Alcom-FT Technical Report Series
ALCOMFT-TR-02-138

Hiding Resources that Can Fail: An Axiomatic Perspective*

Anna Philippou[1], Oleg Sokolsky[2], Insup Lee[2],
Rance Cleaveland[3], and Scott A. Smolka[3]

[1]University of Cyprus. annap@cs.ucy.ac.cy
[2]University of Pennsylvania, USA. {sokolsky,lee}@cis.upenn.edu
[3]SUNY at Stony Brook, USA. {rance, sas}@cs.sunysb.edu

Abstract

In earlier work, we presented a process algebra, PACSR, that uses a notion of resource failure to capture probabilistic behavior in reactive systems. PACSR also supports an operator for resource hiding. In this paper, we carefully consider the interaction between these two features from an axiomatic perspective. For this purpose, we introduce a subset of PACSR, called "PACSR-lite," that allows us to isolate the semantic issues surrounding resource hiding in a probabilistic setting, and provide a sound and complete axiomatization of strong bisimulation for this fragment.

1 Introduction

The real-time process algebra ACSR [7] features a notion of *resource-dependent* actions. A process needs to have access to a set of resources specified in an action before it can proceed with the action. Recently, in the context of the process algebra PACSR [11], we extended the ACSR framework with the possibility of resource failures which happen with a given probability.

Previous work on extending process algebra with probability information, such as [4, 14, 1, 3, 5, 13], typically associates probabilities with process terms. An advantage of associating probabilities with resources, rather than process terms, is that the specification of a process does not involve probabilities directly. Failure probabilities of individual resources are defined separately and are used only during analysis. This makes specifications simpler and ensures a more systematic way of applying probabilistic information. In addition, this approach allows one to explore the impact of changing probabilities of failures on the overall behavior, without changing the specification.

In this paper, we explore the effects of resource failures in a setting where resources may be hidden from the observer (i.e., private to a process). Specifically, we present PACSR-lite, a fragment of PACSR that allows us to isolate the issues surrounding resource hiding, and present a sound and complete axiomatization of strong bisimulation equivalence for this fragment. Due to the limitation of space, proofs of some of the results are only briefly sketched. The complete proofs can be found in [12].

*Research supported in part by the Future and Emerging Technologies programme of the EU under contract number IST-1999-14186 (ALCOM-FT) and by grants AFOSR F49620-95-1-0508, ARO DAAH04-95-1-0092, NSF CCR-9988409, NSF CCR-9619910, and ONR N00014-97-1-0505 (MURI).

2 The Syntax of PACSR-lite

PACSR-lite is a subset of the probabilistic process algebra PACSR [11]. An action of a PACSR process specifies access to a (possibly empty) set of resources that the process requires to perform the action. Moreover, each resource has an associated failure probability. Resources can be *hidden*, making their identity invisible to the environment, but their failures can be observed.

Resources and actions. We assume that a system contains a finite set of serially reusable resources drawn from the infinite set Res. We write $\overline{Res}$ for the set that contains, for each $r \in Res$, an element $\overline{r}$, representing the *failed* resource r, and R for $Res \cup \overline{Res}$. An action is drawn from the domain $\boldsymbol{P}(\mathsf{R})$ with the restriction that each resource is represented at most once. For example, the singleton action $\{r\}$ denotes the use of resource r. This action cannot happen if r has failed. On the other hand, action $\{\overline{r}\}$ takes place given that resource r has failed. A notation for failed resources is useful for specifying recovery from failures. Action $\emptyset$ represents idling since no resource is consumed. We let Act denote the domain of actions and α, A, B range over Act.

For all $r \in Res$ we denote by $\mathsf{p}(r) \in [0,1]$ the probability of resource r being up, while $\mathsf{p}(\overline{r}) = 1 - \mathsf{p}(r)$ denotes the probability of r failing. For example, consider the action $\{cpu\}$, where resource cpu has probability of failure $1/3$, i.e. $\mathsf{p}(cpu) = 2/3$. Then, $\{cpu\}$ may occur with probability $2/3$ and fails with probability $1/3$. We assume the existence of an infinite number of resources for each probability failure in $[0,1]$.

Processes. The set Pr of PACSR-lite processes, ranged over by P and Q, is given by:

$$P \ ::= \ \mathrm{NIL} \mid A{:}P \mid P + P \mid P\backslash\backslash I$$

where $I \subseteq Res$. The process NIL represents the inactive process. $A{:}P$ executes a resource-consuming action and proceeds to process P. The process $P + Q$ represents a nondeterministic choice between the two summands. $P\backslash\backslash I$ hides resources in I so that they are not visible to the environment. The full process algebra, PACSR, additionally contains constructs for recursion, parallel composition, restriction, etc.

In $P\backslash\backslash I$ the displayed occurrence of each of the resources in I is *binding* with scope P. An occurrence of a resource in a process is *bound* if it lies within the scope of a binding occurrence of the resource, otherwise the occurrence is free. We write $\mathsf{fr}(P)$ for the set of resources that have a free occurrence in P and $\mathsf{br}(P)$ for the set of resources all of whose occurrences are bound. In what follows, we work up to α-conversion on bound resources. In this way, bound resources in a process are assumed to be different from each other and from the free resources.

Let $Z = \{r_1, \ldots, r_n\} \subseteq \mathsf{R}$. Then $\mathsf{p}(Z) = \Pi_{1 \le i \le n}\mathsf{p}(r_i)$; $\mathcal{W}(Z) = \{Z' \subseteq Z \cup \overline{Z} \mid r \in Z' \text{ iff } \overline{r} \notin Z'\}$; and $res(Z) = \{r \in Res \mid r \in Z \text{ or } \overline{r} \in Z\}$. Thus $\mathcal{W}(Z)$ denotes the set of all possible worlds involving resources Z, that is, the set of all combinations of the resources in Z being up or down, and $res(Z)$ the world where all resources in Z are up. For example, $\mathcal{W}(\{r_1, \overline{r_2}\}) = \{\{\overline{r_1}, \overline{r_2}\}, \{\overline{r_1}, r_2\}, \{r_1, \overline{r_2}\}, \{r_1, r_2\}\}$, $res(\{r_1, \overline{r_2}\}) = \{r_1, r_2\}$. Note that $\mathsf{p}(\emptyset) = 1$ and $\mathcal{W}(\emptyset) = \{\emptyset\}$. We also write $res(P)$ for $res(\mathsf{fr}(P) \cup \mathsf{br}(P))$. Finally, function $\mathsf{imr}(P)$, defined below, associates each process with the set of resources on which its behavior immediately depends:

$$\begin{aligned}
&\mathsf{imr}(\mathrm{NIL}) = \emptyset\\
&\mathsf{imr}(P_1 + P_2) = \mathsf{imr}(P_1) \cup \mathsf{imr}(P_2)\\
&\mathsf{imr}(A{:}P) = res(A)\\
&\mathsf{imr}(P\backslash\backslash I) = \mathsf{imr}(P)
\end{aligned}$$

