1, q_1) \xrightarrow{\alpha} (q_1, q_1)$ has the same action transition as $q_1 \xrightarrow{\alpha} q_1$ for all q_1. Examining [C3], since $P_1 \cap P_1 = P_1$, the resulting transition $(q_1, q_1) \overset{P_1}{\dashrightarrow} (q_1, q_1)$ has the same probabilistic transition as $q_1 \overset{P_1 \cap P_1}{\dashrightarrow} q_1$ for all q_1. So we have idempotency. □

Lemma 11 (Congruence of refinement for $\wedge$ over the same alphabets)**.** *For all delimited unambiguous contracts C_1, C_2, C_3, if $C_1 \leq C_2$, then $C_1 \wedge C_3 \leq C_2 \wedge C_3$.*

Proof. Note that, if $C_1 \not\sim C_3$, then $C_1 \wedge C_3$ is $C_\perp$ (recall that $C_\perp$ has been defined in Definition 3). Since $\perp$ refines any state, we have $C_1 \wedge C_3 \leq C_2 \wedge C_3$. So we only have to consider the case where $C_1 \sim C_3$. By Lemma 8 (Monotonicity of similarity), we know $C_2 \sim C_3$. Let

$$\begin{array}{rcl} C_1 & = & (\mathcal{Q}_1, \mathcal{A}, \rightarrow_1, \sigma_1, s_0) \\ C_2 & = & (\mathcal{Q}_2, \mathcal{A}, \rightarrow_2, \sigma_2, t_0) \\ C_3 & = & (\mathcal{Q}_3, \mathcal{A}, \rightarrow_3, \sigma_3, u_0) \\ C_1 \wedge C_3 & = & (\mathcal{Q}_{13}, \mathcal{A}, \rightarrow_{13}, \sigma_{13}, (s_0, u_0)) \\ C_2 \wedge C_3 & = & (\mathcal{Q}_{23}, \mathcal{A}, \rightarrow_{23}, \sigma_{23}, (t_0, u_0)) \end{array}$$

Notation: for all interval σ, let $\underline{\sigma}$ and $\overline{\sigma}$ denote respectively the lower bound and the upper bound of σ.

Let $\theta \subseteq \mathcal{Q}_1 \times \mathcal{Q}_2$ be the refinement relation such that $(s,t) \in \theta$ iff $s \leq t$. Let $\theta' \subseteq \mathcal{Q}_{13} \times \mathcal{Q}_{23}$ be a binary relation such that $((s,u),(t,u)) \in \theta'$ iff $(s,t) \in \theta$, $s \sim u$ and $t \sim u$. We now prove that θ' allows us to establish that $(s,u) \leq (t,u)$.

First, we consider the 3 cases involving the state $\top_i$.

(a) Case $s = \top_1$. Since $s \leq t$, by Definition 5 ($\leq$) (1), $t = \top_2$. By Definition 16 (Conjunction), the conjunction of C_1 and C_3 is in the state $\top$ and the conjunction of C_2 and C_3 is also in the state $\top$. Since $\top \leq \top$, we have the desired result.

(b) Case $t = \top_2$. By Definition 16 (Conjunction), the state (t,u) in the conjunction is replaced by $\top$. Since any state refines $\top$, we have the desired result.

(c) Case $u = \top_3$. By Definition 16 (Conjunction), the conjunction of C_1 and C_3 is in the state $\top$ and the conjunction of C_2 and C_3 is also in the state $\top$. Since $\top \leq \top$, we have the desired result.

Second, we consider the 3 cases involving the state $\perp_i$:

(a) Case $s = \perp_1$. By Definition 16 (Conjunction), the state (s,u) in the conjunction is replaced by $\perp$. Since $\perp$ refines any state, we have the desired result.

(b) Case $t = \perp_2$. Since $s \leq t$, by Definition 5 ($\leq$) (2), s is $\perp_1$. By Definition 16 (Conjunction), the conjunction of C_1 and C_3 is in the state $\perp$ and the conjunction of C_2 and C_3 is also in the state $\perp$. Since $\perp \leq \perp$, we have the desired result.

(c) Case $u = \perp_3$. By Definition 16 (Conjunction), the conjunction of C_1 and C_3 is in the state $\perp$ and the conjunction of C_2 and C_3 is also in the state $\perp$. the state of conjunction for both sides is $\perp$. Since $\perp \leq \perp$, we have the desired result.

Now, we consider cases where states s, t, u are neither $\top_i$ nor $\perp_i$. We have the following co-induction hypothesis: for all s', t', u' such that s', t', u' are the next states of s, t, u respectively, and $((s',u'),(t',u')) \in \theta'$,

$$s' \leq t' \Rightarrow (s',u') \leq (t',u') \quad \text{[H]}$$

Given $((s,u),(t,u)) \in \theta'$, we have the following cases to consider.

