Theoretical Computer Science 637 (2016) 30–58

Contents lists available at ScienceDirect

Theoretical Computer Science

www.elsevier.com/locate/tcs

A logic of separating modalities

Jean-René Courtault[a], Didier Galmiche[a], David Pym[b,*]

[a] LORIA, Université de Lorraine, Campus Scientifique, BP 239, 54506 Vandoeuvre-lès-Nancy Cedex, France
[b] University College London, Gower Street, London WC1E 6BT, UK

ARTICLE INFO

Article history:
Received 29 April 2015
Received in revised form 16 February 2016
Accepted 30 April 2016
Available online 6 May 2016
Communicated by A. Avron

Keywords:
Bunched logic
Separation logic
Modal logic
Resource semantics
Tableaux
Concurrency

ABSTRACT

We present a logic of separating modalities, LSM, that is based on Boolean BI. LSM's modalities, which generalize those of S4, combine, within a quite general relational semantics, BI's resource semantics with modal accessibility. We provide a range of examples illustrating their use for modelling. We give a proof system based on a labelled tableaux calculus with countermodel extraction, establishing its soundness and completeness with respect to the semantics.

1. Introduction

The concept of resource is important in many fields of enquiry — including, among others, computer science, economics, and security. In recent years, mathematical work in logic has begun to analyse the concept of resource in quite systematic and quite useful ways, with computer science providing a rich source of motivations and examples.

One impetus for this work was provided by the so-called resource interpretation of Girard's Linear Logic [19], in which the number of occurrences of a propositional formula in a sequent is counted and in which the exponentials are used to provide countably infinitely many copies of propositional formulæ. An alternative approach — inspired, on the one hand, by a long semantic history in relevant logic (e.g., [34,11]) and, on the other, by work in the semantics of type theories — is exemplified by O'Hearn and Pym's Logic of Bunched Implications (BI) [30,26,33,16,17]. In BI, the concept of resource resides in an interpretation of BI's semantics: this approach, and its developments, is known as resource semantics.

Conceptually, resource semantics begins with a simple axiomatization of resource. Starting with a given homogeneous set of resource elements — for example, bags of fruit, units of currency, or computer memory — we expect the following properties:

- to be able to combine two units of the given type of resource to form a new unit of that type of resource;
- to be able to compare (using either a simple equality or an ordering) two units of a given type of resource;
- that combination and comparison should be appropriately compatible.

[*] Corresponding author.
E-mail addresses: jean-rene.courtault@loria.fr (J.-R. Courtault), didier.galmiche@loria.fr (D. Galmiche), d.pym@ucl.ac.uk (D. Pym).

http://dx.doi.org/10.1016/j.tcs.2016.04.040

This basic axiomatization has proved remarkably robust, supporting, for example, a good deal of work in Separation Logic and its precursors and developments, [11,22,28,35,27], and a vast subsequent literature.

Mathematically, this basic set-up is captured by a pre-ordered monoid of resources, defined as follows: $\mathbf{R} = (R, \sqsubseteq, \bullet, e)$, where R is a set of resource elements, $\sqsubseteq$ is a pre-order (writing $=$ for $\sqsubseteq \cap \sqsupseteq$) and $\bullet$ is a monoidal composition with unit e, subject to the functoriality coherence condition that if $r = s$ and $r' = s'$, then $r \bullet r' = s \bullet s'$ [30,26,33,17].

The semantics of (Boolean) BI is given using a satisfaction relation between resources and propositional formulæ, with cases such as

$$r \models \phi_1 \wedge \phi_2 \text{ iff } r \models \phi_1 \text{ and } r \models \phi_2,$$

that give the usual (additive) classical connectives, and cases such as

$$\begin{aligned} r \models \phi_1 * \phi_2 \text{ iff } & \text{there exist } r_1 \text{ and } r_2 \text{ such that } r_1 \bullet r_2 = r \text{ and} \\ & r_1 \models \phi_1 \text{ and } r_2 \models \phi_2 \end{aligned}$$

and

$$\begin{aligned} r \models \phi \mathrel{-\!\!*} \psi \text{ iff } & \text{for all } s \text{ such that } s \models \phi, \\ & r \bullet s \models \psi \end{aligned}$$

that give the multiplicative, or separating, connectives.

In terms of resource semantics, the additive conjunction ($\wedge$) is simply interpreted as specifying that the conjuncts must share the available resources whereas in the case of multiplicative conjunction ($*$) the available resources must be divided between the two conjuncts. Similarly, in the multiplicative implication ($\mathrel{-\!\!*}$), the resources required to support the implicational formula must be combined with those required to support the 'input' formula in order to obtain, by implication, the resources required to support the 'output' formula.

We can also work with intuitionistic BI, with its intuitionistic additives, as in [30,33,16,17], by considering a monoid of resources that carries not merely an equality but a pre-order, allowing intuitionistic implication to be defined in the usual way and leading to the multiplicative conjunction

$$\begin{aligned} r \models \phi_1 * \phi_2 \text{ iff } & \text{there exist } r_1 \text{ and } r_2 \text{ such that } r_1 \bullet r_2 \sqsubseteq r \text{ and} \\ & r_1 \models \phi_1 \text{ and } r_2 \models \phi_2 \end{aligned}$$

In this case, the functoriality condition is that if $r \sqsubseteq s$ and $r' \sqsubseteq s'$, then $r \bullet r' \sqsubseteq s \bullet s'$.

The dynamics of systems is a central concern in computer science. Many models and logics have been proposed in order to capture system behaviours and reason about their properties. In particular, modal logics based on S4 or S5 and their intuitionistic variants [2,36] and temporal logics such as LTL [31] or CTL [12]. The interest in such logics derives from their ability to express properties such as *invariance* (is a property satisfied in all reachable states of the system?) and *reachability* (is it possible to reach a state satisfying a property?).

Modal extensions of BI have been proposed in order to introduce dynamics into resource semantics. One of them, called MBI [6,4,5], is a logic in which resources and processes co-evolve according to an operational semantics based on judgements of the form $R, E \xrightarrow{a} R', E'$, meaning that the process E evolves by performing an action a relative to available resources R so as to become the process E' with available resources R'. This logic captures the manipulation of resources through the dynamic of a system, but is not able to express properties relative to quantified actions (e.g., properties deriving from performing *any* action). MBI's purely logical theory remains relatively undeveloped. Nevertheless, the use of these ideas as a basis for a rigorously resource-based modelling tool has been described in [7,5].

Another modal extension of BI, called DBI, introduces a simple notion of dynamic resource in which properties of resources can change or be modified during the iteration of the system [8]. The modalities of DBI ($\Diamond$ and $\Box$) allow the expression of properties of resources at any reachable state. Moreover, there exists a sound and complete calculus with a countermodel extraction method for this logic. DBI is not able to capture resource manipulations by a system: its models capture systems that modify properties of resources, but not systems that produce and consume resources.

In this paper, we present a modal logic of resources — LSM, for 'Logic of Separating Modalities' — that is based on Boolean BI's resource semantics. The logic extends S4. The basic idea is to work with two-dimensional worlds (w, r) that correspond to the purely modal and purely resource components of the semantics. The key development derives from their combination to define resource-modalities $\Diamond_r$ and $\Box_r$ in which 'modal truth' is offset by 'resource truth'. These modalities generalize their counterparts in S4 ($\Diamond$ and $\Box$). In Section 2, we introduce the language and the semantics of LSM, using a quite general relational formulation. In Section 3, we illustrate the expressiveness of its modalities thorough a range of core examples from computer systems. Then, in Section 4, we develop an extended example, showing that LSM provides useful tools for reasoning about a rich model of concurrent computation: in particular, we show that LSM is able to express directly and conveniently properties of timed Petri nets [24,1]. In Section 5, we place LSM in the broader context of modal logic by establishing, using a straightforward method based on countermodels, that LSM is a conservative extension of the classical modal logic S4. Then, in Section 6, we provide a proof system for LSM as a labelled tableaux calculus with countermodel extraction, in the spirit of similar approaches for BI and Boolean BI [16–18]. We show its soundness and completeness. Finally, in Section 7, we summarize our contribution and discuss a range of directions for further work, including both purely logical aspects and applications to program analysis and verification in the spirit of the work of Ishtiaq, O'Hearn, and Reynolds on Separation Logic [22,35].

2. A logic with separating modalities, LSM

We establish a development of BI's resource semantics [30,33,16,17,6,4,5] that is capable of defining a quite general notion of modality.

Let Prop be a countable set of propositional symbols and Σ_R be a countable set of resource symbols. The language $\mathcal{L}_{\Sigma_R}$ of LSM is defined as follows, where $\mathrm{p} \in \mathrm{Prop}$ and $r \in \Sigma_R$:

$$\begin{aligned}\phi \ ::= \ & \mathrm{p} \mid \top \mid \bot \mid \neg\phi \mid \phi \wedge \phi \mid \phi \vee \phi \mid \phi \to \phi \\ & \mid I \mid \phi * \phi \mid \phi \mathrel{-\!\!*} \phi \\ & \mid \Diamond_r \phi \mid \Box_r \phi\,.\end{aligned}$$

Note that I (resp. $\top$, $\bot$) is the unit of $*$ (resp. $\wedge$, $\vee$). Moreover $r_1 \bullet r_2 \downarrow$ means $r_1 \bullet r_2$ is defined and $r_1 \bullet r_2 \uparrow$ means $r_1 \bullet r_2$ is undefined.

Definition 1 *(Partial resource monoid).* A *partial resource monoid* (PRM) is a structure $\mathcal{M} = (Res, \bullet, e)$, where

1. Res is a set of *resources*
2. $e \in Res$
3. $\bullet : Res \times Res \rightharpoonup Res$ such that, for all $r_1, r_2, r_3 \in Res$,
   - Neutral element: $r_1 \bullet e \downarrow$ and $r_1 \bullet e = r_1$
   - Commutativity: if $r_1 \bullet r_2 \downarrow$, then $r_2 \bullet r_1 \downarrow$ and $r_1 \bullet r_2 = r_2 \bullet r_1$
   - Associativity: if $r_1 \bullet (r_2 \bullet r_3) \downarrow$, then $(r_1 \bullet r_2) \bullet r_3 \downarrow$ and $r_1 \bullet (r_2 \bullet r_3) = (r_1 \bullet r_2) \bullet r_3$.

We call $\bullet$ the *resource composition* and e the *unit resource*.

Definition 2 *(Model).* A $\mathcal{L}_{\Sigma_R}$*-model* is a 4-tuple $\mathcal{K} = (W, \mathcal{M}, \mathbf{R}, V)$, where

1. W is a set of *worlds*,
2. $\mathcal{M} = (Res, \bullet, e)$ is a PRM,
3. $\mathbf{R} \subseteq (W \times Res) \times (W \times Res)$ such that, for all $w_1, w_2, w_3 \in W$ and all $r_1, r_2, r_3 \in Res$,
   - Reflexivity: $(w_1, r_1)\mathbf{R}(w_1, r_1)$
   - Transitivity: if $(w_1, r_1)\mathbf{R}(w_2, r_2)$ and $(w_2, r_2)\mathbf{R}(w_3, r_3)$, then $(w_1, r_1)\mathbf{R}(w_3, r_3)$,
4. Every $r \in \Sigma_R$ has a unique interpretation $[\![r]\!] \in Res$, and
5. $V : \mathrm{Prop} \to \wp(W \times Res)$, with $\wp(S)$ being the power set of S.

$\mathbf{R}$ is called a *reachability relation* and V is called a *valuation*.

Note that the interpretation $[\![-]\!]$ is a partial function such that $[\![e]\!] = e$. Henceforth, we abuse notation and write r for $[\![r]\!]$, neglecting further mention of $[\![-]\!]$ (this is the default approach in process logics, such as Hennessey–Milner logic [21,25,37]). Moreover Definitions 1 and 2 ensure the necessary coherence between modal accessibility and resources.