3 Operational Semantics

A *configuration* is a pair of the form $(P, W) \in \mathsf{Pr} \times 2^{\mathsf{R}}$, representing a process P in world W. A world captures the state (up or down) of resources relevant to P. We write S for the set of configurations. The semantics of PACSR-lite is given in terms of a labeled transition system whose states are configurations and whose transitions are either probabilistic (labeled by a probability) or nondeterministic (labeled by an action). The idea is that, for a process P, computation begins in the *initial configuration* $(P, \emptyset)$. Probabilistic transitions are performed to determine the status of resources immediately relevant for execution (as specified by $\mathsf{imr}(P)$) but for which there is no knowledge in the configuration's world. The status of a resource does not change until an action-labeled transition occurs; moreover, actions erase all previous knowledge of the configuration's world (see law (Act)). Nondeterministic transitions are possible from configurations containing all necessary knowledge regarding the state of resources.

With this view of computation in mind, we partition S as follows:

$S_n = \{(P, W) \in \mathsf{S} \mid \mathsf{imr}(P) - \mathit{res}(W) = \emptyset\}$, the set of *nondeterministic configurations*, and

$S_p = \{(P, W) \in \mathsf{S} \mid \mathsf{imr}(P) - \mathit{res}(W) \neq \emptyset\}$, the set of *probabilistic configurations*.

The operational semantics of PACSR-lite processes is given as a combination of two labeled transition relations: $\longrightarrow_p \subset S_p \times [0,1] \times S_n$ is the probabilistic transition relation and $\longrightarrow_n \subset S_n \times \mathit{Act} \times \mathsf{S}$ is the nondeterministic transition relation. We write elements of $\longrightarrow_p$ as $(P, W) \xrightarrow{p}_p (P', W')$ and elements of $\longrightarrow_n$ as $(P, W) \xrightarrow{\alpha}_n (P', W')$.

The probabilistic transition relation is given by the rule (PROB) in Table 1. Note that configuration (P, W) evolves into $(P, W \cup Z_2)$ which is, by definition, a nondeterministic configuration. Further, it can be shown that for all $s \in S_p$, $\sum \{\!| p \mid (s, p, s') \in \longrightarrow_p |\!\} = 1$, where $\{\!|$ and $|\!\}$ are multiset brackets and the summation over the empty multiset is 1.

The nondeterministic transition relation is given by rules (Act), (Sum), and (Hide) of Table 1. The symmetric version of rule (Sum) has been omitted. Note that in rule (Act), the occurrence of an action A re-initializes the world to $\emptyset$. It can be shown that the semantics of PACSR-lite processes define alternating transition systems, that is, transition systems where nondeterministic and probabilistic states alternate [4].

To illustrate the semantics, consider process $\{r_1, \overline{r_2}\}{:}P$, which, in a world where resource r_1 is up and r_2 is down, may evolve to P. Let $\mathsf{p}(r_1) = \mathsf{p}(r_2) = 0.5$. Then, by (PROB), $(\{r_1, \overline{r_2}\}{:}P, \emptyset) \xrightarrow{0.25}_p (\{r_1, \overline{r_2}\}{:}P, W\})$, for each $W \in \mathcal{W}(\{r_1, r_2\})$, and, by (Act), $(\{r_1, \overline{r_2}\}{:}P, \{r_1, \overline{r_2}\}) \xrightarrow{\{r_1, \overline{r_2}\}}_n (P, \emptyset)$, whereas the remainder of the configurations have no transitions.

4 Strong Bisimulation

We introduce the notion of (strong) bisimulation [8, 10] for PACSR-lite processes. It captures formally the notion that equivalent systems exhibit the same behavior, including probabilistic behavior, at their interfaces with the environment. Our definition of probabilistic strong bisimulation is closely related to those studied by [6, 4].

Definition 4.1 For $s \in \mathsf{S}$ and $\mathcal{M} \subseteq \mathsf{S}$, $\mu(s, \mathcal{M}) = \sum_{s' \in \mathcal{M}} \{\!| p \mid (s, p, s') \in \longrightarrow_p |\!\}$. That is, $\mu(s, \mathcal{M})$ denotes the probability that s may perform a probabilistic transition to a configuration in $\mathcal{M}$. $\square$

Definition 4.2 An equivalence relation $\mathcal{R} \subseteq \mathsf{S} \times \mathsf{S}$ is a *strong bisimulation* if, whenever $s \mathcal{R} t$ (1) for all $\alpha \in \mathit{Act}$, if $s, t \in S_n$ and $s \xrightarrow{\alpha}_n s'$ then $t \xrightarrow{\alpha}_n t'$ and $s' \mathcal{R} t'$; (2) for all $\mathcal{M} \in \mathsf{S}/\mathcal{R}$, if $s, t \in S_p$, $\mu(s, \mathcal{M}) = \mu(t, \mathcal{M})$.

Two configurations s and t are *strong bisimulation equivalent*, written $s \sim t$, if there exists a strong bisimulation $\mathcal{R}$ such that $s \mathcal{R} t$. $\square$

Thus, two configurations are related by a strong bisimulation $\mathcal{R}$ if they can reach all equivalence classes of the relation with the same probability and they can simulate each

$$\text{(PROB)} \quad \frac{(P,W) \in S_p, Z_1 = \mathsf{imr}(P) - res(W), Z_2 \in \mathcal{W}(Z_1)}{(P,W) \xrightarrow{\mathsf{p}(Z_2)}_p (P, W \cup Z_2)}$$

$$\text{(Act)} \quad (A{:}P,W) \xrightarrow{A}_n (P,\emptyset), \text{ if } A \subseteq W \qquad \text{(Sum)} \quad \frac{(P_1,W) \xrightarrow{\alpha}_n (P,W')}{(P_1+P_2,W) \xrightarrow{\alpha}_n (P,W')}$$

$$\text{(Hide)} \quad \frac{(P,W) \xrightarrow{A}_n (P',W'),\ A' = A - I}{(P\backslash\backslash I,W) \xrightarrow{A'}_n (P'\backslash\backslash I,W')}$$

Table 1: The probabilistic and nondeterministic transition relations

other's behavior. It can be shown that $\sim$ is the largest strong bisimulation [4].