- Case $s \in \mathcal{Q}_1^a, t \in \mathcal{Q}_2^a, u \in \mathcal{Q}_3^a$. Since $s \leq t$, we have (1) $s \xrightarrow{\alpha}_1 s'$; (2) $t \xrightarrow{\alpha}_2 t'$; (3) $u \xrightarrow{\alpha}_3 u'$; (4) $s' \leq t'$. From (1) and (3), by rule [C1], we have (5) $(s,u) \xrightarrow{\alpha}_{13} (s',u')$. From (2) and (3), by rule [C1], we have (6) $(t,u) \xrightarrow{\alpha}_{23} (t',u')$. From (4), by the co-induction hypothesis [H], we have (7) $(s',u') \leq (t',u')$. The conditions (5), (6) and (7) meet Definition 5 ($\leq$) (3).

- Case $s \in \mathcal{Q}_1^a, t \in \mathcal{Q}_2^a, u \in \mathcal{Q}_3^p$. We have (1) $u \overset{P_3}{\dashrightarrow}_3 u'$. Since $C_1 \sim C_3$, (2) $u' \sim s$. From $s \in \mathcal{Q}_1^a$, (1) and (2), by rule [C4R], we have (3) $(s,u) \overset{P_3}{\dashrightarrow}_{13} (s,u')$. (Note that, since u' is a state in an unambiguous contract (Definition 15), it is impossible to have more than one u' such that $s \sim u'$.) Since $C_2 \sim C_3$, we have (4) $t \sim u'$. From (1), $t \in \mathcal{Q}_2^a$ and (4), by rule [C4R], we have (5) $(t,u) \overset{P_3}{\dashrightarrow}_{13} (t,u')$. As $s \leq t$, by the co-induction hypothesis [H], we have (6) $(s,u') \leq (t,u')$. From (3) and (5), we can find a probability distribution $\delta' \subset \mathcal{Q}_{13} \times \mathcal{Q}_{23} \times [0,1]$, such that Definition 5 ($\leq$) (4) holds, that is: $\delta(s,u')(t,u') = 1$. Thus, $(s,u) \leq (t,u)$.

- Case $s \in \mathcal{Q}_1^a, t \in \mathcal{Q}_2^p, u \in \mathcal{Q}_3^a$. Given $s \leq t$, by Definition 5 ($\leq$) (5), $\exists t^a \in \mathcal{Q}_2^a : t \overset{>0}{\dashrightarrow}_2^+ t^a \wedge s \leq t^a$ and $\forall t' \in \mathcal{Q}_2$, $\left(t \overset{>0}{\dashrightarrow}_2 t' \implies s \leq t'\right)$. From $s \leq t^a$ and $s \leq t'$, by the co-induction hypothesis [H], we have (1) $(s,u) \leq (t^a,u)$ and (2) $(s,u) \leq (t',u)$ respectively. By applying rule [C4R] multiple times, we have (3) $(t,u) \overset{>0}{\dashrightarrow}_{23}^+ (t^a,u)$. From (3), (1) and (2), by Definition 5 ($\leq$) (5), we have $(s,u) \leq (t,u)$.

- Case $s \in \mathcal{Q}_1^a, t \in \mathcal{Q}_2^p, u \in \mathcal{Q}_3^p$. We have (1) $t \overset{P_2}{\dashrightarrow}_2 t'$ and (2) $u \overset{P_3}{\dashrightarrow}_3 u'$. Since $C_1 \sim C_3$, we have (3) $s \sim u'$. Since $C_2 \sim C_3$, we have (4) $P_2 \cap P_3 \neq \emptyset$ and $t' \sim u'$. From $s \in \mathcal{Q}_1^a$, (2) and (3), by rule [C4R], we have $(s,u) \overset{P_3}{\dashrightarrow}_{13} (s,u')$. From (1), (3) and (4), by rule [C3], we have $(t,u) \overset{P_2 \cap P_3}{\dashrightarrow}_{23} (t',u')$. Since $s \leq t$, by Definition 5 ($\leq$) (5) we have (5) $s \leq t'$. Note that, $s \leq t' \implies s \sim t'$. Now, since t' is a state in an unambiguous contract, it is impossible to have more than one t' such that $s \sim t'$. So the t' is unique. From (5), by the co-induction hypothesis [H], we have $(s,u') \leq (t',u')$. As C_2 is *delimited* (Definition 4) and *unambiguous* (Definition 15) and $C_1 \leq C_2$, there is only one t' from t. As C_3 is also delimited and unambiguous and $C_2 \sim C_3$, there is only one u' from u. That is, $P_2 = P_3 = [0,1]$. So $P3 \subseteq P2 \cap P3$. We can find a probability distribution $\delta' \subset \mathcal{Q}_{13} \times \mathcal{Q}_{23} \times [0,1]$, such that Definition 5 ($\leq$) (4) holds, that is: $\delta(s,u')(t',u') = 1$. Thus, $(s,u) \leq (t,u)$.

- Case $s \in \mathcal{Q}_1^p, t \in \mathcal{Q}_2^a, u \in \mathcal{Q}_3^a$. Similar reasoning as in Case $s \in \mathcal{Q}_1^a, t \in \mathcal{Q}_2^p, u \in \mathcal{Q}_3^a$.

- Case $s \in \mathcal{Q}_1^p, t \in \mathcal{Q}_2^a, u \in \mathcal{Q}_3^p$. Similar reasoning as in Case $s \in \mathcal{Q}_1^a, t \in \mathcal{Q}_2^p, u \in \mathcal{Q}_3^p$.