Definition 3 *(Satisfaction relation, validity).* Let $\mathcal{K} = (W, \mathcal{M}, \mathbf{R}, V)$ be a $\mathcal{L}_{\Sigma_R}$-model. The satisfaction relation $\vDash_{\mathcal{K}} \subseteq W \times Res \times \mathcal{L}_{\Sigma_R}$ is defined by structural induction, for all $w \in W$ and all $r \in Res$, as follows:

$$\begin{array}{rll}
w, r \models_{\mathcal{K}} \mathrm{p} & \text{iff} & (w, r) \in V(\mathrm{p}) \\
w, r \models_{\mathcal{K}} \top & \text{always} & \\
w, r \models_{\mathcal{K}} \bot & \text{never} & \\
w, r \models_{\mathcal{K}} \neg\phi & \text{iff} & w, r \not\models_{\mathcal{K}} \phi \\
w, r \models_{\mathcal{K}} \phi \wedge \psi & \text{iff} & w, r \models_{\mathcal{K}} \phi \text{ and } w, r \models_{\mathcal{K}} \psi \\
w, r \models_{\mathcal{K}} \phi \vee \psi & \text{iff} & w, r \models_{\mathcal{K}} \phi \text{ or } w, r \models_{\mathcal{K}} \psi \\
w, r \models_{\mathcal{K}} \phi \rightarrow \psi & \text{iff} & \text{if } w, r \models_{\mathcal{K}} \phi\text{, then } w, r \models_{\mathcal{K}} \psi \\
 & & \\
w, r \models_{\mathcal{K}} I & \text{iff} & r = e \\
w, r \models_{\mathcal{K}} \phi * \psi & \text{iff} & \text{there exist } r_1, r_2 \in Res \text{ such that} \\
 & & r_1 \bullet r_2 \downarrow, r = r_1 \bullet r_2\text{, and} \\
 & & w, r_1 \models_{\mathcal{K}} \phi \text{ and } w, r_2 \models_{\mathcal{K}} \psi \\
w, r \models_{\mathcal{K}} \phi -\!\!* \psi & \text{iff} & \text{for all } r' \in Res \text{ if } r \bullet r' \downarrow \text{ and } w, r' \models_{\mathcal{K}} \phi, \\
 & & \text{then } w, r \bullet r' \models_{\mathcal{K}} \psi \\
 & & \\
w, r \models_{\mathcal{K}} \Diamond_s\phi & \text{iff} & \text{there exist } w' \in W \text{ and } r' \in Res \text{ such that } r \bullet s \downarrow, \\
 & & (w, r \bullet s)\mathbf{R}(w', r') \text{ and } w', r' \models_{\mathcal{K}} \phi \\
w, r \models_{\mathcal{K}} \Box_s\phi & \text{iff} & \text{for all } w' \in W \text{ and all } r' \in Res\text{, if } r \bullet s \downarrow \text{ and} \\
 & & (w, r \bullet s)\mathbf{R}(w', r')\text{, then } w', r' \models_{\mathcal{K}} \phi
\end{array}$$

We say that a formula ϕ is *valid*, denoted $\models \phi$, if and only if, for all worlds w and all resources r in all models $\mathcal{K}$, $w, r \models_{\mathcal{K}} \phi$. We write $\phi \models \psi$ if and only if, for all worlds w and all resources r in all models $\mathcal{K}$, $w, r \models_{\mathcal{K}} \phi$ implies $w, r \models_{\mathcal{K}} \psi$.

We emphasize that, suppression of the distinction between s and $\llbracket s \rrbracket$ notwithstanding, it is not supposed that $\Sigma_R \subseteq Res$. The judgement $w, r \models_{\mathcal{K}} \Diamond_s\phi$ is defined only if $r \bullet s\downarrow$ and then only if $\llbracket s \rrbracket \in Res$. In other words, we consider that the meaning of $w, r \models_{\mathcal{K}} \Diamond_s\phi$ is: 's is a resource (such that $\llbracket s \rrbracket \in Res$) which can be composed with r ($r \bullet s\downarrow$) and if we compose these resources, then the system can reach a world w' and a resource r' ($(w, r \bullet s)\mathbf{R}(w', r')$) satisfying ϕ ($w', r' \models_{\mathcal{K}} \phi$).

The language of LSM can be extended with the two modalities described in Section 1.

Definition 4 *(Additional modalities)*. For a given Σ_R, the language $\mathcal{L}_{\Sigma_R}$ can be extended as follows:

$$\begin{array}{rl}
\phi ::= & \ldots \mid \Diamond\phi \mid \Box\phi \\
 & \mid \Diamond_\bullet\phi \mid \Box_\bullet\phi
\end{array}$$

The satisfaction relation given in Definition 3 can be extended to define these additional modalities.

Definition 5 *(Satisfaction for the additional modalities)*. The satisfaction relation of the additional modalities of Definition 4 is defined by the following extension of Definition 3:

$$\begin{array}{rll}
w, r \models_{\mathcal{K}} \Diamond\phi & \text{iff} & \text{there exist } w' \in W \text{ and } r' \in Res \text{ such that } (w, r)\mathbf{R}(w', r') \\
 & & \text{and } w', r' \models_{\mathcal{K}} \phi \\
w, r \models_{\mathcal{K}} \Box\phi & \text{iff} & \text{for all } w' \in W \text{ and all } r' \in Res\text{, if } (w, r)\mathbf{R}(w', r') \text{ then} \\
 & & w', r' \models_{\mathcal{K}} \phi \\
w, r \models_{\mathcal{K}} \Diamond_\bullet\phi & \text{iff} & \text{there exist } w' \in W \text{ and } s, r' \in Res \text{ such that } r \bullet s \downarrow, \\
 & & (w, r \bullet s)\mathbf{R}(w', r')\text{, and } w', r' \models_{\mathcal{K}} \phi \\
w, r \models_{\mathcal{K}} \Box_\bullet\phi & \text{iff} & \text{for all } w' \in W \text{ and all } s, r' \in Res\text{, if } (r \bullet s \downarrow \text{ and} \\
 & & (w, r \bullet s)\mathbf{R}(w', r')) \text{ then } w', r' \models_{\mathcal{K}} \phi
\end{array}$$

The pairs modalities $\Diamond$ and $\Box$ (S4) and $\Diamond_\bullet$ and $\Box_\bullet$ can both be derived from the modalities $\Diamond_s$ and $\Box_s$. For any ϕ, ψ in some given $\mathcal{L}_{\Sigma_R}$, we write $\phi \equiv \psi$ if and only if $\phi \models \psi$ and $\psi \models \phi$.

Lemma 6. *The following equivalences hold:*

1. $\Diamond\phi \equiv \Diamond_e\phi$ *and* $\Box\phi \equiv \Box_e\phi$*;*
2. $\Diamond_\bullet\phi \equiv \neg(\top -\!\!* \neg\Diamond_e\phi)$ *and* $\Box_\bullet\phi \equiv \top -\!\!* \Box_e\phi$*.*

Proof. Straightforward applications of the relevant cases of the satisfaction relation. □

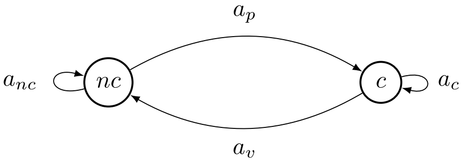

Fig. 1. Example of processes in mutual exclusion.

3. The expressiveness of LSM

We consider, in this section, some examples that are intended to illustrate the uses and expressiveness of LSM. First, we illustrate the interest and use of LSM's modalities, in the context of systems and security, by considering the mutual exclusion and producer–consumer problems, revisiting examples considered in [6,4,5,9]. Then, we consider the relative expressiveness of the three modalities and show that, for example, they allow us to eliminate ambiguities occurring in the expression 'to be able to'.

3.1. Mutual exclusion

We consider two processes (P_1 and P_2) that are in mutual exclusion. The automaton that describes the behaviour of the processes is given in Fig. 1.

The processes have two states: nc, meaning that the process is in the non-critical section; and c, meaning that it is in the critical section. We denote by $\mathcal{S} = \{nc, c\}$ the state set of the processes.

In order to enter into the critical section, a process must hold a token, denoted J, and it releases the token when it leaves the critical section. The processes can perform four actions: a_{nc} a non-critical action, a_c a critical action, a_p the action that consists in taking a token and a_v the action that consists in releasing a token. We denote by $\mathcal{A} = \{a_{nc}, a_c, a_p, a_v\}$ the action set that can be performed by the processes.

We represent the resources (the token J) with $\mathcal{M} = (\{J^n \mid n \in \mathbb{N}\}, +, J^0)$, where $J^m + J^n = J^{m+n}$. In other words, J^n represents n tokens that are available for the system (the processes P_1 and P_2). We remark that $\mathcal{M}$ is obviously a PRM. Now, we need a function that captures resource consumption and production when an action is performed. Following the approach taken in [6,4,5], based on an idea first considered for MBI in [32], we define a partial function $\mu : \mathcal{A} \times \{J^n \mid n \in \mathbb{N}\} \rightharpoonup \{J^n \mid n \in \mathbb{N}\}$ such that

$$\mu(a, J^n) = \begin{cases} J^n & \text{if } a \in \{a_{nc}, a_c\} \\ J^{n+1} & \text{if } a = a_v \\ J^{n-1} & \text{if } a = a_p \text{ and } n \geqslant 1 \\ \uparrow & \text{if } a = a_p \text{ and } n = 0 \end{cases}$$

where ↑ means 'undefined' and ↓ means 'defined'. We remark that performing a critical or a non-critical action (a_c and a_{nc}) consumes and produces no token, releasing a token (a_v) produces a token (J^{n+1}) and taking a token (a_p) consumes a token (J^{n-1}). Of course, $\mu(a_p, J^n)$ is defined if and only if there is at least one available token ($n \geqslant 1$). We introduce a relation that captures the transitions of a process and their effects on the available resources: $s, J^n \xrightarrow{a} s', J^m$ iff $s \xrightarrow{a} s'$ is a transition of Fig. 1, $\mu(a, J^n)\downarrow$ and $\mu(a, J^n) = J^m$. For instance, we have $nc, J^1 \xrightarrow{a_p} c, J^0$, but $nc, J^1 \xrightarrow{a_v} c, J^0$ does not hold (because there is no transition $nc \xrightarrow{a_v} c$ in the automaton of Fig. 1). This relation is really closed to the spirit of the judgements introduced in the SCRP calculus [6,4,5], which are of the form $R, E \xrightarrow{a} R', E'$, meaning that a process E performs an action a on a resource R and then provides the resource R' and the process E'. In order to deal with concurrent transitions, we need to define a set of concurrent states $W = \{s_1\#s_2 \mid s_1, s_2 \in \mathcal{S}\}$ (where s_i is the state of the process P_i), a set of concurrent actions $\mathcal{A}^\# = \{a_1\#a_2 \mid a_1, a_2 \in \mathcal{A}\}$ (where a_i is the action performed by the process P_i) and the following relation: $s_1\#s_2, J^{n_1} + J^{n_2} \overset{a_1\#a_2}{\Longrightarrow} s'_1\#s'_2, J^{m_1} + J^{m_2}$ if and only if $s_1, J^{n_1} \xrightarrow{a_1} s'_1, J^{m_1}$ and $s_2, J^{n_2} \xrightarrow{a_2} s'_2, J^{m_2}$.

For example, the concurrent state $nc\#c$ is a state that captures P_1 in state nc and P_2 in state c. Moreover, the concurrent action $a_c\#a_p$ represents P_1 performing the action a_c and P_2 performing the action a_p. Concerning the relation $\Longrightarrow$, as $nc, J^1 \xrightarrow{a_p} c, J^0$ and $nc, J^0 \xrightarrow{a_{nc}} nc, J^0$ hold, then we have $nc\#nc, J^1 + J^0 \overset{a_p\#a_{nc}}{\Longrightarrow} c\#nc, J^0 + J^0$. Thus $nc\#nc, J^1 \overset{a_p\#a_{nc}}{\Longrightarrow} c\#nc, J^0$.

We are able to model the behaviour of the processes P_1 and P_2 and the token manipulation using the following LSM model $\mathcal{K} = (W, \mathcal{M}, \mathbf{R}, V)$, where

- $W = \{s_1\#s_2 \mid s_1, s_2 \in \mathcal{S}\}$,
- $\mathcal{M} = (\{J^n \mid n \in \mathbb{N}\}, +, J^0)$,
- $\mathbf{R}$ is the reflexive and transitive closure of $\Longrightarrow$, and
- V is defined by

p	$(w, r) \in V(\mathrm{p})$ iff
J	$r = J^1$
nc_1	$w = nc\#nc$ or $w = nc\#c$
nc_2	$w = nc\#nc$ or $w = c\#nc$
c_1	$w = c\#nc$ or $w = c\#c$
c_2	$w = nc\#c$ or $w = c\#c$

We illustrate **R**. As $c\#nc, J^0 \overset{a_v\#a_{nc}}{\Longrightarrow} nc\#nc, J^1$ and $nc\#nc, J^1 \overset{a_{nc}\#a_p}{\Longrightarrow} nc\#c, J^0$ hold, then $(c\#nc, J^0)\mathbf{R}(nc\#nc, J^1)$ and $(nc\#nc, J^1)\mathbf{R}(nc\#c, J^0)$. By transitive closure, we have $(c\#nc, J^0)\mathbf{R}(nc\#c, J^0)$. Concerning the valuation V, J is the proposition meaning that there is one and only one available token, c_i is the proposition meaning that the process P_i is in critical section and nc_i is the proposition meaning that the process P_i is not in critical section.

We consider that the initial state of the system is $nc\#nc$ (each process is in non-critical section) and there is only one available token (J). We can obviously express that, in this initial state, each process is in non-critical section and there is only one available token as follows: $nc\#nc, J \vDash_{\mathcal{K}} nc_1 \wedge nc_2 \wedge J$.

The first important point is that LSM is a modal logic and it is possible to express properties on reachable states and available tokens. For example, we can express that it is impossible that the processes will be together in critical section: $nc\#nc, J \vDash_{\mathcal{K}} \neg\Diamond(c_1 \wedge c_2)$ and also that it is always possible that each process can enter in critical section: $nc\#nc, J \vDash_{\mathcal{K}} \Box\Diamond c_1 \wedge \Box\Diamond c_2$.