We say that two PACSR-lite processes P and Q are bisimilar, written $P \sim Q$, when their initial configurations are bisimilar; i.e., $(P,\emptyset) \sim (Q,\emptyset)$. It can be proved that $\sim$ is a congruence with respect to the PACSR-lite operators.

5 The Laws

Tables 2 and 3 contain our axiomatization of strong bisimulation for PACSR-lite, which we refer to as $\mathcal{A}$. We shall subsequently show that $\mathcal{A}$ is a sound and complete axiomatization of strong bisimulation. In the sequel, we will use the equality symbol "=" when two processes can be shown to be equivalent using $\mathcal{A}$.

Law Hide(2) describes how the hiding operator distributes over summation. In order to push a summation outside a hiding operator, we must ensure that no pair of summands share any bound resources; otherwise a resource that was shared by the two summands of the left-hand side process will become two different resources in the right-hand side. This can result in processes that exhibit different probabilistic behavior.Law Down states that a process which is only willing to engage in an action involving a failed resource is in fact a failed process, and Law Up shows that employing a bound resource that never fails is equivalent to not using the resource at all. Law Rename establishes the equivalence of processes that only differ by a change of bound resources that have the same probability of failure.

The laws of Table 3 are central for the completeness of the strong bisimulation characterization. Law Extend allows us to rewrite a summation of prefixes by enriching each summand with information about the state of a new hidden resource, thus replacing each process $A{:}P$ with the summation $(A \cup \{r\}){:}P + (A \cup \{\overline{r}\}){:}P$, assuming $r \notin res(A)$.

Laws Standard provide a standard form for a summation of processes. Each of the laws assumes that all summands of the left-hand side process have the same hidden resources, although different summands may concern different worlds of these resources. Then, it identifies the possible observable behaviors $\sum_k A_k \cup B_i : P_k$ that can arise in a single world of the hidden resources, B_i, and finally groups together the worlds B_{ij} which present the same observable behaviors, $\sum_{j=1}^{J_i} \sum_{k=1}^{K_i} (A_{ik} \cup B_{ij}) : P_{ik}$. On the right-hand side of the laws each of these similar branches of branches (of which it is assumed there are I) is collapsed into a single set of branches $\sum_{k=1}^{K_i}(A_{ik} \cup C_i) : P_{ik}$, which involves a world of some newly-defined hidden resources, $\{\rho_i\}_i$. The number of new resources used differs in the two laws: Law Standard(1) covers the case where the B_{ij}'s do not constitute all worlds of the hidden resources of the process, that is, there exists at least some world of the hidden resources for which no behavior is defined. Then, I new resources are used, and $C_i = \bigcup_{1 \le j < i} \{\overline{\rho_j}\} \cup \{\rho_i\}$, for all i, $1 \le i \le I$. Law Standard (2) handles the case where behavior is described for all worlds of the hidden resources. In this case $I-1$ resources are used and the I possible behaviors of the process are captured by the resource combinations $C_i = \bigcup_{1 \le j < i}\{\overline{\rho_j}\} \cup \{\rho_i\}$, $1 \le i \le I-1$, $C_I = \{\overline{\rho_1}, \ldots, \overline{\rho_{I-1}}\}$. Thus, a set of new resources is used to create a number of mutually exclusive worlds, each of which is used to represent different behaviors of the left-hand side process. The probabilities of each of the required resources can be obtained by solving the set of equations $\mathsf{p}(C_i) = \sum_{j=1}^{J_i} \mathsf{p}(B_{ij})$, for all i. It can be shown that a unique solution exists to this set of equations with each of the solutions in $[0,1]$, as required. In particular, we have that, if $\sum_{j=1}^{J_i} \mathsf{p}(B_{ij}) = \pi_i$, $0 < \mathsf{p}(\rho_i) = \frac{\pi_i}{1 - \sum_{i=1}^{i-1} \pi_i} \le 1$.

We illustrate the intuition behind the two Standard laws with two examples. First, let $I = 1$ and $J_1 = K_1 = 2$. Then, assuming all resources are hidden and omitting the index i, the left-hand side process of both Standard laws is $P = (B_1{:}P_1 + B_1{:}P_2 + B_2{:}P_1 + B_2{:}P_2)\backslash\backslash V$. Figure 1(a) gives the transitions for $(P, \emptyset)$. Law Standard(1) allows us to merge the probabilistic branches that lead to the same processes, arriving at a bisimilar process $Q = (C{:}P_1 + C{:}P_2)\backslash\backslash V \cup C$, as illustrated in Figure 1 (b). In this case, $C = \{\rho\}$ with $\mathsf{p}(C) = \mathsf{p}(B_1) + \mathsf{p}(B_2)$. For a more detailed example, consider the process $P = (\{r_1, r_2\}{:}P_1 + \{r_1, r_2\}{:}P_2 + \{r_1, \overline{r_2}\}{:}P_3 + \{\overline{r_1}, r_2\}{:}P_3)\backslash\backslash\{r_1, r_2\}$. If both resources r_1, r_2 are available, P can silently evolve into either P_1 or P_2. If either one of the resources is available, P can evolve into P_3. Otherwise, P is deadlocked. We need to group together the cases where P evolves into P_3 into a single term, introducing new hidden resources in order to match the probability of arriving at P_3. Applying Law Standard(1), we obtain the process $Q = (\{\rho_1\}{:}P_1 + \{\rho_1\}{:}P_2 + \{\overline{\rho_1}, \rho_2\}{:}P_3)\backslash\backslash\{r_1, r_2, \rho_1, \rho_2\}$, where the failure probabilities are assigned to ρ_1 and ρ_2 in such a way that $\mathsf{p}(\rho_1) = \mathsf{p}(r_1) \cdot \mathsf{p}(r_2)$ and

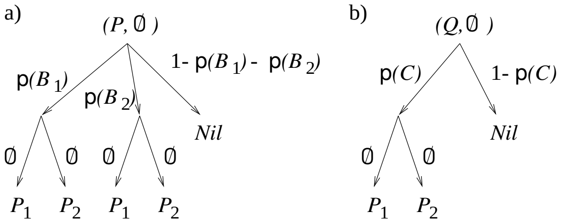

Figure 1: Law Standard(1)

$\mathsf{p}(\overline{\rho_1}) \cdot \mathsf{p}(\rho_2) = \mathsf{p}(r_1) \cdot \mathsf{p}(\overline{r_2}) + \mathsf{p}(\overline{r_1}) \cdot \mathsf{p}(r_2)$.