- Case $s \in \mathcal{Q}_1^p, t \in \mathcal{Q}_2^p, u \in \mathcal{Q}_3^a$. Similar reasoning as in Case $s \in \mathcal{Q}_1^a, t \in \mathcal{Q}_2^a, u \in \mathcal{Q}_3^p$, but with a probability distribution $\delta' \subset \mathcal{Q}_{13} \times \mathcal{Q}_{23} \times [0,1]$, such that Definition 5 ($\leq$) (4) holds, that is: $\delta'(s',u)(t',u) = \delta(s')(t')$.

- Case $s \in \mathcal{Q}_1^p, t \in \mathcal{Q}_2^p, u \in \mathcal{Q}_3^p$. We have (1) $s \overset{P_1}{\dashrightarrow}_1 s'$, (2) $t \overset{P_2}{\dashrightarrow}_2 t'$, (3) $u \overset{P_3}{\dashrightarrow}_3 u'$. Since $C_1 \sim C_3$, (4) $s' \sim u'$. Since $C_2 \sim C_3$, (5) $t' \sim u'$. From (1), (3) and (4), by rule [C3], we have (6) $(s,u) \overset{P_1 \cap P_3}{\dashrightarrow}_{13} (s',u')$. From (2), (3) and (4), by rule [C3], we have (7) $(t,u) \overset{P_2 \cap P_3}{\dashrightarrow}_{23} (t',u')$. We know:

$$
\begin{aligned}
(\dagger_1)\ \sigma_{13}(s,u)(s',u') &= [\underline{\sigma_{13}}(s,u)(s',u'), \overline{\sigma_{13}}(s,u)(s',u')] \\
&= [max(\underline{\sigma_1}(s,s'), \underline{\sigma_3}(u,u')), min(\overline{\sigma_1}(s,s'), \overline{\sigma_3}(u,u'))]
\end{aligned}
$$

$$
\begin{aligned}
(\dagger_2)\ \sigma_{23}(t,u)(t',u') &= [\underline{\sigma_{23}}(t,u)(t',u'), \overline{\sigma_{23}}(t,u)(t',u')] \\
&= [max(\underline{\sigma_2}(t,t'), \underline{\sigma_3}(u,u')), min(\overline{\sigma_2}(t,t'), \overline{\sigma_3}(u,u'))]
\end{aligned}
$$

By Definition 5 (4), we also know that there is a probability distribution $\delta \subset \mathcal{Q}_1 \times \mathcal{Q}_2 \times [0,1]$, such that, $\forall f(s') \in \sigma_1(s)(s'), t' \in \mathcal{Q}_2$,

$$
\sum_{s' \in \mathcal{Q}_1} (f(s') * \delta(s')(t')) \in \sigma_2(t)(t') \text{ and } \forall s' \in \mathcal{Q}_1, \delta(s')(t') > 0 \Rightarrow s' \leq t'
$$

Moreover, we have:

$$
\begin{aligned}
(\dagger_3) \quad & \sum_{s' \in \mathcal{Q}_1} (f(s') * \delta(s')(t')) \in \sigma_2(t)(t') \\
\Longleftrightarrow \quad & \sum_{s' \in \mathcal{Q}_1} ([\underline{\sigma_1}(s)(s'), \overline{\sigma_1}(s)(s')] * \delta(s')(t')) \subseteq \sigma_2(t)(t') \\
\Longleftrightarrow \quad & \sum_{s' \in \mathcal{Q}_1} [\underline{\sigma_1}(s)(s') * \delta(s')(t'), \overline{\sigma_1}(s)(s') * \delta(s')(t')] \subseteq [\underline{\sigma_2}(t)(t'), \overline{\sigma_2}(t)(t')]
\end{aligned}
$$

We want to show that there is a probability distribution $\delta' \subset \mathcal{Q}_{13} \times \mathcal{Q}_{23} \times [0,1]$, such that Definition 5 (4) holds for all $f'(s',u') \in \sigma_{13}(s,u)(s',u')$ and all $(t',u') \in \mathcal{Q}_{23}$. Let $|s'|$ be the number of outgoing states from s where $\delta(s')(t') > 0$. Let $\delta'(s',u')(t',u') = \delta(s')(t') * |s'|$.

(By $(\dagger_3)$)
$\sum_{s' \in \mathcal{Q}_1} [\underline{\sigma_1}(s)(s') * \delta(s')(t'), \overline{\sigma_1}(s)(s') * \delta(s')(t')] \subseteq [\underline{\sigma_2}(t)(t'), \overline{\sigma_2}(t)(t')]$

$\iff$ (By set theory, if $[a,b],[c,d],[e,f] \subseteq [0,1]$, then
$[a,b] \subseteq [c,d] \iff [\max(a,e), \min(b,f)] \subseteq [\max(c,e), \min(d,f)]$.
By distributivity of $*$ over max and min.
We also know that $\sigma_3(u)(u') \subseteq [0,1]$)

$$\forall u' \in \mathcal{Q}_3, \sum_{s' \in \mathcal{Q}_1} [\max(\underline{\sigma_1}(s)(s'), \underline{\sigma_3}(u)(u')) * \delta(s')(t'), \min(\overline{\sigma_1}(s)(s'), \overline{\sigma_3}(u)(u')) * \delta(s')(t')] \subseteq [\max(\underline{\sigma_2}(t)(t'), \underline{\sigma_3}(u)(u')), \min(\overline{\sigma_2}(t)(t'), \overline{\sigma_3}(u)(u'))]$$