The second important point is that LSM is a modal logic extended with the resource composition (denoted $\bullet$) that allows us to express properties of resources on the tokens that are produced and consumed. In particular, we can express that, in any reachable state, it is impossible that there can be more than one available token: $nc\#nc, J \vDash_{\mathcal{K}} \Box\neg(J * J * \top)$. It is also possible to express that if one process is in a non-critical section, then there is no available token $nc\#nc, J \vDash_{\mathcal{K}} \Box((c_1 \vee c_2) \to I)$. Indeed, only the unit resource satisfies I and, in our example, this unit resource is J^0 which encodes no available token.

Notice that the formula $\neg\Diamond(c_1 \wedge c_2)$, with the S4-like modality, fails to capture a vulnerability in the system. This security breach is highlighted by the new modalities: $nc\#nc, J \nvDash_{\mathcal{K}} \neg\Diamond_{\bullet}(c_1 \wedge c_2)$. Indeed, if we assume that an intruder introduces one token in our system, then both processes can enter the critical section, because of the presence of a second token: $nc\#nc, J^1 + J^1 \overset{a_p\#a_p}{\Longrightarrow} c\#c, J^0$.

It follows that we can identify a new solution for the mutual exclusion problem such that $nc\#nc, J \vDash_{\mathcal{K}} \neg\Diamond_{\bullet}(c_1 \wedge c_2)$; that is, such that the processes cannot both enter into the critical section, whatever number of tokens is added.

3.2. Producer–consumer

We propose here another example based on the producer–consumer problem, but with a different approach: one in which the set of worlds W encodes the actions that the processes are performing and does not encode the current state of the processes. In this example, we consider two processes: a producer P_p and a consumer P_c that manipulate resources represented with $\mathcal{M} = (\{R^n \mid n \in \mathbb{N}\}, +, R^0)$, just as in the previous example.

The producer can perform just two actions: p (it is producing a new resource) and np (it is not producing). The consumer can also perform only two actions, which are c (it is consuming a resource) and nc (it is not consuming). Thus $W = \{p\#c, np\#c, p\#nc, np\#nc\}$ is the set of all concurrent actions that can be performed by the processes.

For instance, $p\#nc$ means that P_p is producing (p) and P_c is not consuming (nc). Clearly, only the following transitions hold, for all $w \in W$:

1. $np\#nc, R^n \Longrightarrow w, R^n$;
2. $p\#c, R^n \Longrightarrow w, R^n$;
3. $np\#c, R^n \Longrightarrow w, R^{n-1}$ only if $n \geqslant 1$; and
4. $p\#nc, R^n \Longrightarrow w, R^{n+1}$.

We remark that $np\#c, R^n \Longrightarrow w, R^{n-1}$ holds only if $n \geqslant 1$. Indeed, if there is no resource (R^0) and if P_p does not produce a new resource (np) then P_c cannot consume a resource (c).

Concerning the relation **R**, we consider the reflexive and transitive closure of $\Longrightarrow$. Like in the previous example, we are able to propose a model for this system, that is $\mathcal{K} = (W, \mathcal{M}, \mathbf{R}, V)$ such that V is defined by

p	$(w, r) \in V(\mathrm{p})$ iff
R	$r = R^1$
np	$w = np\#nc$ or $w = np\#c$
p	$w = p\#nc$ or $w = p\#c$
nc	$w = np\#nc$ or $w = p\#nc$
c	$w = np\#c$ or $w = p\#c$

In this model, by definition of $\mathbf{R}$ and reflexivity, $(np\#c, R^0)\mathbf{R}(w, R^n)$ only if $w = np\#c$ and $n = 0$, and we can express that if there is no resource (R^0), if P_p is not producing a new resource, and if P_c is consuming a resource, then the system is blocked (it never changes its state). In LSM, we can express this property as follows, for any $w \in W$ and any $n \in \mathbb{N}$: $w, R^n \vDash_{\mathcal{K}} \Box((I \wedge np \wedge c) \to \Box(I \wedge np \wedge c))$. It means that, for all reachable states (pairs of world/resource) and starting from any state, if there is no resource (I) and if P_p is not producing a new resource (np) and if P_c is consuming a resource (c) then the system always remains in this state ($\Box(I \wedge np \wedge c)$). Now, using multiplicative modalities, we can express that it is possible to unblock the system adding a resource as follows: $w, R^n \vDash_{\mathcal{K}} \Box((I \wedge np \wedge c) \to \Diamond_{\bullet}\neg(I \wedge np \wedge c))$.

3.3. Expressiveness of the modalities

We consider here the relative expressiveness of the three kinds of modalities, and observe that these modalities eliminate ambiguities concerning the assumptions require to support the expression ‘to be able to’.

In this example, we consider three agents that are A_1, A_2, and A_3 and also one action *act*. We suppose that A_1 and A_2 are able to perform the action *act*, but A_3 is not able to perform it. We consider the set of resources $Res = \{R^n \mid n \in \mathbb{N}\}$, where R^n means n occurrences of R, and the resource composition $+$ defined by $R^m + R^n = R^{m+n}$. In this example, the agents want to achieve the goal G, which consists in performing the action *act*. In order to perform this action, the agent A_1 needs no resource and A_2 needs two resources (we recall that A_3 cannot perform the action *act*). Then, we propose three LSM models, one for each agent, that are, for $i \in \{1, 2, 3\}$, $\mathcal{K}_i = (\{a_i, G_i\}, \mathcal{M}, \mathbf{R}_i, V_i)$, where a_i is the agent A_i in his initial state and G_i is A_i that has achieved the goal G, $\mathcal{M} = (Res, +, R^0)$, $\mathbf{R}_i$ are the reflexive and transitive closure of

- $(a_1, R^n)\mathbf{R}_1(G_1, R^n)$, for all $n \in \mathbb{N}$
- $(a_2, R^n)\mathbf{R}_2(G_2, R^{n-2})$, for all $n \geqslant 2$
- $(a_3, R^n)\mathbf{R}_3(G_3, R^m)$ never holds for all $n, m \in \mathbb{N}$

and V_i is defined by $(w, r) \in V_i(P_G)$ iff $w = G_i$.

Now, we consider the agents being in their initial states and trying to achieve the goal without resource. Then the question is: ‘which agent is able to achieve G?’. As we observe that

- $a_1, R^0 \vDash_{\mathcal{K}_1} \Diamond P_G$,
- $a_2, R^0 \vDash_{\mathcal{K}_2} \neg\Diamond P_G$, and
- $a_3, R^0 \vDash_{\mathcal{K}_3} \neg\Diamond P_G$,

we can see that only A_1 is able to achieve the goal; the other agents are not. We remark also, however, that the question is ambiguous. Indeed, A_2 is also able to achieve G, because it is able to perform the action *act*, but it needs more resources to do it.

Then, the question of which agent is able to achieve G (whatever the resources provided to the agent) can be viewed as a second meaning of the question. LSM allows us to express this second meaning:

- $a_1, R^0 \vDash_{\mathcal{K}_1} \Diamond_{\bullet} P_G$;
- $a_2, R^0 \vDash_{\mathcal{K}_2} \Diamond_{\bullet} P_G$;
- $a_3, R^0 \vDash_{\mathcal{K}_3} \neg\Diamond_{\bullet} P_G$.

We observe that a_3 is not able to achieve G, whatever the quantity of resources provided. Finally, we can be more precise, expressing that A_1 needs no more resource to achieve G but A_2 needs two more resources as follows: $a_1, R^0 \vDash_{\mathcal{K}_1} \Diamond_{R^0} P_G$ and $a_2, R^0 \vDash_{\mathcal{K}_2} \Diamond_{R^2} P_G$.

In this example, we give three models, one for each agent. An alternative, that might be developed in future work, would be to internalize agents in the syntax of LSM (as a modality parameter) in the spirit of epistemic logics [38,10]. Moreover, we will study the relationships of our logic with some propositional dynamic logics [20].

4. LSM and timed Petri nets

We complete our set of examples of the uses of LSM’s modalities by showing that LSM can conveniently express properties of rich models of concurrent and distributed computation; that is, timed Petri nets (TPN) [24,1]. This example builds on the spirit of Winskel’s work on Petri net semantics for intuitionistic linear logic [13,14] and O’Hearn and Yang’s Petri net semantics of BI [29].

Timed Petri nets are a model of computation that can describe distributed systems, concurrency, production and consumption of resources. In these models, resources are represented by *places* and the consumption and production of resources is captured by *transitions*. We describe the amount of resources using multisets, a multiset over a finite set P being a function $M : P \to \mathbb{N}$. We say that M is a finite multiset iff $\sum_{p \in P} M(p) \in \mathbb{N}$. We denote by $\mathfrak{M}_P$ the set of finite multisets over P.

Definition 7 *(Petri net).* A *Petri net* is a 4-tuple $\mathcal{P} = (P, T, pre, post)$ such that P is a finite set of *places*, T is a finite set of *transitions*, and pre and $post$ are two functions $T \to \mathfrak{M}_P$.

The markings are denoted $[p_1, \ldots, p_n]$, where p_i are places. For instance, the marking $M = [p_1, p_2, p_2]$ is the function such that $M(p_1) = 1$, $M(p_2) = 2$ and $M(p_i) = 0$ for all $p_i \in P \setminus \{p_1, p_2\}$. In this example we can say that there are two *tokens* in the place p_2 and one *token* in p_1. $[]$ is the empty marking, that is $[](p) = 0$, for all $p \in P$.

The marking addition $M + N$ is defined by $(M + N)(p_i) = M(p_i) + N(p_i)$ for all $p_i \in P$. We say that M is a *submarking* of N, denoted $M \leq N$, iff $M(p_i) \leqslant N(p_i)$ for all $p_i \in P$. We also define the marking subtraction $M - N$ by $(M - N)(p_i) = M(p_i) - N(p_i)$ for all $p_i \in P$, and we remark that $M - N$ is defined if and only if $N \leq M$.

When a transition t_i is fired, resources are consumed, given by $pre(t_i)$, and also produced, given by $post(t_i)$. We denote by $M \xrightarrow{t_i} N$ when the marking (the resources) M, after firing the transition t_i, becomes the marking N. Thus, we have $M \xrightarrow{t_i} N$ iff $pre(t_i) \leq M$ and $N = M - pre(t_i) + post(t_i)$. We say that the transition t_i is *enabled* for the marking M iff $pre(t_i) \leq M$. Sometimes, when we considered implicitly a marking M, we will say that t_i is enabled, rather than t_i is enabled for M. Considering a marking M, we denote by $T_{/M}$ the set of all transitions that are enabled for M.

Definition 8 *(Timed Petri net).* A *timed Petri net* is a 6-tuple $\mathcal{T} = (P, T, pre, post, \alpha, \beta)$ such that $(P, T, pre, post)$ is a Petri net, $\alpha : T \to \mathbb{R}^+$ and $\beta : T \to \mathbb{R}^+ \cup \{\infty\}$

Timed Petri nets, denoted TPN, are particular Petri nets in which each transition t_i has an associated time interval $[\alpha(t_i), \beta(t_i)]$. These intervals capture the delay and duration of transition firing. For instance, if the interval $[2, 5]$ is associated with the transition t_i, then it means that if t_i becomes enabled at time θ and t_i stays continuously enabled then t_i may be fired after time $\theta + 2$ and must be fired before time $\theta + 5$. Thus, in order to capture time elapsing, implicit clocks $\nu : T \to \mathbb{R}^+$ are considered. For example, if the current time is θ and $\nu(t_i) = 2$, then it means that t_i becomes enabled at time $\theta - 2$ and remains continuously enabled until now. Moreover, if a transition t_i is not enabled, then we have $\nu(t_i) = 0$ and the value of the implicit clock of t_i remains equal to 0 until t_i becomes enabled.

In other words, $\nu(t_i)$ can be viewed as a chronometer which starts when the transition t_i becomes enabled and which is reset to 0 when the transition becomes disabled or is fired. We define $\nu' = \nu + d$ the function such that, for all $t_i \in T_{/M}$, we have $\nu'(t_i) = \nu(t_i) + d$.

Therefore, in TPN, there is a transition relation dealing with time elapsing and another one dealing with transition firing:

- Time elapsing d: $(\nu, M) \xrightarrow{d} (\nu + d, M)$ iff $\forall t_i \in T_{/M} \cdot \nu(t_i) + d \leqslant \beta(t_i)$
- Transition firing t_i: $(\nu, M) \xrightarrow{t_i} (\nu', N)$ iff $M \xrightarrow{t_i} N$, $\nu(t_i) \geqslant \alpha(t_i)$, and

$$\forall t_j \in T \cdot \nu'(t_j) = \begin{cases} 0 & \text{if } t_j \notin T_{/N} \text{ or } t_i = t_j \text{ or} \\ & t_j \notin T_{/(M - pre(t_i))} \\ \nu(t_j) & \text{otherwise.} \end{cases}$$

We remark that it is not allowed for time to elapse in such a way that an implicit clock of an enabled transition t_i becomes greater than $\beta(t_i)$ and then $\forall t_i \in T_{/M} \cdot \nu(t_i) + d \leqslant \beta(t_i)$.