6 Soundness

[2] provides a sound axiomatization for the nonprobabilistic process algebra ACSR. We note that every PACSR-lite term is also an ACSR term, and that all Choice and Hide laws in Table 2 hold for ACSR as well. We refer to these laws as $\mathcal{A}'$. Their soundness with respect to probabilistic strong bisimulation can be derived as a consequence of these facts. In the sequel we will use $P =' Q$ to denote that P and Q can be shown to be equivalent by using laws $\mathcal{A}'$, $\sim'$ to refer to strong nonprobabilistic bisimulation, and $\longrightarrow'$ to refer to the transition relation of ACSR, as defined in [2]. We introduce the notion of compatibility between PACSR-lite processes as follows.

Definition 6.1 An equivalence relation $\mathcal{R} \subseteq \sim'$ is a *compatibility relation* if, whenever $P\mathcal{R}Q$, 1) $\mathsf{imr}(P) = \mathsf{imr}(Q)$, and 2) for all $\alpha \in Act$, if $P \xrightarrow{\alpha}{}' P'$ then $Q \xrightarrow{\alpha}{}' Q'$ and $P'\mathcal{R}Q'$. Two processes P and Q are *compatible*, if there exists a compatibility relation $\mathcal{R}$ such that $P\mathcal{R}Q$. □

A useful fact that we will be using is that if $P =' Q$ then P and Q are compatible to each other. This can be easily proved by induction on the size of the $='$-proof.

The following theorem achieves that, if two PACSR-lite processes can be shown to be equivalent by using laws in $\mathcal{A}'$, then they are bisimilar.

Theorem 6.2 If $P =' Q$ then $P \sim Q$.

Proof: Let

$$\mathcal{R} = \{((P,\emptyset),(Q,\emptyset)) \mid P, Q \text{ are compatible}\} \cup \{((P,W),(Q,W)) \mid P, Q \text{ are compatible}, (P,W),(Q,W) \in S_n\}$$

The proof involves showing that $\mathcal{R} \subseteq \sim$. This follows easily given the compatibility of the processes in the two types of configurations. Then, since $P =' Q$ implies that P and Q are compatible, we may conclude that $P \sim Q$ as required. $\square$

It remains to establish the soundness of laws Rename, Down, Up, and the laws of Table 3.

Lemma 6.3 If P and Q are related by the laws Rename, Down, Up, Extend, Standard(1), or Standard(2), then $P \sim Q$.

Proof: The proof follows easily from the definition of strong bisimulation. We consider the two most interesting laws:

Extend Let $P \equiv (\sum_{i\in I} A_i{:}P_i)\backslash\backslash V$ and $Q \equiv (\sum_{j\in I, r\notin A_j}(A_j \cup \{r\}){:}P_j + (A_j \cup \{\overline{r}\}){:}P_j) + \sum_{j \in I, r\in A_j} A_j{:}P_j)\backslash\backslash V$, $r \in V$. Clearly, $\{r\} \cup \mathsf{imr}(P) = \mathsf{imr}(Q)$. For each world W where $(Q,W) \in S_n$, $(P,W) \in S_n$ and (P,W) has exactly the following transitions: (1) if $r \notin A_i$ and either $A_i \cup \{r\} \subseteq W$ or $A_i \cup \{\overline{r}\} \subseteq W$, then $(P,W) \xrightarrow{A_i - V} (P_i, W)$ and (2) if $r \in A_i$ and $A_i \subseteq W$, then $(P,W) \xrightarrow{A_i - V} (P_i,W)$. (Q,W) has exactly the same transitions. If $r \in \mathsf{imr}(P)$ then $\mathsf{imr}(P) = \mathsf{imr}(Q)$, and $(P,\emptyset) \xrightarrow{p}_p (P,W)$ iff $(Q,\emptyset) \xrightarrow{p}_p (Q,W)$. Otherwise, for every W such that $(P,\emptyset) \xrightarrow{p}_p (P,W)$, Q reaches, with the same probability p, the set $\{(Q, W \cup \{r\}), (Q, W\cup\{\overline{r}\})\}$, where, clearly, $(Q, W\cup\{r\}) \sim (Q, W \cup \{\overline{r}\})$. The result follows.

Standard(1) Let P, Q denote the left-hand and right-hand sides of this law, respectively. We prove the soundness of a restricted version of this law where P, Q have no free resources and $K_i = 1$, for all i. This allows us to concentrate on the essence of the law, that is, the effect of renaming bound resources. The full result follows easily given that the processes on each side of the equation have the same behavior under each valuation of the bound resources. Let $P \equiv (\sum_{i=1}^{I}\sum_{j=1}^{J_i} B_{ij}{:}P_i)\backslash\backslash V$ and $Q \equiv (\sum_{i=1}^{I} C_i{:}P_i)\backslash\backslash V \cup \{\rho_1, \ldots, \rho_I\}$. We observe that both processes can evolve into the equivalence classes $\mathcal{M}_i = [\emptyset{:}P_i]_\sim, 1 \leq i \leq I$ and the equivalence class $[\text{NIL}]_\sim$. Then, $\mu(P, \mathcal{M}_i) = \sum_{j=1}^{J_i} \mathsf{p}(B_{ij}) = \mathsf{p}(C_i) = \mu(Q, \mathcal{M}_i)$. Therefore, $P \sim Q$. $\square$

7 Completeness of the axiomatization

In this section we will prove that the laws given in Tables 2 and 3 are complete for PACSR-lite. The completeness proof is carried out in the standard way: First, we develop a kind of standard set of equations and show that it is satisfied by any PACSR-lite process. We then show that two bisimilar processes can be shown to satisfy a common set of standard equations and, finally, we appeal to the result that such sets of equations have a unique solution up to bisimulation. While this approach may seem unnecessarily complicated, given that PACSR-lite processes exhibit only finite behaviors, we want to be able to reuse the arguments for the case of the full PACSR which uses recursion to express infinite behaviors.

7.1 Standard Set of Equations

In this section we show that any $P \in \mathsf{Pr}$ provably satisfies a particular set of equations. Let $\widetilde{X}$ be a set of variables and $\widetilde{H}$ be terms. We say that a process P provably satisfies a set of equations $S : \widetilde{X} = \widetilde{H}$ if there is a set of terms $\widetilde{P} = \{P_1, P_2, \ldots, P_n\}$ such that $\widetilde{P} = \widetilde{H}[\widetilde{P}/\widetilde{X}]$ and $P = P_1$.