$\iff$ (By definition of $\sum$, we can apply $\sum_{u' \in \mathcal{Q}_3}$ to both sides of $\subseteq$)

$$\sum_{u' \in \mathcal{Q}_3} \sum_{s' \in \mathcal{Q}_1} [\max(\underline{\sigma_1}(s,s'), \underline{\sigma_3}(u)(u')) * \delta(s')(t'), \min(\overline{\sigma_1}(s)(s'), \overline{\sigma_3}(u)(u')) * \delta(s')(t')] \subseteq \sum_{u' \in \mathcal{Q}_3} [\max(\underline{\sigma_2}(t)(t'), \underline{\sigma_3}(u)(u')), \min(\overline{\sigma_2}(t)(t'), \overline{\sigma_3}(u)(u'))]$$

$\iff$ (By definition of $\sum$)

$$\sum_{(s',u') \in \mathcal{Q}_{13}} [\max(\underline{\sigma_1}(s)(s'), \underline{\sigma_3}(u)(u')) * \delta(s')(t'), \min(\overline{\sigma_1}(s)(s'), \overline{\sigma_3}(u)(u')) * \delta(s')(t')] \subseteq [\max(\underline{\sigma_2}(t)(t'), \underline{\sigma_3}(u)(u')) * (1/|s'|), \min(\overline{\sigma_2}(t)(t'), \overline{\sigma_3}(u)(u')) * (1/|s'|)]$$

$\iff$ (By multiplying both sides of $\subset$ by $|s'|$)

$$\sum_{(s',u') \in \mathcal{Q}_{13}} [\max(\underline{\sigma_1}(s)(s'), \underline{\sigma_3}(u)(u')) * \delta(s')(t') * |s'|, \min(\overline{\sigma_1}(s)(s'), \overline{\sigma_3}(u)(u')) * \delta(s')(t') * |s'|] \subseteq [\underline{\sigma_2}(t)(t') * \underline{\sigma_3}(u)(u'), \overline{\sigma_2}(t)(t') * \overline{\sigma_3}(u)(u')]$$

$\iff$ (By factorization, extract $(\delta(s')(t') * |s'|)$)

$$\sum_{(s',u') \in \mathcal{Q}_{13}} [\max(\underline{\sigma_1}(s)(s'), \underline{\sigma_3}(u)(u')), \min(\overline{\sigma_1}(s)(s'), \overline{\sigma_3}(u)(u'))] * \delta(s')(t') * |s'| \subseteq [\max(\underline{\sigma_2}(t)(t'), \underline{\sigma_3}(u)(u')), \min(\overline{\sigma_2}(t)(t'), \overline{\sigma_3}(u)(u'))]$$

$\iff$ (By definition of δ')

$$\sum_{(s',u') \in \mathcal{Q}_{13}} [\max(\underline{\sigma_1}(s)(s'), \underline{\sigma_3}(u)(u')), \min(\overline{\sigma_1}(s)(s'), \overline{\sigma_3}(u)(u'))] * \delta'(s',u')(t',u') \subseteq [\max(\underline{\sigma_2}(t)(t'), \underline{\sigma_3}(u)(u')), \min(\overline{\sigma_2}(t)(t'), \overline{\sigma_3}(u)(u'))]$$

$\iff$ (By $(\dagger_2)$)

$$\sum_{(s',u') \in \mathcal{Q}_{13}} ([\max(\underline{\sigma_1}(s)(s'), \underline{\sigma_3}(u)(u')), \min(\overline{\sigma_1}(s)(s'), \overline{\sigma_3}(u)(u'))] * \delta'(s',u')(t',u')) \subseteq \sigma_{23}(t,u)(t',u')$$

$\iff$ (By $(\dagger_1)$)

$$\sum_{(s',u') \in \mathcal{Q}_{13}} (\delta_{13}(s,u)(s',u') * \delta'(s',u')(t',u')) \subseteq \sigma_{23}(t,u)(t',u')$$

$\iff$ (By definition of f')

$$\sum_{(s',u') \in \mathcal{Q}_{13}} (f'(s',u') * \delta'(s',u')(t',u')) \in \sigma_{23}(t,u)(t',u')$$

□

Theorem 8 (Congruence of refinement for $\wedge$) For all delimited unambiguous contracts C_1, C_2, C_3, and C_4 over the same alphabet, if $C_1 \leq C_2$ and $C_3 \leq C_4$,

then $C_1 \wedge C_3 \leq C_2 \wedge C_4$.

Proof.