We also note that, when time elapses, only implicit clocks of enabled transitions are increased, by definition of $\nu + d$. Concerning a transition firing $(\nu, M) \xrightarrow{t_i} (\nu', N)$, we remark that, after firing a transition t_i, the implicit clocks are updated as follows:

- An implicit clock of a transition t_j is reset to 0 if t_j is not enabled for the new marking N, that is $t_j \notin T_{/N}$;
- An implicit clock of a transition t_j is reset to 0 if t_j was the fired transition, that is $t_i = t_j$;
- An implicit clock of a transition t_j is reset to 0 if t_j does not stayed continuously enabled, especially during the step of token consumption ($t_j \notin T_{/(M - pre(t_i))}$);
- Otherwise, the implicit clock of a transition t_j does not change its value.

The reachability relation is formally defined as follows: $(\nu, M) \rightsquigarrow (\nu', N)$ iff $(\nu, M) \xrightarrow{a_1} (\nu_1, M_1) \xrightarrow{a_2} \ldots \xrightarrow{a_{n-1}} (\nu_{n-1}, M_{n-1}) \xrightarrow{a_n} (\nu', N)$ for a_i being a delay or a transition. We remark that this relation is obviously transitive and, considering $n = 0$, is reflexive, $(\nu, M) \rightsquigarrow (\nu, M)$.

Considering the TPN of Fig. 2, we see that there are four places ($P = \{p_1, p_2, p_3, p_4\}$) and three transitions ($T = \{t_1, t_2, t_3\}$). Moreover, a time interval is associated with each transition. We have $\alpha(t_3) = 1$ and $\beta(t_3) = 4$, meaning that if t_3 becomes enabled at time θ and remains continuously enabled, then this transition may fire after time $\theta + 1$ and must fire before time $\theta + 4$. We can also observe that $\alpha(t_2) = 2$ and $\beta(t_2) = \infty$, meaning that the transition t_2 may just fire after time $\theta + 2$ (there is no other constraint concerning its firing time).

In this example, we consider that the initial marking is $[p_4, p_4]$. All implicit clocks are initialized to 0, giving $\nu(t_1) = \nu(t_2) = \nu(t_3) = 0$. We use the denotation $\langle 0, 0, 0 \rangle$ to represent the value of all implicit clocks. As $0 \ngeqslant 2$ and $0 \ngeqslant 1$, it is not

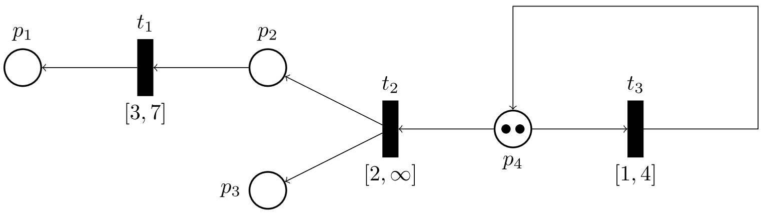

Fig. 2. An example of a timed Petri net.

possible to fire the transition t_2 or t_3. But, it is possible to let time elapse. We have, for example, $(\langle 0,0,0\rangle,[p_4,p_4]) \xrightarrow{1.5} (\langle 0,1.5,1.5\rangle,[p_4,p_4])$. We remark that the implicit clock of t_1 is not equal to 1.5, because this transition is not enabled for $[p_4,p_4]$.

Now, as $\nu(t_3) \geqslant \alpha(t_3)$ $(1.5 \geqslant 1)$, then it is possible to fire the transition t_3. But it is also possible to let time elapse again: $(\langle 0,1.5,1.5\rangle,[p_4,p_4]) \xrightarrow{2} (\langle 0,3.5,3.5\rangle,[p_4,p_4])$. Moreover $(\langle 0,1.5,1.5\rangle,[p_4,p_4]) \xrightarrow{3} (\langle 0,4.5,4.5\rangle,[p_4,p_4])$ does not hold, because we have $\nu(t_3)+d \nleqslant \beta(t_3)$ $(1.5+3 \nleqslant 4)$. In the context $(\langle 0,3.5,3.5\rangle,[p_4,p_4])$, the transitions t_2 and t_3 can fire. If the transition t_2 fires, we have $(\langle 0,3.5,3.5\rangle,[p_4,p_4]) \xrightarrow{t_2} (\langle 0,0,3.5\rangle,[p_2,p_3,p_4])$. We observe that t_1 becomes enabled, the implicit clock of t_2 is initialized to 0 (t_2 is fired) and the implicit clock of t_3 does not change (t_3 remains continuously enabled during this transition).

Now, we suppose that $(\langle 0,0,3.5\rangle,[p_2,p_3,p_4]) \xrightarrow{0.2} (\langle 0.2,0.2,3.7\rangle,[p_2,p_3,p_4])$. If t_3 fires, then we have $(\langle 0.2,0.2,3.7\rangle,[p_2,p_3,p_4]) \xrightarrow{t_3} (\langle 0.2,0,0\rangle,[p_2,p_3,p_4])$ and we remark that the implicit clock of t_2 is initialized to 0 because t_2 does not remain continuously enabled: t_2 was not enabled for the marking $[p_2,p_3,p_4] - pre(t_3) = [p_2,p_3]$. Finally, we have $(\langle 0,0,0\rangle,[p_4,p_4]) \rightsquigarrow (\langle 0.2,0,0\rangle,[p_2,p_3,p_4])$.

Finally we show that LSM is able to express properties on TPN. Let E be any set, we denote by $card(E)$ the cardinality of E, that is the number of elements of E.

Lemma 9. *Let $\mathcal{T} = (P,T,pre,post,\alpha,\beta)$ be a TPN and let*

$$\mathcal{K} = ((\mathbb{R}^+)^{card(T)}, \mathcal{M}, \rightsquigarrow, i())$$

such that $\mathcal{M} = (\mathfrak{M}_P,+,[])$ and $i(p) = \{(\nu,[p]) \mid \nu \in (\mathbb{R}^+)^{card(T)}\}$.
Then $\mathcal{K}$ is a model.

Proof. It is sufficient to verify that $\mathcal{K}$ satisfies Definition 2. □

We consider the following function:

$$\widehat{M} = \begin{cases} I & \text{if } M = [] \\ p_1 * \ldots * p_n & \text{if } M = [p_1,\ldots,p_n] \end{cases}$$

Proposition 10. *Let $\mathcal{T} = (P,T,pre,post,\alpha,\beta)$ be a TPN and let*

$$\mathcal{K} = ((\mathbb{R}^+)^{card(T)}, \mathcal{M}, \rightsquigarrow, i())$$

such that $\mathcal{M} = (\mathfrak{M}_P,+,[])$ and $i(p) = \{(\nu,[p]) \mid \nu \in (\mathbb{R}^+)^{card(T)}\}$. For any implicit clock $\nu \in (\mathbb{R}^+)^{card(T)}$ and any marking $M \in \mathfrak{M}_P$, we have $\nu, M \models_{\mathcal{K}} \widehat{M}$.

Proof. The proof is by induction on n.

- Base case $(n = 0)$. By Lemma 9, $\mathcal{K}$ is a model. Then $\nu,[] \models_{\mathcal{K}} I$, and we have $\nu,[] \models_{\mathcal{K}} \widehat{[]}$.
- Inductive case. We suppose that the Proposition holds for all markings that contain n tokens (induction hypothesis), and then prove it for all markings that contain $n+1$ tokens.
  Let $M = [p_1,\ldots,p_{n+1}]$. By definition, $(\nu,[p_{n+1}]) \in i(p_{n+1})$, then we have $\nu,[p_{n+1}] \models_{\mathcal{K}} p_{n+1}$. By the induction hypothesis (IH), $\nu,[p_1,\ldots,p_n] \models_{\mathcal{K}} p_1 * \ldots * p_n$. As $M = [p_1,\ldots,p_n] + [p_{n+1}]$, we have $\nu,[p_1,\ldots,p_n] + [p_{n+1}] \models_{\mathcal{K}} (p_1 * \ldots * p_n) * p_{n+1}$. Thus $\nu, M \models_{\mathcal{K}} \widehat{M}$. □

We now illustrate properties that can be expressed on TPN by LSM. We consider the TPN of Fig. 2. The initial marking is $[p_4,p_4]$ and the values of the implicit clock are $\langle 0,0,0\rangle$. As $\widehat{[p_4,p_4]} = p_4 * p_4$, by Proposition 10, we have $\langle 0,0,0\rangle,[p_4,p_4] \models_{\mathcal{K}} p_4 * p_4$, which illustrates the use of *separation*. Indeed, $p_4 * p_4$ means that the marking $[p_4,p_4]$ can be separated/decomposed into two submarkings such that the first submarking satisfies p_4 and the second one satisfies p_4 ($[p_4, p_4] = [p_4] + [p_4]$ and $\langle 0, 0, 0\rangle, [p_4] \vDash_{\mathcal{K}} p_4$).

Moreover, $(\langle 0, 0, 0\rangle, [p_4, p_4]) \rightsquigarrow (\langle 0.2, 0, 0\rangle, [p_2, p_3, p_4])$ and we then have that $\langle 0, 0, 0\rangle, [p_4, p_4] \vDash_{\mathcal{K}} \Diamond(p_2 * p_3 * p_4)$, which illustrates the *reachability* relation: $\Diamond\phi$ means that there is a reachable state from $(\langle 0, 0, 0\rangle, [p_4, p_4])$, where a state is a pair composed by an implicit clock and a marking, that satisfies the property ϕ. As we have $\langle 0, 0, 0\rangle, [p_4, p_4] \vDash_{\mathcal{K}} p_4 * p_4$ and $\langle 0, 0, 0\rangle, [p_4, p_4] \vDash_{\mathcal{K}} \Diamond(p_2 * p_3 * p_4)$, we can deduce that $\langle 0, 0, 0\rangle, [p_4, p_4] \vDash_{\mathcal{K}} (p_4 * p_4) \wedge \Diamond(p_2 * p_3 * p_4)$. This formula illustrates the use of *sharing*: the state $(\langle 0, 0, 0\rangle, [p_4, p_4])$ shares two properties that are $p_4 * p_4$ and $\Diamond(p_2 * p_3 * p_4)$.

We illustrate the modality $\Diamond_{\bullet}$. As $(\langle 0, 0, 0\rangle, [p_2]) \xrightarrow{4} (\langle 4, 0, 0\rangle, [p_2]) \xrightarrow{t_1} (\langle 0, 0, 0\rangle, [p_1])$, we have $(\langle 0, 0, 0\rangle, [p_2]) \rightsquigarrow (\langle 0, 0, 0\rangle, [p_1])$ and $\langle 0, 0, 0\rangle, [] \vDash_{\mathcal{K}} \Diamond_{\bullet} p_1$. Here, $\Diamond_{\bullet}\phi$ expresses that the timed Petri net can reach a state that satisfies ϕ, but additional resources (tokens) may be needed to achieve it. This modality is also interesting if it is combined with negation. For example, $\langle 0, 0, 0\rangle, [p_4] \vDash_{\mathcal{K}} \neg\Diamond_{\bullet} p_1$ expresses that it is not possible, whatever the resources/tokens that are added to the timed Petri net, to reach the marking $[p_1]$. Finally, the resource-indexed modality $\Diamond_s\phi$, allows us to express that adding the marking s, the timed Petri net can reach a marking that satisfies ϕ. For instance, we have $\langle 0, 0, 0\rangle, [] \vDash_{\mathcal{K}} \Diamond_{[p_2]} p_1$, because $(\langle 0, 0, 0\rangle, [p_2]) \rightsquigarrow (\langle 0, 0, 0\rangle, [p_1])$.

In conclusion, we have shown that the LSM models are really used to capture reachability in timed Petri nets. This point comes from the multi-dimension of the structures based on pairs (world, resource).

5. Conservativity of LSM over S4

In this section, we show that LSM is a conservative extension of the modal logic S4 (e.g., [3]). More specifically, we show that a formula ϕ is valid in S4 if and only if ϕ is valid in LSM. Then, with the equivalences of Lemma 6, we have that the resource-indexed modalities properly generalize the S4 modalities.

5.1. The logic S4

Let Prop be a countable set of propositional symbols. The language $\mathcal{L}_{S4}$ of S4 is defined as follows, where $\mathrm{p} \in \mathrm{Prop}$:

$$\phi \ ::= \ \mathrm{p} \mid \neg\phi \mid \bot \mid \top \mid \phi \vee \phi \mid \phi \wedge \phi \mid \phi \to \phi \mid \Diamond\phi \mid \Box\phi\,.$$

Definition 11 *(S4-model).* An *S4-model* is a triple $\mathcal{K}_{S4} = (W_{S4}, \mathbf{R}_{S4}, V_{S4})$, where

1. W_{S4} is a set of *worlds*,
2. $\mathbf{R}_{S4} \subseteq W_{S4} \times W_{S4}$ such that, for all $w_1, w_2, w_3 \in W_{S4}$,
   - reflexivity: $w_1 \mathbf{R}_{S4} w_1$, and
   - transitivity: if $w_1 \mathbf{R}_{S4} w_2$ and $w_2 \mathbf{R}_{S4} w_3$, then $w_1 \mathbf{R}_{S4} w_3$, and
3. $V_{S4} : \mathrm{Prop} \to \wp(W_{S4})$.