A set of equations $S : \widetilde{X} = \widetilde{H}$ is said to be *standard* if for all $i \geq 1$

$$X_i = (\sum_{j\in J_i}\sum_{k\in K_i} A_{jk} \cup B_j : X_{jk})\backslash\backslash V_i,$$

where $X_i, X_{jk} \in \widetilde{X}$, for all i, j, k, and

1. $\bigcup_{j\in J_i, k\in K_i} A_{jk} \cap V_i = \emptyset$, $A_{jk} \subseteq \mathsf{fr}(X_1)$, and for all $r \in \bigcup_{j\in J_i, k\in K_i} A_{jk}$, $\mathsf{p}(r) \neq 0$,
2. $\bigcup_{j\in J} B_j = V_i$ and for all $r \in \bigcup_{j\in J_i} B_j$, $\mathsf{p}(r) \notin \{0, 1\}$, and
3. for all $j_l, j_m \in J_i$, $j_l \neq j_m$, either $\overline{B_{j_l}} \subseteq B_{j_m}$ or $\overline{B_{j_m}} \subseteq B_{j_l}$.

Note in this definition that the hide operator cannot be eliminated from standard sets of equations: the probabilistic information that accompanies a hidden resource is necessary for defining the semantics of a process and it cannot be encoded by any other means. (In ACSR this is possible and standard sets of equations can be given as unrestricted summations.) However, the Hide-laws allow us, after possibly renaming some resources, to partially push the hiding operators *inwards* in a given process. Thus in a standard set of equations, an equation contains the summation of a set of prefixed variables restricted only by resources immediately relevant to the process. The conditions stipulate that A_{jk} are the visible resources of the process, all of which have nonzero probability, and $V_i = \bigcup_{j\in J} B_j$ the hidden resources, all of which have probability $0 < p < 1$. Moreover, the B_j's represent mutually distinct worlds.

We will show that every $P \in \mathsf{Pr}$ satisfies a standard set of equations. Before doing this we present a useful lemma.

Lemma 7.1 Suppose P provably satisfies a standard set of equations S. Then $P\backslash\backslash V$ and $P[x/y]$, where $y \in \mathsf{br}(P)$, x is a new name, and $\mathsf{p}(x) = \mathsf{p}(y)$, also satisfy standard sets of equations.

Proof: The proof follows by explicitly constructing the sets of standard equations satisfied by $P\backslash\backslash V$ and $P[x/y]$, transforming the set of standard equations satisfied by P. $\square$

Theorem 7.2 Every PACSR-lite process R provably satisfies a standard set of equations.

Proof: By induction on the structure of R. We present the most interesting case: $R = P + Q$. By the induction hypothesis, P provably satisfies $S : \widetilde{X} = \widetilde{H}$ and Q provably satisfies $T : \widetilde{Y} = \widetilde{G}$. This implies that there exist terms $\widetilde{P}$ and $\widetilde{Q}$ such that $P = P_1$ and $Q = Q_1$ and $P + Q$ has the form

$$\begin{array}{l}(\sum_{j\in J_1}\sum_{k\in K_1} A_{jk} \cup B_j : P_{jk})\backslash\backslash V \\ \quad +(\sum_{l\in L_1}\sum_{m\in M_1} C_{lm} \cup D_l : Q_{lm})\backslash\backslash U \ .\end{array}$$

Using Rename, we can rewrite both summands so that all the bound immediate resources of each summand are fresh and different from the resources of the other summand. Then using Hide(6) and Hide(2) we can pull the hide operation to the outer level of the term, and $P + Q$:

$$\begin{array}{rl} = & (\sum_{j\in J_1}\sum_{k\in K_1} A_{jk} \cup B'_j : P'_{jk})\backslash\backslash V' \\ + & (\sum_{l\in L_1}\sum_{m\in M_1} C_{lm} \cup D'_l : Q'_{lm})\backslash\backslash U' \\ = & (\sum_{j\in J_1}\sum_{k\in K_1} A_{jk} \cup B'_j : P'_{jk} \\ + & \sum_{l\in L_1}\sum_{m\in M_1} C_{lm} \cup D'_l : Q'_{lm})\backslash\backslash V' \cup U', \end{array}$$

where, if $\widetilde{y}_1 = res(\bigcup_j B_j) \cap res(Q)$, $\widetilde{y}_2 = res(\bigcup_l D_l) \cap res(P)$, and $\widetilde{x}_1$, $\widetilde{x}_2$, are fresh resources such that for all i, j, $\mathsf{p}(x_{1_i}) = \mathsf{p}(y_{1_i})$, $\mathsf{p}(x_{2_j}) = \mathsf{p}(y_{2_j})$, $V' = V[\widetilde{x}_1/\widetilde{y}_1]$, $P'_{jk} = P_{jk}[\widetilde{x}_1/\widetilde{y}_1]$, $B'_l = B_l[\widetilde{x}_1/\widetilde{y}_1]$, and $U' = U[\widetilde{x}_2/\widetilde{y}_2]$, $Q'_{lm} = Q_{lm}[\widetilde{x}_2/\widetilde{y}_2]$, $D'_l = D_l[\widetilde{x}_2/\widetilde{y}_2]$.

To transform the above process to standard form and in particular to satisfy condition (1), we will need to apply Laws Extend and Standard. First, we close the summands of the process with information about all immediate hidden resources of the process by applying Law Extend once for every $r \in \bigcup_{j\in J_1} B'_j \cup \bigcup_{l\in L_1} D'_l$ to obtain:

$$(\sum_{n\in N}\sum_{j\in J_1}\sum_{k\in K_1} A_{jk} \cup B'_j \cup E_n : P'_{jk} +$$

$$\sum_{n\in N'}\sum_{l\in L_1}\sum_{m\in M_1} C_{lm}\cup D'_l\cup F_n : Q'_{lm})\backslash\backslash V\cup U'$$

where the $\bigcup_{n\in N} E_n$ are the possible combinations of the immediate bound resources of process Q, $\bigcup_{l\in L_1} D'_l$, and similarly, the $\bigcup_{n\in N'} F_n$ are the possible combinations of the immediate bound resources of process P, $\bigcup_{j\in J_1} B'_j$. Now it remains to rearrange the last two summands in the style of the left-hand side of the Standard-laws by grouping together all processes that can take place under the same evaluation of the hidden resources, and then isolating all worlds that exhibit the same behavior. So, using Choice(3), Choice(4) and finally Standard ((1) or (2) depending on the B'_{ij}'s), we have that $P+Q$