$C_1 \leq C_2$ and $C_3 \leq C_4$
$\Rightarrow$ (By Lemma 11 (Congruence of refinement for $\wedge$) twice)
$C_1 \wedge C_3 \leq C_2 \wedge C_3$ and $C_3 \wedge C_2 \leq C_4 \wedge C_2$
$\Rightarrow$ (By Lemma 9 (Commutativity of $\wedge$))
$C_1 \wedge C_3 \leq C_3 \wedge C_2$ and $C_3 \wedge C_2 \leq C_4 \wedge C_2$
$\Rightarrow$ (By Lemma 2 (Transitivity of $\leq$))
$C_1 \wedge C_3 \leq C_4 \wedge C_2$
$\Rightarrow$ (By Lemma 9 (Commutativity of $\wedge$))
$C_1 \wedge C_3 \leq C_2 \wedge C_4$

□

Theorem 7 (Completeness of conjunction over the same alphabet) For all delimited unambiguous contracts C_1, C_2, C_3, if $C_1 \leq C_2$ and $C_1 \leq C_3$, then $C_1 \leq C_2 \wedge C_3$.

Proof.

$C \leq C_1$ and $C \leq C_2$
$\Rightarrow$ (By Theorem 8 (Congruence of refinement for $\wedge$))
$C \wedge C \leq C_1 \wedge C_2$
$\Rightarrow$ (By Lemma 10 (Idempotence of conjunction))
$C \leq C_1 \wedge C_2$

□

Corollary 2. *For all IMC M and delimited unambiguous contracts C_1 and C_2, if $M \models C_i, i = 1, 2$ then $M \models C_1 \wedge C_2$.*

We do not have completeness for conjunction if two contracts have different alphabets; that is, the following statement *does not hold*:

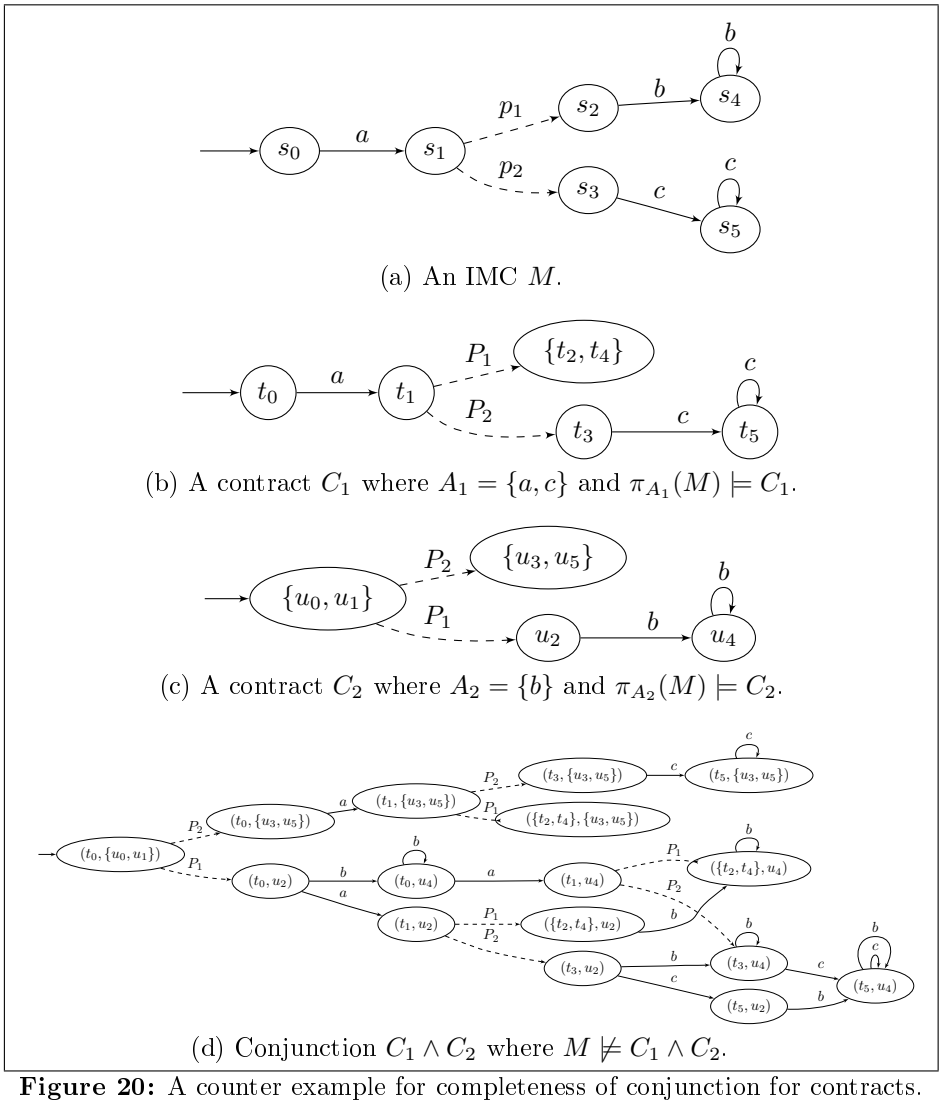
For all IMC M and contracts $C_1 = (\mathcal{Q}_1, \mathcal{A}_1, \rightarrow_1, \sigma_1, s_0)$ and $C_2 = (\mathcal{Q}_2, \mathcal{A}_2, \rightarrow_2, \sigma_2, t_0)$, if $\pi_{\mathcal{A}_i}(M) \models C_i, i = 1, 2$ then $M \models C_1 \wedge C_2$.