Definition 12 *(Satisfaction relation, validity).* Let $\mathcal{K}_{S4} = (W_{S4}, \mathbf{R}_{S4}, V_{S4})$ be an S4-model. The satisfaction relation $\Vdash_{\mathcal{K}_{S4}} \subseteq W_{S4} \times \mathcal{L}_{S4}$ is inductively defined, for all $w \in W_{S4}$, as follows:

$$\begin{array}{rcl}
w \Vdash_{\mathcal{K}_{S4}} \mathrm{p} & \text{iff} & w \in V_{S4}(\mathrm{p}) \\
w \Vdash_{\mathcal{K}_{S4}} \top & \text{always} & \\
w \Vdash_{\mathcal{K}_{S4}} \bot & \text{never} & \\
w \Vdash_{\mathcal{K}_{S4}} \neg\phi & \text{iff} & w \not\Vdash_{\mathcal{K}_{S4}} \phi \\
w \Vdash_{\mathcal{K}_{S4}} \phi \wedge \psi & \text{iff} & w \Vdash_{\mathcal{K}_{S4}} \phi \text{ and } w \Vdash_{\mathcal{K}_{S4}} \psi \\
w \Vdash_{\mathcal{K}_{S4}} \phi \vee \psi & \text{iff} & w \Vdash_{\mathcal{K}_{S4}} \phi \text{ or } w \Vdash_{\mathcal{K}_{S4}} \psi \\
w \Vdash_{\mathcal{K}_{S4}} \phi \to \psi & \text{iff} & \text{if } w \Vdash_{\mathcal{K}_{S4}} \phi\text{, then } w \Vdash_{\mathcal{K}_{S4}} \psi \\
w \Vdash_{\mathcal{K}_{S4}} \Diamond\phi & \text{iff} & \text{there exists } w' \in W_{S4} \text{ such that} \\
 & & w\mathbf{R}_{S4}w' \text{ and } w' \Vdash_{\mathcal{K}_{S4}} \phi \\
w \Vdash_{\mathcal{K}_{S4}} \Box\phi & \text{iff} & \text{for all } w' \in W_{S4}\text{, if } w\mathbf{R}_{S4}w'\text{, then} \\
 & & w' \Vdash_{\mathcal{K}_{S4}} \phi
\end{array}$$

A formula ϕ is *valid*, denoted $\Vdash \phi$, if and only if, for all worlds w in all models $\mathcal{K}_{S4}$, $w \Vdash_{\mathcal{K}_{S4}} \phi$.

Now we can establish that LSM is a conservative extension of S4 logic. That is, for any formula $\phi \in \mathcal{L}_{S4}$, we have $\Vdash \phi$ if and only if $\vDash \phi$.

5.2. From LSM-countermodels to S4-countermodels

In this section, we show how to obtain an S4-countermodel from an LSM-countermodel.

Definition 13 *(The function $T_{LSM\rightarrow S4}$).* Let $\mathcal{K} = (W, \mathcal{M}, \mathbf{R}, V)$, where $\mathcal{M} = (Res, \bullet, e)$ is a PRM, be a LSM-model. The function $T_{LSM\rightarrow S4}$ associates to $\mathcal{K}$ the triple $T_{LSM\rightarrow S4}(\mathcal{K}) = (W_{S4}, \mathbf{R}_{S4}, V_{S4})$, such that $W_{S4} = W \times Res$, $\mathbf{R}_{S4} = \mathbf{R}$, and $V_{S4} = V$.

Proposition 14. *Let $\mathcal{K} = (W, \mathcal{M}, \mathbf{R}, V)$, where $\mathcal{M} = (Res, \bullet, e)$ is a PRM, be an LSM-model. $T_{LSM\rightarrow S4}(\mathcal{K}) = (W_{S4}, \mathbf{R}_{S4}, V_{S4})$ is an S4-model.*

Proof. $\mathbf{R}_{S4}$ is reflexive and transitive because $\mathbf{R}$ is reflexive and transitive. □

Proposition 15. *Let $\mathcal{K} = (W, \mathcal{M}, \mathbf{R}, V)$, where $\mathcal{M} = (Res, \bullet, e)$ is a PRM, be a (LSM) model and $T_{LSM\rightarrow S4}(\mathcal{K}) = (W_{S4}, \mathbf{R}_{S4}, V_{S4})$. For any formula $\phi \in \mathcal{L}_{S4}$, any $w \in W$ and any $r \in Res$, we have $w, r \models_{\mathcal{K}} \phi$ iff $(w, r) \Vdash_{\mathcal{K}_{S4}} \phi$.*

Proof. By induction on the structure of ϕ.

- Base cases.
  - Case $w, r \models_{\mathcal{K}} \mathrm{p}$. By definition $(w, r) \in V(\mathrm{p})$ and by definition of $T_{LSM\rightarrow S4}$, $(w, r) \in V_{S4}(\mathrm{p})$. Then $(w, r) \Vdash_{\mathcal{K}_{S4}} \mathrm{p}$.
  - Case $(w, r) \Vdash_{\mathcal{K}_{S4}} \mathrm{p}$. By definition $(w, r) \in V_{S4}(\mathrm{p})$ and by definition of $T_{LSM\rightarrow S4}$, $(w, r) \in V(\mathrm{p})$. Then $w, r \models_{\mathcal{K}} \mathrm{p}$.
  - Case $w, r \models_{\mathcal{K}} \top$. We have $(w, r) \Vdash_{\mathcal{K}_{S4}} \top$, by definition of $\Vdash_{\mathcal{K}_{S4}}$.
  - Case $(w, r) \Vdash_{\mathcal{K}_{S4}} \top$. We have $w, r \models_{\mathcal{K}} \top$, by definition of $\models_{\mathcal{K}}$.
  - Case $w, r \models_{\mathcal{K}} \bot$. This case is absurd, by definition of $\models_{\mathcal{K}}$.
  - Case $(w, r) \Vdash_{\mathcal{K}_{S4}} \bot$. This case is absurd, by definition of $\Vdash_{\mathcal{K}_{S4}}$.
- Inductive cases. We suppose that the proposition holds for formulæ ϕ and ψ (IH).
  - Case $w, r \models_{\mathcal{K}} \neg\phi$. By definition, $w, r \not\models_{\mathcal{K}} \phi$ and by the induction hypothesis, $(w, r) \nVdash_{\mathcal{K}_{S4}} \phi$. Then $(w, r) \Vdash_{\mathcal{K}_{S4}} \neg\phi$.
  - Case $(w, r) \Vdash_{\mathcal{K}_{S4}} \neg\phi$. By definition, $(w, r) \nVdash_{\mathcal{K}_{S4}} \phi$ and by the induction hypothesis, $w, r \not\models_{\mathcal{K}} \phi$. Then $w, r \models_{\mathcal{K}} \neg\phi$.
  - Case $w, r \models_{\mathcal{K}} \phi \wedge \psi$. By definition, $w, r \models_{\mathcal{K}} \phi$ and $w, r \models_{\mathcal{K}} \psi$. By the induction hypothesis, $(w, r) \Vdash_{\mathcal{K}_{S4}} \phi$ and $(w, r) \Vdash_{\mathcal{K}_{S4}} \psi$. Then $(w, r) \Vdash_{\mathcal{K}_{S4}} \phi \wedge \psi$.
  - Case $(w, r) \Vdash_{\mathcal{K}_{S4}} \phi \wedge \psi$. By definition, $(w, r) \Vdash_{\mathcal{K}_{S4}} \phi$ and $(w, r) \Vdash_{\mathcal{K}_{S4}} \psi$. By the induction hypothesis, $w, r \models_{\mathcal{K}} \phi$ and $w, r \models_{\mathcal{K}} \psi$. Then $w, r \models_{\mathcal{K}} \phi \wedge \psi$.
  - Case $w, r \models_{\mathcal{K}} \Diamond\phi$. By definition, there are $w' \in W$ and $r' \in Res$ such that $(w, r)\mathbf{R}(w', r')$ and $w', r' \models_{\mathcal{K}} \phi$. By definition of $T_{LSM\rightarrow S4}$ and by the induction hypothesis, there is $(w', r') \in W_{S4}$ such that $(w, r)\mathbf{R}_{S4}(w', r')$ and $(w', r') \Vdash_{\mathcal{K}_{S4}} \phi$. Then $(w, r) \Vdash_{\mathcal{K}_{S4}} \Diamond\phi$.
  - Case $(w, r) \Vdash_{\mathcal{K}_{S4}} \Diamond\phi$. By definition, there is $(w', r') \in W_{S4}$ such that $(w, r)\mathbf{R}_{S4}(w', r')$ and $(w', r') \Vdash_{\mathcal{K}_{S4}} \phi$. By inductive hypothesis and by construction, there are $w' \in W$ and $r' \in Res$ such that $(w, r)\mathbf{R}(w', r')$ and $w', r' \models_{\mathcal{K}} \phi$. Then $w, r \models_{\mathcal{K}} \Diamond\phi$.
  - Case $w, r \models_{\mathcal{K}} \Box\phi$. Let $(w', r') \in W_{S4}$ such that $(w, r)\mathbf{R}_{S4}(w', r')$. By definition of $T_{LSM\rightarrow S4}$, we have $(w, r)\mathbf{R}(w', r')$. Then, as $w, r \models_{\mathcal{K}} \Box\phi$ then we have $w', r' \models_{\mathcal{K}} \phi$. Then, by the induction hypothesis, $(w', r') \Vdash_{\mathcal{K}_{S4}} \phi$ and we have $(w, r) \Vdash_{\mathcal{K}_{S4}} \Box\phi$.
  - Case $(w, r) \Vdash_{\mathcal{K}_{S4}} \Box\phi$. Let $w' \in W$ and $r' \in Res$ such that $(w, r)\mathbf{R}(w', r')$. By definition of $T_{LSM\rightarrow S4}$, $(w, r)\mathbf{R}_{S4}(w', r')$. Then, as $(w, r) \Vdash_{\mathcal{K}_{S4}} \Box\phi$ we have $(w', r') \Vdash_{\mathcal{K}_{S4}} \phi$. Then, by the induction hypothesis, $w', r' \models_{\mathcal{K}} \phi$. and we have $w, r \models_{\mathcal{K}} \Box\phi$.
  - The other cases are similar. □

Lemma 16. *Let ϕ be a formula of $\mathcal{L}_{S4}$. If $\Vdash \phi$, then $\models \phi$.*

Proof. We show that if $\not\models \phi$, then $\nVdash \phi$. We suppose that ϕ is not valid in LSM logic. Then there exists a countermodel $\mathcal{K} = (W, \mathcal{M}, \mathbf{R}, V)$, where $\mathcal{M} = (Res, \bullet, e)$, $w \in W$ and $r \in Res$ such that $w, r \not\models_{\mathcal{K}} \phi$. Now, we consider $T_{LSM\rightarrow S4}(\mathcal{K}) = (W_{S4}, \mathbf{R}_{S4}, V_{S4})$. By Proposition 14, it is an S4-model. By Proposition 15, $(w, r) \nVdash_{T_{LSM\rightarrow S4}(\mathcal{K})} \phi$. Thus ϕ is not valid in S4 logic. Therefore if $\not\models \phi$ then $\nVdash \phi$. Thus, if $\Vdash \phi$, then $\models \phi$. □

5.3. From S4-countermodels to LSM-countermodels

We show how to obtain an LSM-countermodel from an S4-countermodel.

Definition 17 *(Function $T_{S4\rightarrow LSM}$).* Let $\mathcal{K}_{S4} = (W_{S4}, \mathbf{R}_{S4}, V_{S4})$ be a S4-model. The function $T_{S4\rightarrow LSM}$ associates to $\mathcal{K}_{S4}$ the 4-tuple $T_{S4\rightarrow LSM}(\mathcal{K}_{S4}) = (W, \mathcal{M}, \mathbf{R}, V)$, where $\mathcal{M} = (Res, \bullet, e)$, such that

1. $W = W_{S4}$,
2. $Res = \{e\}$, where e is any element,
3. $\bullet : Res \times Res \rightharpoonup Res$ is defined by $e \bullet e = e$,
4. $(w, e)\mathbf{R}(w', e)$ iff $w\mathbf{R}_{S4}w'$, and
5. $(w, e) \in V(p)$ iff $w \in V_{S4}(p)$.

Proposition 18. *Let $\mathcal{K}_{S4} = (W_{S4}, \mathbf{R}_{S4}, V_{S4})$ be a S4-model. $T_{S4 \to LSM}(\mathcal{K}_{S4}) = (W, \mathcal{M}, \mathbf{R}, V)$, where $\mathcal{M} = (Res, \bullet, e)$, is a (LSM) model.*

Proof. $\mathcal{M}$ is a PRM and $\mathbf{R}$ is reflexive and transitive, because $\mathbf{R}_{S4}$ is reflexive and transitive. □

Proposition 19. *Let $\mathcal{K}_{S4} = (W_{S4}, \mathbf{R}_{S4}, V_{S4})$ be an S4-model and let*

$$T_{S4 \to LSM}(\mathcal{K}_{S4}) = (W, \mathcal{M}, \mathbf{R}, V),$$

where $\mathcal{M} = (Res, \bullet, e)$. For any formula $\phi \in \mathcal{L}_{S4}$ and any $w \in W_{S4}$, we have $w \Vdash_{\mathcal{K}_{S4}} \phi$ iff $w, e \vDash_{\mathcal{K}} \phi$.