$$\begin{aligned}
&= (\textstyle\sum_{i\in I}\sum_{j\in J_i}\sum_{k\in K_i} A'_{ik}\cup B'_{ij} : R'_{ik})\backslash\backslash V\cup U'\\
&= (\textstyle\sum_{i\in I}\sum_{n\in N_i} A'_{in}\cup C_i : R_{in})\backslash\backslash V\cup U'\cup\widetilde{\rho}\\
&= (\textstyle\sum_{i\in I}\sum_{n\in N_i} A'_{in}\cup C_i : (R_{in}\backslash\backslash V\cup U'))\backslash\backslash\widetilde{\rho}
\end{aligned}$$

where for all $i_l \neq i_m$ either $\overline{C_{i_l}} \subseteq C_{i_m}$ or $\overline{C_{i_m}} \subseteq C_{i_l}$. Further, by Laws Down and Up, $P+Q = (\sum_{i\in I}\sum_{n\in N_i} A'_{in}\cup C'_i : (R_{in}\backslash\backslash V\cup U'))\backslash\backslash\widetilde{\rho}'$, where $C'_i = \{r \mid \mathsf{p}(r)\neq 1, r\in C_i\}$ and $\widetilde{\rho}' = res(\bigcup_i C'_i)$. Since each R_{in} is either a $P'_{jk} = P_{jk}[\widetilde{x}_1/\widetilde{y}_1]$, or a $Q'_{lm} = Q_{lm}[\widetilde{x}_2/\widetilde{y}_2]$, and by the induction hypothesis each P_{jk}, Q_{lm} provably satisfies a standard set of equations, by Lemma 7.1, each R_{in} satisfies a standard set of equations $S^{in} : \widetilde{X}^{in} = \widetilde{H}^{in}$ with distinguished variable X_1^{in}. Then $P+Q$, satisfies the standard set of equations: $\{X_1 = (\sum_{i\in I}\sum_{n\in n_i} A'_{in}\cup C'_i : X_1^{in})\backslash\backslash\widetilde{\rho}'\}\bigcup_{i,n} S^{in}$. □

7.2 Common Set of Standard Equations

Theorem 7.3 *Let P and Q provably satisfy two standard sets of equations S and T. If P and Q are bisimilar, then there exists a third standard set of equations S' satisfied by both P and Q.*

Proof: We will again restrict our attention to processes with standard sets of equations containing no visible resources, and $K_i = \{1\}$. This allows us to focus on the central aspects of the proof that involve the renaming of bound resources.

Suppose that $\widetilde{X}$ and $\widetilde{Y}$ are disjoint sets of variables, and that the given sets of equations are $S : \widetilde{X} = \widetilde{H}$, $T : \widetilde{Y} = \widetilde{G}$. Further, let $\widetilde{P}$ and $\widetilde{Q}$ be such that $\widetilde{P} = \widetilde{H}[\widetilde{P}/_{\widetilde{X}}]$, $\widetilde{Q} = \widetilde{G}[\widetilde{Q}/_{\widetilde{Y}}]$, with $P = P_1$, $Q = Q_1$, so that $P_i = (\sum_{j\in J_i} B_j{:}P_j)\backslash\backslash U_i$, and $Q_i = (\sum_{l\in L_i} D_l{:}Q_l)\backslash\backslash V_i$. Let us consider the relation $\mathcal{R}$ such that $(u,v)\in\mathcal{R}$ iff $P_u \sim Q_v$. Clearly, $(1,1)\in\mathcal{R}$. Let $(u,v)\in\mathcal{R}$ and consider P_u and Q_v. Suppose that there exists $W\in\mathcal{W}(\bigcup_j B_j)$ such that for all j, $B_j \nsubseteq W$. (The other case follows similarly with the exception that law Standard(2) is used instead of Standard(1).) We may construct a partition $\Lambda = \{\widetilde{j}_1,\ldots,\widetilde{j}_n\}$ of J_u, such that if $j,j'\in\widetilde{j}_\lambda$, $P_j \sim P_{j'}$, and vice versa. Similarly, let $\Lambda' = \{\widetilde{l}_1,\ldots,\widetilde{l}_{n'}\}$ be the equivalent partition of Q_v. Since P_u and Q_v must have equal transitions, the following statement is true:

> $n = n'$, and for each $\widetilde{j}_\lambda \in \Lambda$, there exists $\widetilde{l}_{\lambda'}\in\Lambda'$ such that for any $j\in\widetilde{j}_\lambda$, $l\in\widetilde{l}_{\lambda'}$, $(j,l)\in\mathcal{R}$, $\sum_{j\in\widetilde{j}_\lambda}\mathsf{p}(B_j) = \sum_{l\in\widetilde{l}_{\lambda'}}\mathsf{p}(D_l)$.

Thus P_u and Q_v can be rewritten as follows $P_u = (\sum_{\lambda=1}^n\sum_{j\in\widetilde{j}_\lambda} B_j{:}P_j)\backslash\backslash U_u, Q_v = (\sum_{\lambda=1}^n\sum_{l\in\widetilde{l}_\lambda} D_l{:}Q_l)\backslash\backslash V_v$, where we assume that the summations are ordered so that for all $1\leq\lambda\leq n$, classes $\widetilde{j}_\lambda$, $\widetilde{l}_\lambda$ are matching, in the sense of the above statement.

However, despite the bisimilarity of the two processes and the fact that they have the same cumulative probability of reaching each equivalence class of $\sim$, they may be using different sets of bound resources and thus may have different branching structures. Our intention is to show that P_u and Q_v can be rewritten into equal processes having identical branching structures. To do this we will employ a set of new hidden resources, and rewrite the two processes in such a way that each probabilistic transition of the initial processes with probability p is replaced by a set of probabilistic transitions with cumulative probability p. In particular, given an equivalence class λ we will use the greatest common divisor, γ_λ, of the probabilities $\mathsf{p}(B_j)$, $\mathsf{p}(D_l)$, where $j \in \widetilde{j}_\lambda$, $l \in \widetilde{l}_\lambda$, and, if $\mathsf{p}(B_j) = p$, we will replace the term $B_j{:}P_j$ by a summation of the form $\sum_{\nu \in N_j} \widetilde{\rho}_\nu{:}P_j$, where each $\mathsf{p}(\widetilde{\rho}_\nu) = \gamma_\lambda$ and $|N_j| = \frac{p}{\gamma_\lambda}$, for some appropriately chosen worlds of bound resources $\widetilde{\rho}_\nu$. A similar treatment will be applied for each term $D_l{:}Q_l$. This will ensure that both resulting processes have exactly the same probabilistic transitions to each equivalence class of $\sim$. We achieve this as follows:

For every λ, let γ_λ be the greatest common divisor of the probabilities $\mathsf{p}(B_j)$, $\mathsf{p}(D_l)$, for all $j \in \widetilde{j}_\lambda$, $l \in \widetilde{l}_\lambda$. Further, let $\Delta^\lambda = \frac{\sum_{j \in \widetilde{j}_\lambda} \mathsf{p}(B_j)}{\gamma_\lambda}$ and $\Delta = \sum_\lambda \Delta^\lambda$. By the definition of γ_λ, Δ^λ and thus Δ are integers. Let $\widetilde{\rho}_{uv} = \rho_1, \ldots, \rho_\Delta$, be new resources and $\widetilde{\rho}_1, \ldots, \widetilde{\rho}_\Delta$, mutually exclusive worlds involving these resources, as defined in Law Standard(1), such that the first Δ^1 worlds have probability γ_1, the next Δ^2 worlds probability γ_2, and so on. Finally, if $j \in \widetilde{j}_\lambda$, let $\delta_j^\lambda = \frac{\mathsf{p}(B_j)}{\gamma_\lambda}$, and let $\Delta_j^\lambda = \{\sum_{\lambda' < \lambda} \Delta^\lambda + \sum_{r<j} \delta_r^\lambda + 1, \sum_{\lambda' < \lambda} \Delta^\lambda + \sum_{r<j} \delta_r^\lambda + 2, \ldots, \sum_{\lambda' < \lambda} \Delta^\lambda + \sum_{r \leq j} \delta_r^\lambda\}$. Similarly, if $l \in \widetilde{l}_\lambda$, let $\epsilon_l^\lambda = \frac{\mathsf{p}(D_l)}{\gamma_\lambda}$, and let $E_l^\lambda = \{\sum_{\lambda' < \lambda} \Delta_\lambda + \sum_{r<l} \epsilon_r^\lambda + 1, \sum_{\lambda' < \lambda} \Delta^\lambda + \sum_{r<l} \epsilon_r^\lambda + 2, \ldots, \sum_{\lambda' < \lambda} \Delta^\lambda + \sum_{r \leq l} \epsilon_r^\lambda\}$. We may see that $\bigcup_{\lambda,j} \{\Delta_j^\lambda\}$ and $\bigcup_{\lambda,l} \{E_l^\lambda\}$ are partitions of $\{1, \ldots, \Delta\}$. By laws Extend and Standard(1), we have that the two processes satisfy the following equations: $P_u = (\sum_{\lambda=1}^n \sum_{j \in \widetilde{j}_\lambda} \sum_{\nu \in \Delta_j^\lambda} \widetilde{\rho}_\nu{:}P_j) \backslash\backslash \widetilde{\rho}_{uv}$, $Q_v = (\sum_{\lambda=1}^n \sum_{l \in \widetilde{l}_\lambda} \sum_{\nu \in E_l^\lambda} \widetilde{\rho}_\nu{:}Q_l) \backslash\backslash \widetilde{\rho}_{uv}$.

Let $\widetilde{X}'$ and $\widetilde{Y}'$, be disjoint sets of variables, and consider the sets of equations $S' : \widetilde{X}' = \widetilde{H}'$, $T' : \widetilde{Y}' = \widetilde{G}'$, where $X'_u = (\sum_{\lambda=1}^n \sum_{j \in \widetilde{j}_\lambda} \sum_{\nu \in \Delta_j^\lambda} \widetilde{\rho}_\nu{:}X'_j)) \backslash\backslash \widetilde{\rho}_{uv}$, $Y'_v = (\sum_{\lambda=1}^n \sum_{l \in \widetilde{l}_\lambda} \sum_{\nu \in E_l^\lambda} \widetilde{\rho}_\nu{:}Y'_l) \backslash\backslash \widetilde{\rho}_{uv}$. It can be shown that S' and T' are satisfied by P and Q respectively.

Let us now consider the set of equations $\widetilde{Z} = \widetilde{F}$, defined for all $(u,v) \in \mathcal{R}$ by

$$Z_{u,v} = (\sum_{\lambda=1}^{n} \sum_{\nu=1}^{\Delta} \sum_{(j,l) \in K_{uv\nu}} \widetilde{\rho}_\nu{:}Z_{j,l}) \backslash\backslash \widetilde{\rho}_{uv}$$

with $K_{uv\nu} = \{(j,l)\}$ s.t. $\widetilde{\rho}_\nu{:}P_j$ is a summand of P_u, $\widetilde{\rho}_\nu{:}Q_l$ is a summand of Q_v, $(j,l) \in \mathcal{R}$. Again, it is easy to prove that this is a set of standard equations.

Now take the set of processes $R_{j,l} = P_j$, for all l. Terms $F_{i,j}[\widetilde{R}/\widetilde{Z}]$ contain the same summands as $H'_i[\widetilde{P}/\widetilde{X'}]$. In particular, $F_{1,1}[\widetilde{R}/\widetilde{Z}] = P_1 = P$. Hence P satisfies this new set of equations. A similar reasoning can be applied to show that Q satisfies the same set of equations. This completes the proof.

□

7.3 Unique Solution

We now have to prove that if two processes satisfy the same set of standard equations, they are bisimilar. Such is the objective of the following theorem. Its proof follows exactly the proof given by Milner[9].

Theorem 7.4 *A set of standard equations has a unique solution up to a bisimulation.*

Since, by Theorem 7.3, if $P \sim Q$ then P and Q satisfy a common set of standard equations, by Theorem 7.4 we have the final result:

Theorem 7.5 *For any two processes P and Q, if $P \sim Q$ then $P = Q$.*

8 Conclusions

We have presented a sound and complete axiomatization of strong bisimulation for PACSR-lite: a fragment of the resource-oriented process algebra PACSR. The key technical hurdle was to axiomatically characterize the effects of resource hiding in a probabilistic setting. As ongoing work, we are extending the axiomatization to the full PACSR.

Acknowledgments: We thank the anonymous referees for valuable comments and suggestions.

References

[1] J. Baeten, J. Bergstra, and S. Smolka. Axiomatizing probabilistic processes: ACP with generative probabilities. *Information and Computation*, 121(2):234–255, 1995.

[2] P. Brémond-Grégoire, J. Choi, and I. Lee. A complete axiomatization of finite-states ACSR processes. *Information and Computation*, 138(2):124–159, 1997.

[3] A. Giacalone, C. Jou, and S. Smolka. Algebraic reasoning for probabilistic concurrent systems. In *Proceedings of Working Conference on Programming Concepts and Methods*. IFIP TC 2, North-Holland, 1990.