A counter-example is shown in Figure 20, where $A_1 = \{a, c\}$, $A_2 = \{b\}$, and $P_i = [p_i, p_i]$ for $i = 1, 2, 3, 4$. For the ease of checking $\pi_{\mathcal{A}_i}(M) \models C_i$, we simply let the C_i be $\lfloor \pi_{\mathcal{A}_i}(M) \rfloor$ and rename the labelling of the states accordingly. Intuitively, it is impossible for M to produce a sequence ba. Specifically, $s_1 \not\leq (t_0, u_2)$, so $s_0 \not\leq (t_0, \{u_0, u_1\})$ and $M \not\models C_1 \wedge C_2$.

B.5 Associativity of Conjunction

Before proving Theorem 5, let us show that we do not have associativity of conjunction if two contracts have *different* alphabets. That is, the following statement *does not hold*:

For all unambiguous contracts $C_1, C_2,$ and $C_3, (C_1 \wedge C_2) \wedge C_3 \equiv C_1 \wedge (C_2 \wedge C_3)$.



(a) An IMC M.

(b) A contract C_1 where $A_1 = \{a, c\}$ and $\pi_{A_1}(M) \models C_1$.

(c) A contract C_2 where $A_2 = \{b\}$ and $\pi_{A_2}(M) \models C_2$.

(d) Conjunction $C_1 \wedge C_2$ where $M \not\models C_1 \wedge C_2$.

Figure 20: A counter example for completeness of conjunction for contracts.

Figure 21 shows a counter example. In Figure 21 (e), there is no transition from state $((\top_1, t_0), u_0)$ because the action transition c from state $(\top_1, t_0)$ in $C_1 \wedge C_2$ is in the set of actions of C_3 (i.e., we cannot apply the conjunction rule [LIFTL]). However, in its corresponding state $(\top_1, (t_0, u_0))$ in Figure 21 (g), we can have transitions that follow the contract $C_2 \wedge C_3$ due to the conjunction rule [C2R].