Proof. By induction on the structure of ϕ.

- Base cases.
  - Case $w \Vdash_{\mathcal{K}_{S4}}$ p. By definition, $w \in V_{S4}(\mathrm{p})$ and by definition of $T_{S4 \to LSM}$, $(w, e) \in V(\mathrm{p})$. Then $w, e \vDash_{\mathcal{K}}$ p.
  - Case $w, e \vDash_{\mathcal{K}}$ p. By definition, $(w, e) \in V(\mathrm{p})$ and by definition of $T_{S4 \to LSM}$, $w \in V_{S4}(\mathrm{p})$. Then $w \Vdash_{\mathcal{K}_{S4}}$ p.
  - Case $w \Vdash_{\mathcal{K}_{S4}} \top$. We have $w, e \vDash_{\mathcal{K}} \top$, by definition of $\vDash_{\mathcal{K}}$.
  - Case $w, e \vDash_{\mathcal{K}} \top$. We have $w \Vdash_{\mathcal{K}_{S4}} \top$, by definition of $\Vdash_{\mathcal{K}_{S4}}$.
  - Case $w \Vdash_{\mathcal{K}_{S4}} \bot$. This case is absurd, by definition of $\Vdash_{\mathcal{K}_{S4}}$.
  - Case $w, e \vDash_{\mathcal{K}} \bot$. This case is absurd, by definition of $\vDash_{\mathcal{K}}$.
- Inductive cases. We suppose that this proposition holds for formulæ ϕ and ψ (this is the induction hypothesis).
  - Case $w \Vdash_{\mathcal{K}_{S4}} \neg\phi$. By definition, $w \nVdash_{\mathcal{K}_{S4}} \phi$ and by the induction hypothesis, $w, e \nvDash_{\mathcal{K}} \phi$. Then $w, e \vDash_{\mathcal{K}} \neg\phi$.
  - Case $w, e \vDash_{\mathcal{K}} \neg\phi$. By definition, $w, e \nvDash_{\mathcal{K}} \phi$ and by the induction hypothesis, $w \nVdash_{\mathcal{K}_{S4}} \phi$. Then $w \Vdash_{\mathcal{K}_{S4}} \neg\phi$.
  - Case $w \Vdash_{\mathcal{K}_{S4}} \phi \wedge \psi$. By definition, $w \Vdash_{\mathcal{K}_{S4}} \phi$ and $w \Vdash_{\mathcal{K}_{S4}} \psi$. By the induction hypothesis, $w, e \vDash_{\mathcal{K}} \phi$ and $w, e \vDash_{\mathcal{K}} \psi$. Then $w, e \vDash_{\mathcal{K}} \phi \wedge \psi$.
  - Case $w, e \vDash_{\mathcal{K}} \phi \wedge \psi$. By definition, $w, e \vDash_{\mathcal{K}} \phi$ and $w, e \vDash_{\mathcal{K}} \psi$. By the induction hypothesis, $w \Vdash_{\mathcal{K}_{S4}} \phi$ and $w \Vdash_{\mathcal{K}_{S4}} \psi$. Then $w \Vdash_{\mathcal{K}_{S4}} \phi \wedge \psi$.
  - Case $w \Vdash_{\mathcal{K}_{S4}} \Diamond\phi$. By definition, there is $w' \in W_{S4}$ such that $w\mathbf{R}_{S4}w'$ and $w' \Vdash_{\mathcal{K}_{S4}} \phi$. By the induction hypothesis and by construction, there is $w' \in W$ such that $(w, e)\mathbf{R}(w', e)$ and $w', e \vDash_{\mathcal{K}} \phi$. Then $w, e \vDash_{\mathcal{K}} \Diamond\phi$.
  - Case $w, e \vDash_{\mathcal{K}} \Diamond\phi$. By definition, there are $w' \in W$ and $r' \in Res$ such that $(w, e)\mathbf{R}(w', r')$ and $w', r' \vDash_{\mathcal{K}} \phi$. As $Res = \{e\}$, by definition of $T_{S4 \to LSM}$, we have $r' = e$. Then $(w, e)\mathbf{R}(w', e)$ and $w', e \vDash_{\mathcal{K}} \phi$. By definition of $T_{S4 \to LSM}$ and by the induction hypothesis, there is $w' \in W_{S4}$ such that $w\mathbf{R}_{S4}w'$ and $w' \Vdash_{\mathcal{K}_{S4}} \phi$. Then $w \Vdash_{\mathcal{K}_{S4}} \Diamond\phi$.
  - Case $w \Vdash_{\mathcal{K}_{S4}} \Box\phi$. Let $w' \in W$ and $r' \in Res$ such that $(w, e)\mathbf{R}(w', r')$. As $Res = \{e\}$, by definition of $T_{S4 \to LSM}$, we have $r' = e$. Then $(w, e)\mathbf{R}(w', e)$. By definition of $T_{S4 \to LSM}$, $w\mathbf{R}_{S4}w'$. Thus, as $w \Vdash_{\mathcal{K}_{S4}} \Box\phi$ we have $w' \Vdash_{\mathcal{K}_{S4}} \phi$. Then, by the induction hypothesis, $w', e \vDash_{\mathcal{K}} \phi$ and $w', r' \vDash_{\mathcal{K}} \phi$. Then we have $w, e \vDash_{\mathcal{K}} \Box\phi$.
  - Case $w, e \vDash_{\mathcal{K}} \Box\phi$. Let $w' \in W_{S4}$ such that $w\mathbf{R}_{S4}w'$. By definition of $T_{S4 \to LSM}$, $(w, e)\mathbf{R}(w', e)$. Then, as $w, e \vDash_{\mathcal{K}} \Box\phi$ we have $w', e \vDash_{\mathcal{K}} \phi$. Then, by the induction hypothesis, $w' \Vdash_{\mathcal{K}_{S4}} \phi$ and we have $w \Vdash_{\mathcal{K}_{S4}} \Box\phi$.
  - The other cases are similar. □

Lemma 20. *Let ϕ a formula of $\mathcal{L}_{S4}$ be a formula. If $\vDash \phi$, then $\Vdash \phi$.*

Proof. We show that if $\nVdash \phi$, then $\nvDash \phi$. We suppose that ϕ is not valid in S4. Then there exist a countermodel $\mathcal{K}_{S4} = (W_{S4}, \mathbf{R}_{S4}, V_{S4})$ and a world $w \in W_{S4}$ such that $w \nVdash_{\mathcal{K}_{S4}} \phi$. Now, we consider $T_{S4 \to LSM}(\mathcal{K}_{S4}) = (W, \mathcal{M}, \mathbf{R}, V)$, where $\mathcal{M} = (Res, \bullet, e)$. By Proposition 18, it is a (LSM) model. By Proposition 19, $w, e \nvDash_{\mathcal{K}} \phi$. Then ϕ is not valid in LSM. Therefore if $\nVdash \phi$ then $\nvDash \phi$. We conclude that if $\vDash \phi$ then $\Vdash \phi$. □

Theorem 21. *LSM is a conservative extension of S4 logic.*

Proof. Let $\phi \in \mathcal{L}_{S4}$ be a formula. By Lemmas 16 and 20, ϕ is valid in LSM ($\vDash \phi$) if and only if ϕ is valid in S4 ($\Vdash \phi$). □

6. A proof system for LSM

In this section, we develop a calculus for the logic LSM in the spirit of the tableaux calculus for BI and BBI [16,17,23], using notions introduced in these papers. Here, we introduce new rules to deal with modalities and also new label constraints to capture the reachability relation $\mathbf{R}$. One main difficulty is to deal with the interaction between the resource constraints, which encode the equality on the resources, and the reachability constraints, which encode the relation $\mathbf{R}$.

6.1. Labels for worlds and resources

We first define world and resource labels that are related, respectively, to the sets W and Res. Moreover, to capture the reachability relation ($\mathbf{R}$) and the equality on resources, we introduce two kinds of label constraints. Such labels and constraints allow, in the case of the non-validity of a formula, a countermodel to be extracted.

Rules for resource constraints

$$\frac{}{1 \sim 1}\langle 1\rangle \qquad \frac{x \sim y}{y \sim x}\langle s_r\rangle \qquad \frac{xy \sim xy}{x \sim x}\langle d_r\rangle \qquad \frac{x \sim y \qquad y \sim z}{x \sim z}\langle t_r\rangle$$

$$\frac{x \sim y \qquad yk \sim yk}{xk \sim yk}\langle c_r\rangle \qquad \frac{(u,x) \rightsquigarrow (v,y)}{x \sim x}\langle k_{r_1}\rangle \qquad \frac{(u,x) \rightsquigarrow (v,y)}{y \sim y}\langle k_{r_2}\rangle$$

Rules for reachability constraints

$$\frac{(u,x) \rightsquigarrow (v,y) \qquad z \sim z}{(u,z) \rightsquigarrow (u,z)}\langle r_{a_1}\rangle \qquad \frac{(u,x) \rightsquigarrow (v,y) \qquad z \sim z}{(v,z) \rightsquigarrow (v,z)}\langle r_{a_2}\rangle$$

$$\frac{(u,x) \rightsquigarrow (v,y) \qquad (v,y) \rightsquigarrow (w,z)}{(u,x) \rightsquigarrow (w,z)}\langle t_a\rangle \qquad \frac{(u,x) \rightsquigarrow (v,y) \qquad x \sim x' \qquad y \sim y'}{(u,x') \rightsquigarrow (v,y')}\langle k_a\rangle$$

Fig. 3. Rules for constraints.

Definition 22 *(World labels).* L_W is an infinite countable set of world labels. We let s and v, possibly subscripted, denote elements of L_W.

Definition 23 *(Resource labels).* L_R is a set of *resource labels* built from the set of resource symbols $\Sigma_R \setminus \{e\}$, an infinite countable set of constants $\gamma_R = \{c_1, c_2, \ldots\}$, a constant $1 \notin \Sigma_R \cup \gamma_R$, and a function denoted $\circ$:

$$X ::= 1 \mid r_i \mid c_i \mid X \circ X,$$

where $r_i \in \Sigma_R \setminus \{e\}$, $c_i \in \gamma_R$ and $\Sigma_R \cap \gamma_R = \emptyset$. Moreover, $\circ$ is a function on L_R that is associative, commutative, and has 1 as its unit.

We denote by xy the resource label $x \circ y$. In other words, $c_1c_2c_3c_3$ is the resource label $c_1 \circ c_2 \circ c_3 \circ c_3$. Moreover, we say that x is a *resource sub-label* of y if and only if there exists z such that $x \circ z = y$. The set of resource sub-labels of x is denoted $\mathcal{E}(x)$.

Definition 24 *(Constraints).* A *resource constraint* is an expression of the form $x \sim y$, where x and y are resource labels. A *reachability constraint* is an expression of the form $(u,x) \rightsquigarrow (v,y)$, where u and v are world labels and x and y are resource labels.

A *set of constraints* $\mathcal{C}$ is a set that contains resource constraints and relation constraints. For example, $\mathcal{C} = \{c_1 \sim c_2, c_2 \sim c_3, (s_1, c_1) \rightsquigarrow (s_2, c_1c_3)\}$ is a set of constraints.

Now, we define the domain and the alphabet of such sets. Let $\mathcal{C}$ be a constraint set. The (resource) *domain* of $\mathcal{C}$ is the set of all resource sub-labels appearing in $\mathcal{C}$. In particular,

$$\mathcal{D}_r(\mathcal{C}) = \left[\bigcup_{x \sim y \in \mathcal{C}} (\mathcal{E}(x) \cup \mathcal{E}(y))\right] \cup \left[\bigcup_{(u,x) \rightsquigarrow (v,y) \in \mathcal{C}} (\mathcal{E}(x) \cup \mathcal{E}(y))\right].$$

The world/resource *alphabet* of $\mathcal{C}$ is the set of world/resource constants appearing in $\mathcal{C}$. In particular, we have $\mathcal{A}_w(\mathcal{C}) = \bigcup_{(u,x) \rightsquigarrow (v,y) \in \mathcal{C}} \{u, v\}$ and $\mathcal{A}_r(\mathcal{C}) = (\Sigma_R \cup \gamma_R) \cap \mathcal{D}_r(\mathcal{C})$. We notice that, for any set of constraints $\mathcal{C}$, as $1 \notin \Sigma_R \cup \gamma_R$ then $1 \notin \mathcal{A}_r(\mathcal{C})$. But $1 \in \mathcal{D}_r(\mathcal{C})$, for any non-empty $\mathcal{C} \neq \emptyset$, because $1 \in \mathcal{E}(x)$, for all resource labels x.