[4] H. Hansson. *Time and Probability in Formal Design of Distributed Systems*. PhD thesis, Department of Computer Systems, Uppsala University, 1991. DoCS 91/27.

[5] J.-P. Katoen, R. Langerak, and D. Latella. Modeling systems by probabilistic process algebra: An event structures approach. In *Proceedings of FORTE '92*, pages 255–270, 1993.

[6] K. Larsen and A. Skou. Bisimulation through probabilistic testing. In *Conference Record of the* 16^{th} *ACM Symposium on Principles of Programming Languages*, pages 344–352, 1989.

[7] I. Lee, P. Brémond-Grégoire, and R. Gerber. A process algebraic approach to the specification and analysis of resource-bound real-time systems. *Proceedings of the IEEE*, pages 158–171, 1994.

[8] R. Milner. *A Calculus of Communicating Systems*, volume 92 of *Lecture Notes in Computer Science*. Springer-Verlag, 1980.

[9] R. Milner. A complete axiomatization for observational congruence of finite-state behaviors. *Information and Computation*, 81:227–247, 1989.

[10] D. Park. Concurrency and automata on infinite sequences. In *Proceedings of* 5^{th} *GI Conference*, volume 104 of *Lecture Notes in Computer Science*, pages 167–183, 1981.

[11] A. Philippou, O. Sokolsky, R. Cleaveland, I. Lee, and S. Smolka. Probabilistic resource failure in a real-time process algebra. In *Proceedings of CONCUR '98*, 1998.

[12] A. Philippou, O. Sokolsky, I. Lee, R. Cleaveland, and S. Smolka. Hiding resources that can fail: An axiomatic perspective. Technical Report TR-2001-1, Department of Computer Science, University of Cyprus, 2001. Available at http://www.cs.ucy.ac.cy/Research/Technical_reports.html.

[13] K. Seidel. *Probabilistic CSP*. PhD thesis, Oxford University, 1992.

[14] C. Tofts. Processes with probabilities, priorities and time. *Formal Aspects of Computing*, 4:536–564, 1994.

Choice(1)	$P + \mathrm{NIL} = P$
Choice(2)	$P + P = P$
Choice(3)	$P + Q = Q + P$
Choice(4)	$(P + Q) + R = P + (Q + R)$
Hide(1)	$\mathrm{NIL}\backslash\backslash I = \mathrm{NIL}$
Hide(2)	$(P + Q)\backslash\backslash I = (P\backslash\backslash I) + (Q\backslash\backslash I)$ if $\mathsf{imr}(P) \cap \mathsf{imr}(Q) \cap I = \emptyset$
Hide(3)	$(A{:}P)\backslash\backslash I = (A{:}(P\backslash\backslash I))\backslash\backslash res(A) \cap I$
Hide(4)	$P\backslash\backslash I\backslash\backslash J = P\backslash\backslash I \cup J$
Hide(5)	$P\backslash\backslash\emptyset = P$
Hide(6)	$P\backslash\backslash I = P\backslash\backslash I \cup \{r\}$ if $r \notin res(P)$
Down	$A{:}P = \mathrm{NIL}$, if for some $r \in A, \mathsf{p}(r) = 0$
Up	$A{:}P\backslash\backslash I = ((A - \{r\}) : P)\backslash\backslash I$, $r \in A \cap (I \cup \overline{I}), \mathsf{p}(r) = 1$
Rename	$P\backslash\backslash I = P[r'/r]\backslash\backslash(I - \{r\}) \cup \{r'\}$ if $r \in I,\ r' \notin res(P)$ and $\mathsf{p}(r) = \mathsf{p}(r')$

Table 2: Laws for sum and hiding

Extend	$(\sum_{i\in I} A_i{:}P_i)\backslash\backslash V = (\sum_{j\in I, r\notin A_j}(A_j \cup \{r\}) : P_j + (A_j \cup \{\overline{r}\}) : P_j)$ $+\sum_{j\in I, r\in A_j} A_j : P_j)\backslash\backslash V$ where $r \in V$
Standard(1)	$(\sum_{i=1}^{I}\sum_{j=1}^{J_i}\sum_{k=1}^{K_i}(A_{ik} \cup B_{ij}) : P_{ik})\backslash\backslash V$ $= (\sum_{i=1}^{I}\sum_{k=1}^{K_i}(A_{ik} \cup C_i) : P_{ik})\backslash\backslash V \cup \{\rho_1, \ldots, \rho_I\}$ if $\exists W \in \mathcal{W}(\bigcup_{i,j} B_{ij})\ \forall i, j \cdot B_{ij} \not\subseteq W$, and whenever $i, j \neq m, n,\ res(B_{ij}) = res(B_{mn}),\ B_{ij} \neq B_{mn}$ and where $\bigcup_{i,j} B_{ij} \subseteq V,\ (\bigcup_{i,k} A_{ik}) \cap V = \emptyset$, $C_i = \bigcup_{1\leq j<i}\{\overline{\rho_j}\} \cup \{\rho_i\}$, where $\rho_1, \ldots, \rho_I$ are fresh resources, such that $\mathsf{p}(C_i) = \sum_{j=1}^{J_i}\mathsf{p}(B_{ij})$
Standard(2)	$(\sum_{i=1}^{I}\sum_{j=1}^{J_i}\sum_{k=1}^{K_i}(A_{ik} \cup B_{ij}) : P_{ik})\backslash\backslash V$ $= (\sum_{i=1}^{I}\sum_{k=1}^{K_i}(A_{ik} \cup C_i) : P_{ik}$ if $\forall W \in \mathcal{W}(\bigcup_{i,j} B_{ij})\ \cdot \exists i, j\ A_{ik} \cup B_{ij} \subseteq W$, and whenever $i, j \neq m, n,\ res(B_{ij}) = res(B_{mn}),\ B_{ij} \neq B_{mn}$ and where $\bigcup_{i,j} B_{ij} \subseteq V,\ (\bigcup_{i,k} A_{ik}) \cap V = \emptyset$, $C_i = \bigcup_{1\leq j<i}\{\overline{\rho_j}\} \cup \{\rho_i\},\ 1 \leq i \leq I - 1,\ C_I = \{\overline{\rho_1}, \ldots, \overline{\rho_{I-1}}\}$, where $\rho_1, \ldots, \rho_{I-1}$ are fresh resources, such that $\mathsf{p}(C_i) = \sum_{j=1}^{J_i}\mathsf{p}(B_{ij})$

Table 3: Laws for reintroduction of hidden resources