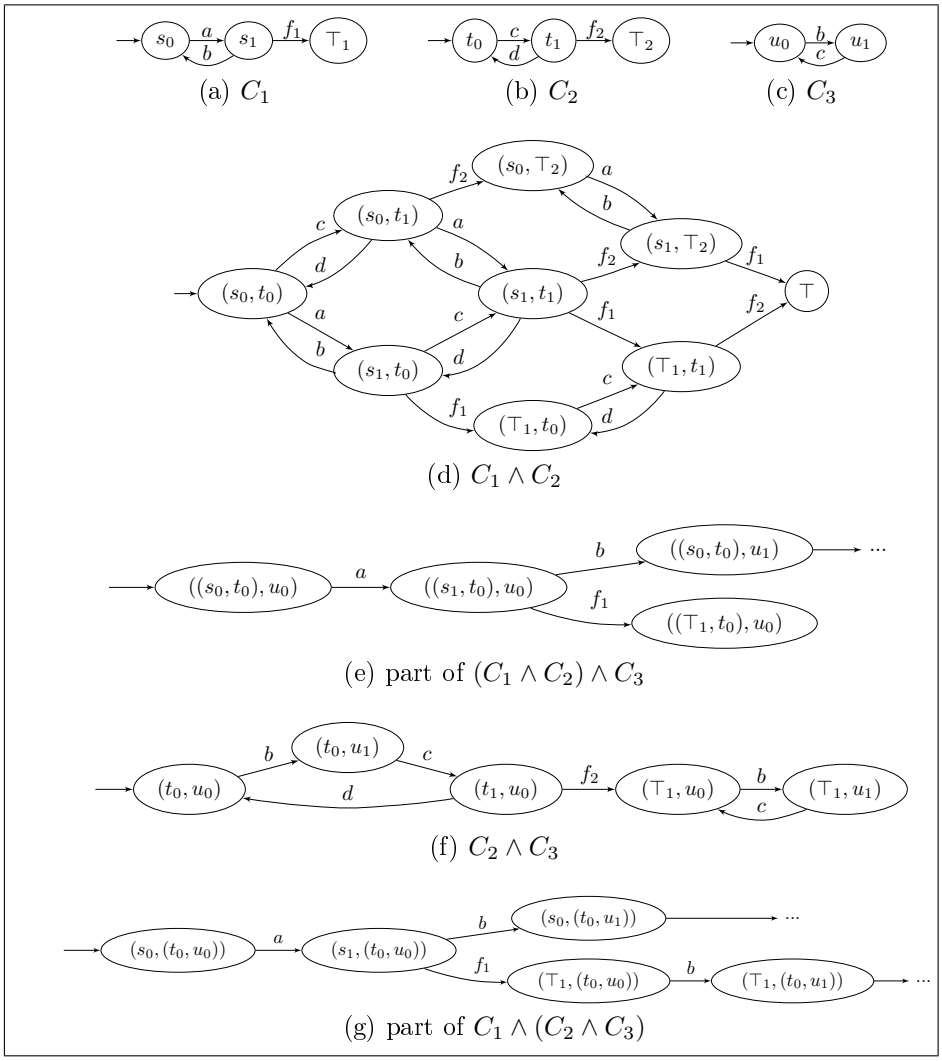


Figure 21: Counter example for associativity of conjunction

Definition 17 (Equality of contracts)**.** *For all contracts* $C_1 = (\mathcal{Q}_1, \mathcal{A}, \rightarrow_1, \sigma_1, s_0)$ *and* $C_2 = (\mathcal{Q}_2, \mathcal{A}, \rightarrow_2, \sigma_2, t_0)$*,* C_1 *is equal to* C_2 *(written* $C_1 = C_2$*) iff there exists a bijection* $\rho : \mathcal{Q}_1 \rightarrow \mathcal{Q}_2$ *such that* $t_0 = \rho(s_0)$ *and for all* $s, s' \in \mathcal{Q}_1$*, we have:* $s \xrightarrow{a} s' \iff \rho(s) \xrightarrow{a} \rho(s')$*, and* $s \overset{P}{\dashrightarrow} s' \iff \rho(s) \overset{P}{\dashrightarrow} \rho(s')$*.*

Theorem 5 [Associativity of conjunction over the same alphabet] For all unambiguous contracts $C_1 = (\mathcal{Q}_1, \mathcal{A}, \rightarrow_1, \sigma_1, s_0)$, $C_2 = (\mathcal{Q}_2, \mathcal{A}, \rightarrow_2, \sigma_2, t_0)$, and $C_3 = (\mathcal{Q}_3, \mathcal{A}, \rightarrow_3, \sigma_3, u_0)$, $(C_1 \wedge C_2) \wedge C_3 = C_1 \wedge (C_2 \wedge C_3)$.

Proof. Let

$$\begin{array}{rcl} C_1 & = & (\mathcal{Q}_1, \mathcal{A}, \rightarrow_1, \sigma_1, s_0) \\ C_2 & = & (\mathcal{Q}_2, \mathcal{A}, \rightarrow_2, \sigma_2, t_0) \\ C_3 & = & (\mathcal{Q}_3, \mathcal{A}, \rightarrow_3, \sigma_3, u_0) \\ C_1 \wedge C_2 & = & (\mathcal{Q}_{12}, \mathcal{A}, \rightarrow_{12}, \sigma_{12}, (s_0, t_0)) \\ C_2 \wedge C_3 & = & (\mathcal{Q}_{23}, \mathcal{A}, \rightarrow_{23}, \sigma_{23}, (t_0, u_0)) \\ (C_1 \wedge C_2) \wedge C_3 & = & (\mathcal{Q}_{12.3}, \mathcal{A}, \rightarrow_{12.3}, \sigma_{12.3}, ((s_0, t_0), u_0)) \\ C_1 \wedge (C_2 \wedge C_3) & = & (\mathcal{Q}_{1.23}, \mathcal{A}, \rightarrow_{1.23}, \sigma_{1.23}, (s_0, (t_0, u_0))) \end{array}$$

Let ρ be the state mapping from $\mathcal{Q}_{12.3}$ to $\mathcal{Q}_{1.23}$ such that $\rho(\bot_{12.3}) = \bot_{1.23}$, $\rho(\top_{12.3}) = \top_{1.23}$, and for all $((s,t),u) \in \mathcal{Q}_{12.3}$ such that $s \sim t \sim u$, we have $\rho(((s,t),u)) = (s,(t,u))$. We must show the following property:

$$\forall q, q' \in \mathcal{Q}_{12.3},\ q \xrightarrow{a} q' \iff \rho(q) \xrightarrow{a} \rho(q') \text{ and } q \overset{P}{\dashrightarrow} q' \iff \rho(q) \overset{P}{\dashrightarrow} \rho(q') \quad [\mathrm{P}]$$

If $q = \bot_{12.3}$ or $q = \top_{12.3}$, then the property [P] is trivially satisfied. Otherwise, q is of the form $((s,t),u)$ with $s \sim t \sim u$, and we have the following cases:

(1) Case where $q' = \bot$. We thus have the following (not necessarily exclusive) subcases:

(1a) $s \rightarrow \bot_1$. According to Rule 2 of Definition 16, we have $(s,t) \rightarrow \bot_{12}$. Hence $((s,t),u) \rightarrow \bot_{12.3}$. Similarly, whatever the transition from (t,u) in C_{23}, we have $(s,(t,u)) \rightarrow \bot_{1.23}$. Since $\rho(\bot_{12.3}) = \bot_{1.23}$, the states q and q' satisfy [P].

(1b) The subcases $t \rightarrow \bot_1$ and/or $u \rightarrow \bot_1$ are analogous to (1a).

(1c) The three states are action states with $s \rightarrow s'$, $t \rightarrow t'$, and $u \rightarrow u'$, and are such that $s' \not\sim t'$. Firstly, according to Rule 2 of Definition 16, we have $(s,t) \rightarrow \bot_{12}$. Hence $((s,t),u) \rightarrow \bot_{12.3}$. Secondly, either $t' \sim u'$ or $t' \not\sim u'$. The first case implies that $(t,u) \rightarrow (t',u')$. It follows that $s' \not\sim (t',u')$. The second case implies that $(t,u) \rightarrow \bot_{23}$. So in both cases, $(s,(t,u)) \rightarrow \bot_{1.23}$. Since $\rho(\bot_{12.3}) = \bot_{1.23}$, the states q and q' satisfy [P].