Definition 25 *(Closure of constraints).* Let $\mathcal{C}$ be a set of constraints. The closure of $\mathcal{C}$, denoted $\overline{\mathcal{C}}$, is the least relation closed under the rules of Fig. 3 such that $\mathcal{C} \subseteq \overline{\mathcal{C}}$.

Considering the rules of Fig. 3, there are seven rules ($\langle 1\rangle$, $\langle s_r\rangle$, $\langle d_r\rangle$, $\langle t_r\rangle$, $\langle c_r\rangle$, $\langle k_{r_1}\rangle$ and $\langle k_{r_2}\rangle$) that produce resource constraints and there are four rules ($\langle r_{a_1}\rangle$, $\langle r_{a_2}\rangle$, $\langle t_a\rangle$ and $\langle k_a\rangle$) that produce reachability constraints.

As it is impossible to close separately a resource constraint set and a reachability constraint set, because of rules $\langle k_{r_1}\rangle$, $\langle k_{r_2}\rangle$, $\langle r_{a_1}\rangle$, $\langle r_{a_2}\rangle$ and $\langle k_a\rangle$, we choose to consider only one set of resource and reachability constraints ($\mathcal{C}$) rather than two sets (one resource constraint set and one reachability constraint set).

We give an example of rule application. With $\mathcal{C} = \{c_1 \sim c_2, c_2 \sim c_3, (s_1, c_1) \rightsquigarrow (s_2, c_4)\}$, we can show that $(s_1, c_3) \rightsquigarrow (s_2, c_4) \in \overline{\mathcal{C}}$ as follows:

$$\dfrac{(s_1,c_1)\rightsquigarrow(s_2,c_4) \qquad \dfrac{c_1\sim c_2 \qquad c_2\sim c_3}{c_1\sim c_3}\langle t_r\rangle \qquad \dfrac{(s_1,c_1)\rightsquigarrow(s_2,c_4)}{c_4\sim c_4}\langle k_{r_2}\rangle}{(s_1,c_3)\rightsquigarrow(s_2,c_4)}\langle k_a\rangle.$$

It is important to note that the rules $\langle r_{a_1}\rangle$ and $\langle r_{a_2}\rangle$ (resp. $\langle k_{r_1}\rangle$ and $\langle k_{r_2}\rangle$) are used in Proposition 26 to prove that the rules $\langle 1_{a_l}\rangle$ and $\langle 1_{a_l}\rangle$ (resp. $\langle q_l\rangle$ and $\langle q_r\rangle$) can be derived. These rules are used to respectively prove the first and second part of Corollary 27.

Proposition 26. *The following rules can be derived from rules of closure of constraints:*

$$\dfrac{xk\sim y}{x\sim x}\langle p_l\rangle \qquad \dfrac{x\sim yk}{y\sim y}\langle p_r\rangle \qquad \dfrac{(u,xk)\rightsquigarrow(v,y)}{x\sim x}\langle q_l\rangle \qquad \dfrac{(u,x)\rightsquigarrow(v,yk)}{y\sim y}\langle q_r\rangle$$

$$\dfrac{(u,x)\rightsquigarrow(v,y)}{(u,1)\rightsquigarrow(u,1)}\langle 1_{a_l}\rangle \qquad \dfrac{(u,x)\rightsquigarrow(v,y)}{(v,1)\rightsquigarrow(v,1)}\langle 1_{a_r}\rangle.$$

Proof. We provide the following deduction trees:

$$\dfrac{\dfrac{xk\sim y \qquad \dfrac{xk\sim y}{y\sim xk}\langle s_r\rangle}{xk\sim xk}\langle t_r\rangle}{x\sim x}\langle d_r\rangle \qquad \dfrac{\dfrac{x\sim yk}{yk\sim x}\langle s_r\rangle}{y\sim y}\langle p_l\rangle \qquad \dfrac{\dfrac{(u,xk)\rightsquigarrow(v,y)}{xk\sim xk}\langle k_{r_1}\rangle}{x\sim x}\langle d_r\rangle \quad 1 \quad \dfrac{\dfrac{(u,x)\rightsquigarrow(v,yk)}{yk\sim yk}\langle k_{r_2}\rangle}{y\sim y}\langle d_r\rangle$$

$$\dfrac{(u,x)\rightsquigarrow(v,y) \qquad \dfrac{}{1\sim 1}\langle 1\rangle}{(u,1)\rightsquigarrow(u,1)}\langle r_{a_1}\rangle \qquad \dfrac{(u,x)\rightsquigarrow(v,y) \qquad \dfrac{}{1\sim 1}\langle 1\rangle}{(v,1)\rightsquigarrow(v,1)}\langle r_{a_2}\rangle. \quad \square$$

Corollary 27. *Let $\mathcal{C}$ be a set of constraints.*
1. $u\in\mathcal{A}_w(\overline{\mathcal{C}})$ iff $(u,1)\rightsquigarrow(u,1)\in\overline{\mathcal{C}}$.
2. $x\in\mathcal{D}_r(\overline{\mathcal{C}})$ iff $x\sim x\in\overline{\mathcal{C}}$.

Proof. 1. We suppose that $u\in\mathcal{A}_w(\overline{\mathcal{C}})$. By definition $u\in\bigcup_{(v,x)\rightsquigarrow(w,y)\in\overline{\mathcal{C}}}\{v,w\}$. Then there exists $(v,x)\rightsquigarrow(w,y)\in\overline{\mathcal{C}}$ such that $u=v$ or $u=w$. Thus, by Proposition 26, $(u,1)\rightsquigarrow(u,1)\in\overline{\mathcal{C}}$. Now, we suppose that $(u,1)\rightsquigarrow(u,1)\in\overline{\mathcal{C}}$. Then, by definition, $u\in\mathcal{A}_w(\overline{\mathcal{C}})$. In conclusion, we have $u\in\mathcal{A}_w(\overline{\mathcal{C}})$ if and only if $(u,1)\rightsquigarrow(u,1)\in\overline{\mathcal{C}}$.
2. We suppose that $x\in\mathcal{D}_r(\overline{\mathcal{C}})$. By definition we have $x\in\bigcup_{y\sim z\in\overline{\mathcal{C}}}(\mathcal{E}(y)\cup\mathcal{E}(z))$ or $x\in\bigcup_{(u,y)\rightsquigarrow(v,z)\in\overline{\mathcal{C}}}(\mathcal{E}(y)\cup\mathcal{E}(z))$. There are two cases:

- there exists $y\sim z\in\overline{\mathcal{C}}$ such that $x\in\mathcal{E}(y)\cup\mathcal{E}(z)$. Then there exists a resource label k such that $xk\sim z\in\overline{\mathcal{C}}$ or $y\sim xk\in\overline{\mathcal{C}}$. Thus, by Proposition 26, $x\sim x\in\overline{\mathcal{C}}$;
- there exists $(u,y)\rightsquigarrow(v,z)\in\overline{\mathcal{C}}$ such that $x\in\mathcal{E}(y)\cup\mathcal{E}(z)$. Then there exists a resource label k such that $(u,xk)\rightsquigarrow(v,z)\in\overline{\mathcal{C}}$ or $(u,y)\rightsquigarrow(v,xk)\in\overline{\mathcal{C}}$. Then, by Proposition 26, $x\sim x\in\overline{\mathcal{C}}$.

If we suppose that $x\sim x\in\overline{\mathcal{C}}$, then, by definition, $x\in\mathcal{D}_r(\overline{\mathcal{C}})$ and we have $x\in\mathcal{D}_r(\overline{\mathcal{C}})$ if and only if $x\sim x\in\overline{\mathcal{C}}$. □

We can deduce by using the rules $\langle s_r\rangle$ and $\langle t_r\rangle$ with Corollary 27 that $\sim$ is an equivalence relation and then $\sim$ is reflexive. Moreover the first part of Corollary 27 allows us to show that $\rightsquigarrow$ is reflexive.

Corollary 28. *Let $\mathcal{C}$ be a set of constraints. If $xy\in\mathcal{D}_r(\overline{\mathcal{C}})$, $x'\sim x\in\overline{\mathcal{C}}$, and $y'\sim y\in\overline{\mathcal{C}}$, then $xy\sim x'y'\in\overline{\mathcal{C}}$.*

Proof. By Corollary 27, $xy\sim xy\in\overline{\mathcal{C}}$. We give the following deduction tree:

$$\dfrac{\dfrac{\dfrac{\dfrac{\vdots}{y'\sim y} \qquad \dfrac{\dfrac{\dfrac{\vdots}{x'\sim x} \qquad \dfrac{\vdots}{xy\sim xy}}{x'y\sim xy}\langle c_r\rangle}{x'y\sim x'y}\langle p_l\rangle}{x'y'\sim x'y}\langle c_r\rangle \qquad \dfrac{\dfrac{\vdots}{x'\sim x} \qquad \dfrac{\vdots}{xy\sim xy}}{x'y\sim xy}\langle c_r\rangle}{x'y'\sim xy}\langle t_r\rangle}{xy\sim x'y'}\langle s_r\rangle. \quad \square$$

Proposition 29. *Let $\mathcal{C}$ a set of constraints. We have $\mathcal{A}_w(\mathcal{C}) = \mathcal{A}_w(\overline{\mathcal{C}})$ and $\mathcal{A}_r(\mathcal{C}) = \mathcal{A}_r(\overline{\mathcal{C}})$.*

Proof. As $\mathcal{C} \subseteq \overline{\mathcal{C}}$, we have $\mathcal{A}_w(\mathcal{C}) \subseteq \mathcal{A}_w(\overline{\mathcal{C}})$ and $\mathcal{A}_r(\mathcal{C}) \subseteq \mathcal{A}_r(\overline{\mathcal{C}})$. For the converse, we observe that the rules of Fig. 3 do not introduce new world/resource constants. Then $\mathcal{A}_w(\overline{\mathcal{C}}) \subseteq \mathcal{A}_w(\mathcal{C})$ and $\mathcal{A}_r(\overline{\mathcal{C}}) \subseteq \mathcal{A}_r(\mathcal{C})$. Therefore $\mathcal{A}_w(\mathcal{C}) = \mathcal{A}_w(\overline{\mathcal{C}})$ and $\mathcal{A}_r(\mathcal{C}) = \mathcal{A}_r(\overline{\mathcal{C}})$. □

Lemma 30 *(Compactness). Let $\mathcal{C}$ be a (possibly countably infinite) set of constraints.*

1. *If $(u, x) \rightsquigarrow (v, y) \in \overline{\mathcal{C}}$, then there is a finite set $\mathcal{C}_f$ such that $\mathcal{C}_f \subseteq \mathcal{C}$ and $(u, x) \rightsquigarrow (v, y) \in \overline{\mathcal{C}_f}$.*
2. *If $x \sim y \in \overline{\mathcal{C}}$, then there is a finite set $\mathcal{C}_f$ such that $\mathcal{C}_f \subseteq \mathcal{C}$ and $x \sim y \in \overline{\mathcal{C}_f}$.*

Proof. Let $\mathcal{C}$ be a set of constraints and $c \in \overline{\mathcal{C}}$ be a constraint. If $c \in \overline{\mathcal{C}}$ because $c \in \mathcal{C}$ then by considering $\mathcal{C}_f = \{c\}$, we have $\mathcal{C}_f \subseteq \mathcal{C}$ and $c \in \overline{\mathcal{C}_f}$. In the other cases, the constraint c is obtained by rules of Fig. 3. We prove the lemma by induction on the size n of the deduction tree of c.

- Base case ($n = 0$). Case rule $\langle 1 \rangle$: the deduction tree is of the form

$$\frac{}{1 \sim 1}\ \langle 1 \rangle$$

  then c is the constraint $1 \sim 1$. If $\mathcal{C}_f = \emptyset$ then we have $\mathcal{C}_f \subseteq \mathcal{C}$ and $c \in \overline{\mathcal{C}_f}$.
- Inductive step. We suppose that the properties (1) and (2) hold for deduction trees whose sizes are less or equal to n (IH). We prove the lemma for deduction trees such that their sizes are equal to $n + 1$.
  – Case $\langle s_r \rangle$: the deduction tree is of the form

$$\frac{\dfrac{\vdots}{x \sim y}}{y \sim x}\ \langle s_r \rangle$$

  In this case, c is the constraint $y \sim x$. This deduction tree is finite, and the deduction tree of $x \sim y$ has size equal to n. Then, by the induction hypothesis, there is a finite set $\mathcal{C}_f \subseteq \mathcal{C}$ such that $x \sim y \in \overline{\mathcal{C}_f}$. Thus, by the rule $\langle s_r \rangle$, $y \sim x \in \overline{\mathcal{C}_f}$.
  – Case $\langle c_r \rangle$: the deduction tree is of the form

$$\frac{\dfrac{\vdots}{x \sim y} \qquad \dfrac{\vdots}{yk \sim yk}}{xk \sim yk}\ \langle c_r \rangle$$

  In this case, c is the constraint $xk \sim yk$. This deduction tree is finite, and the deduction trees of $x \sim y$ and $yk \sim yk$ have size less than or equal to n. Then, by the induction hypothesis, there are $\mathcal{C}_{f_1} \subseteq \mathcal{C}$ and $\mathcal{C}_{f_2} \subseteq \mathcal{C}$ that are finite and such that $x \sim y \in \overline{\mathcal{C}_{f_1}}$ and $yk \sim yk \in \overline{\mathcal{C}_{f_2}}$. Let $\mathcal{C}_f = \mathcal{C}_{f_1} \cup \mathcal{C}_{f_2}$. Then $x \sim y \in \overline{\mathcal{C}_f}$ and $yk \sim yk \in \overline{\mathcal{C}_f}$. Thus, using the rule $\langle c_r \rangle$, $xk \sim yk \in \overline{\mathcal{C}_f}$. Moreover, $\mathcal{C}_f$ is finite as the union of two finite sets and $\mathcal{C}_f \subseteq \mathcal{C}$ as the union of two sets included in $\mathcal{C}$.
  – The other cases are similar. □

6.2. A tableaux calculus for LSM

In this section, we define a labelled tableaux calculus for LSM in the spirit of previous works for BI and BBI [16,17,23].