(1d) The subcases where some states are probabilistic states and/or another pair of destination states is not similar are analogous to (1c).

(2) Case where one or two states among s, t, and u is equal to $\top_i$. We have the following subcases:

(2a) $s = \top_1$, $t \xrightarrow{\beta} t'$, and $u \xrightarrow{\gamma} u'$. Firstly, since $t \sim u$, we necessarily have $\beta = \gamma$. Thus, according to Rule [C1], $(t,u) \xrightarrow{\beta} (t',u')$. Secondly, according to Rule [C2R], $(s,t) \xrightarrow{\beta} (\top_1, t')$ and $(s,(t,u)) \xrightarrow{\beta} (\top_1, (t',u'))$. Thirdly, according to Rule [C1], $((s,t),u) \xrightarrow{\beta} ((\top_1,t'),u')$. In other words, $\rho(((\top_1,t),u)) \xrightarrow{\beta} \rho(((\top_1,t'),u'))$ and the states q and q' satisfy [P].

(2b) The other subcases, including with probabilistic transitions, are analogous to (2a).

(3) Case where $q' = ((s',t'),u')$ with $s' \sim t' \sim u'$. We have the following subcases:

(3a) The three states are action states with $s \xrightarrow{\alpha} s'$, $t \xrightarrow{\beta} t'$, and $u \xrightarrow{\gamma} u'$. Firstly, since $s \sim t \sim u$, we necessarily have $\alpha = \beta = \gamma$. Thus, according to Rule [C1], $(s,t) \xrightarrow{\alpha} (s',t')$ and $(t,u) \xrightarrow{\alpha} (t',u')$. Secondly, applying again Rule [C1] gives $((s,t),u) \xrightarrow{\alpha} ((s',t'),u')$ and $(s,(t,u)) \xrightarrow{\alpha} (s',(t',u'))$. In other words, $\rho(((s,t),u)) \xrightarrow{\alpha} \rho(((s',t'),u'))$ and the states q and q' satisfy [P].

(3b) The other cases with probabilistic transitions are analogous to (3a).

□

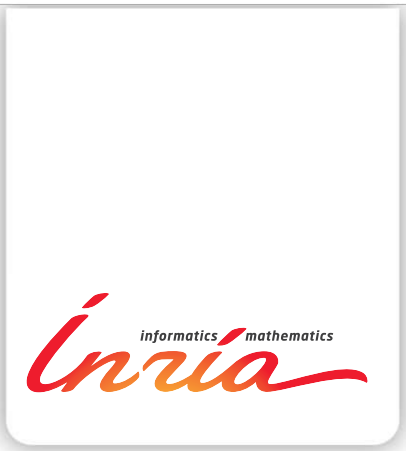
Theorem 9 (Distributivity of $\|$ over $\wedge$)**.** *Let C_i be an unambiguous contract over alphabet $\mathcal{A}_i$, $i = 1,2,3$, such that $(\mathcal{A}_1 \cup \mathcal{A}_2) \cap \mathcal{A}_3 = \emptyset$, and let $\mathcal{I} \subseteq \mathcal{A}_1 \cup \mathcal{A}_2 \cup \mathcal{A}_3 \cup (\mathcal{A}_1 \bowtie \mathcal{A}_2)$, where $S_1 \bowtie S_2 = \{a|b \mid a \in S_1 \wedge b \in S_2\}$. Then,*

$$(C_1 \wedge C_2)\|_{\mathcal{I}} C_3 \;\leq\; (C_1\|_{\mathcal{I}} C_3) \wedge (C_2\|_{\mathcal{I}} C_3)$$

Proof.

(By Theorem 6 [Conjunction is a common refinement])
$C_1 \wedge C_2 \leq C_1$ and $C_1 \wedge C_2 \leq C_2$
$\Rightarrow$ (By Lemma 5 [Congruence of refinement for $||_{\mathcal{I}}$])
$(C_1 \wedge C_2)\|_{\mathcal{I}} C_3 \leq C_1\|_{\mathcal{I}} C_3$ and $(C_1 \wedge C_2)\|_{\mathcal{I}} C_3 \leq C_2\|_{\mathcal{I}} C_3$
$\Rightarrow$ (By Theorem 8 [Congruence of refinement for $\wedge$])
$((C_1 \wedge C_2)\|_{\mathcal{I}} C_3) \wedge ((C_1 \wedge C_2)\|_{\mathcal{I}} C_3) \;\leq\; (C_1\|_{\mathcal{I}} C_3) \wedge (C_2\|_{\mathcal{I}} C_3)$
$\Longleftrightarrow$ (By Lemma 10 [Idempotence of conjunction])
$(C_1 \wedge C_2)\|_{\mathcal{I}} C_3 \;\leq\; (C_1\|_{\mathcal{I}} C_3) \wedge (C_2\|_{\mathcal{I}} C_3)$

□



RESEARCH CENTRE
GRENOBLE – RHÔNE-ALPES

Inovallée
655 avenue de l'Europe Montbonnot
38334 Saint Ismier Cedex

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

ISSN 0249-6399