Definition 31. The function $\|.\| : \Sigma_R \to L_r$ is defined as follows:

$$\|r\| = \begin{cases} 1 & \text{if } r = e \\ r & \text{otherwise} \end{cases}$$

Definition 32. A *labelled formula* is a 4-tuple $(S, \phi, u, x) \in \{\mathbb{T}, \mathbb{F}\} \times \mathcal{L} \times L_w \times L_r$ written $\mathbb{S}\phi : (u, x)$. A *constrained set of statements* (CSS) is a pair $\langle \mathcal{F}, \mathcal{C} \rangle$, where $\mathcal{F}$ is a set of labelled formulæ and $\mathcal{C}$ is a set of constraints, satisfying the following (P_{css}) property:

$$(P_{css}) : \text{ if } \mathbb{S}\phi : (u, x) \in \mathcal{F} \text{ then } (u, 1) \rightsquigarrow (u, 1) \in \overline{\mathcal{C}} \text{ and } x \sim x \in \overline{\mathcal{C}}.$$

A CSS $\langle \mathcal{F}, \mathcal{C} \rangle$ is *finite* if $\mathcal{F}$ and $\mathcal{C}$ are finite. The relation $\preccurlyeq$ is defined by:

$$\langle \mathcal{F}, \mathcal{C} \rangle \preccurlyeq \langle \mathcal{F}', \mathcal{C}' \rangle \text{ iff } \mathcal{F} \subseteq \mathcal{F}' \text{ and } \mathcal{C} \subseteq \mathcal{C}'.$$

We denote by $\langle \mathcal{F}_f, \mathcal{C}_f \rangle \preccurlyeq_f \langle \mathcal{F}, \mathcal{C} \rangle$ when $\langle \mathcal{F}_f, \mathcal{C}_f \rangle \preccurlyeq \langle \mathcal{F}, \mathcal{C} \rangle$ holds and $\langle \mathcal{F}_f, \mathcal{C}_f \rangle$ is finite, meaning that $\mathcal{F}_f$ and $\mathcal{C}_f$ are both finite.

$$\frac{\mathbb{T}I : (u,x) \in \mathcal{F}}{\langle \emptyset, \{x \sim 1\}\rangle}\ \langle \mathbb{T}I\rangle$$

$$\frac{\mathbb{T}\neg\phi : (u,x) \in \mathcal{F}}{\langle \{\mathbb{F}\phi : (u,x)\}, \emptyset\rangle}\ \langle \mathbb{T}\neg\rangle \qquad \frac{\mathbb{F}\neg\phi : (u,x) \in \mathcal{F}}{\langle \{\mathbb{T}\phi : (u,x)\}, \emptyset\rangle}\ \langle \mathbb{F}\neg\rangle$$

$$\frac{\mathbb{T}\phi \wedge \psi : (u,x) \in \mathcal{F}}{\langle \{\mathbb{T}\phi : (u,x), \mathbb{T}\psi : (u,x)\}, \emptyset\rangle}\ \langle \mathbb{T}\wedge\rangle \qquad \frac{\mathbb{F}\phi \wedge \psi : (u,x) \in \mathcal{F}}{\langle \{\mathbb{F}\phi : (u,x)\}, \emptyset\rangle \ \mid\ \langle \{\mathbb{F}\psi : (u,x)\}, \emptyset\rangle}\ \langle \mathbb{F}\wedge\rangle$$

$$\frac{\mathbb{T}\phi \vee \psi : (u,x) \in \mathcal{F}}{\langle \{\mathbb{T}\phi : (u,x)\}, \emptyset\rangle \ \mid\ \langle \{\mathbb{T}\psi : (u,x)\}, \emptyset\rangle}\ \langle \mathbb{T}\vee\rangle \qquad \frac{\mathbb{F}\phi \vee \psi : (u,x) \in \mathcal{F}}{\langle \{\mathbb{F}\phi : (u,x), \mathbb{F}\psi : (u,x)\}, \emptyset\rangle}\ \langle \mathbb{F}\vee\rangle$$

$$\frac{\mathbb{T}\phi \rightarrow \psi : (u,x) \in \mathcal{F}}{\langle \{\mathbb{F}\phi : (u,x)\}, \emptyset\rangle \ \mid\ \langle \{\mathbb{T}\psi : (u,x)\}, \emptyset\rangle}\ \langle \mathbb{T}\rightarrow\rangle \qquad \frac{\mathbb{F}\phi \rightarrow \psi : (u,x) \in \mathcal{F}}{\langle \{\mathbb{T}\phi : (u,x), \mathbb{F}\psi : (u,x)\}, \emptyset\rangle}\ \langle \mathbb{F}\rightarrow\rangle$$

$$\frac{\mathbb{T}\phi * \psi : (u,x) \in \mathcal{F}}{\langle \{\mathbb{T}\phi : (u,c_i), \mathbb{T}\psi : (u,c_j)\}, \{x \sim c_i c_j\}\rangle}\ \langle \mathbb{T}*\rangle \qquad \frac{\mathbb{F}\phi * \psi : (u,x) \in \mathcal{F} \text{ and } x \sim yz \in \overline{\mathcal{C}}}{\langle \{\mathbb{F}\phi : (u,y)\}, \emptyset\rangle \ \mid\ \langle \{\mathbb{F}\psi : (u,z)\}, \emptyset\rangle}\ \langle \mathbb{F}*\rangle$$

$$\frac{\mathbb{T}\phi -\!\!* \psi : (u,x) \in \mathcal{F} \text{ and } xy \sim xy \in \overline{\mathcal{C}}}{\langle \{\mathbb{F}\phi : (u,y)\}, \emptyset\rangle \ \mid\ \langle \{\mathbb{T}\psi : (u,xy)\}, \emptyset\rangle}\ \langle \mathbb{T}-\!\!*\rangle \qquad \frac{\mathbb{F}\phi -\!\!* \psi : (u,x) \in \mathcal{F}}{\langle \{\mathbb{T}\phi : (u,c_i), \mathbb{F}\psi : (u,xc_i)\}, \{xc_i \sim xc_i\}\rangle}\ \langle \mathbb{F}-\!\!*\rangle$$

with s_i, c_i and c_j being new label constants and $\|r\| = 1$ if $r = e$, otherwise r.

Fig. 4. Tableaux non-modal rules for LSM.

Proposition 33. *For any CSS $\langle \mathcal{F}_f, \mathcal{C}\rangle$ in which $\mathcal{F}_f$ is finite, there exists $\mathcal{C}_f \subseteq \mathcal{C}$ such that $\mathcal{C}_f$ is finite and $\langle \mathcal{F}_f, \mathcal{C}_f\rangle$ is a CSS.*

Proof. By induction on the number of labelled formulæ that belong to $\mathcal{F}_f$ and using Lemma 30. □

Figs. 4 and 5 present the rules of tableaux calculus for LSM, the later including the rules on modalities. Note that 's_i is a new label constant' means $s_i \in L_w \setminus \mathcal{A}_w(\mathcal{C})$ and that 'c_i and c_j are new label constants' means $c_i \neq c_j \in \gamma_R \setminus \mathcal{A}_r(\mathcal{C})$. We denote by $\oplus$ the concatenation of lists.

Definition 34 *(Tableaux).* Let $\langle \mathcal{F}_0, \mathcal{C}_0\rangle$ be a finite CSS. A *tableau* for this CSS is a list of CSS, called *branches*, built inductively according the following rules:

1. The one ranch list $[\langle \mathcal{F}_0, \mathcal{C}_0\rangle]$ is a tableau for $\langle \mathcal{F}_0, \mathcal{C}_0\rangle$
2. If the list $\mathcal{T}_m \oplus [\langle \mathcal{F}, \mathcal{C}\rangle] \oplus \mathcal{T}_n$ is a tableau for $\langle \mathcal{F}_0, \mathcal{C}_0\rangle$ and

$$\frac{\text{cond}\langle \mathcal{F}, \mathcal{C}\rangle}{\langle \mathcal{F}_1, \mathcal{C}_1\rangle \mid \ldots \mid \langle \mathcal{F}_k, \mathcal{C}_k\rangle}$$

is an instance of a rule of Figs. 4 and 5 for which $\text{cond}\langle \mathcal{F}, \mathcal{C}\rangle$ is fulfilled, then the list

$$\mathcal{T}_m \oplus [\langle \mathcal{F} \cup \mathcal{F}_1, \mathcal{C} \cup \mathcal{C}_1\rangle; \ldots; \langle \mathcal{F} \cup \mathcal{F}_k, \mathcal{C} \cup \mathcal{C}_k\rangle] \oplus \mathcal{T}_n$$

is a tableau for $\langle \mathcal{F}_0, \mathcal{C}_0\rangle$.

A *tableau* for the formula ϕ is a *tableau* for $\langle \{\mathbb{F}\phi : (s_1, c_1)\}, \{(s_1, c_1) \rightsquigarrow (s_1, c_1)\}\rangle$.

We can show that the rules of Figs. 4 and 5 preserve the property (P_{css}) of Definition 32 (using Corollary 27).

Observing the rules we can say that there are two particular kinds of rules. First there are the rules $\langle \mathbb{T}I\rangle$, $\langle \mathbb{T}*\rangle$, $\langle \mathbb{F}-\!\!*\rangle$, $\langle \mathbb{T}\Diamond_y\rangle$, $\langle \mathbb{F}\Box_y\rangle$ $\langle \mathbb{T}\Diamond\rangle$, $\langle \mathbb{F}\Box\rangle$, $\langle \mathbb{T}\Diamond_\bullet\rangle$, and $\langle \mathbb{F}\Box_\bullet\rangle$. They introduce new constraints and also new label constants (s_i, c_i and c_j), except for $\langle \mathbb{T}I\rangle$ that only introduces a new constraint. We illustrate the $\langle \mathbb{T}\Diamond\rangle$ rule. When we apply this rule on a labelled formula $\mathbb{T}\Diamond\phi : (s_2, c_4)$ that belongs to a CSS $\langle \mathcal{F}, \mathcal{C}\rangle$, we have to choose a new world label and a new resource label which does not appear in $\mathcal{C}$. For example, we suppose that $s_5 \in L_w \setminus \mathcal{A}_w(\mathcal{C})$ and $c_6 \in \gamma_R \setminus \mathcal{A}_r(\mathcal{C})$. Thus, choosing these labels, we can apply the rule, getting the new CSS $\langle \mathcal{F} \cup \{\mathbb{T}\phi : (s_5, c_6)\}, \mathcal{C} \cup \{(s_2, c_4) \rightsquigarrow (s_5, c_6)\}\rangle$. We remark that the new reachability constraint $(s_2, c_4) \rightsquigarrow (s_5, c_6)$ added to the set of constraints.

There are rules $\langle \mathbb{F}*\rangle$, $\langle \mathbb{T}-\!\!*\rangle$, $\langle \mathbb{F}\Diamond_y\rangle$, $\langle \mathbb{T}\Box_y\rangle$ $\langle \mathbb{F}\Diamond\rangle$, $\langle \mathbb{T}\Box\rangle$, $\langle \mathbb{F}\Diamond_\bullet\rangle$, and $\langle \mathbb{T}\Box_\bullet\rangle$. They have a condition on the closure of label constraints. In order to apply one of these rules we have to choose labels which satisfy the condition and then apply the rule using it. Otherwise, we cannot apply the rule. We illustrate the $\langle \mathbb{T}\Box\rangle$ rule. Consider a CSS $\langle \mathcal{F}, \mathcal{C}\rangle$ such that $\mathbb{T}\Box\phi : (s_1, c_1) \in \mathcal{F}$. To apply this rule, we have to choose a world label u and a resource label x such that $(s_1, c_1) \rightsquigarrow (u, x) \in \overline{\mathcal{C}}$. We

$$\frac{\mathbb{T}\Diamond_y\phi : (u,x) \in \mathcal{F}}{\langle\{\mathbb{T}\phi : (s_i,c_i)\}, \{(u, x \circ \|y\|) \rightsquigarrow (s_i,c_i)\}\rangle}\ \langle\mathbb{T}\Diamond_y\rangle \qquad \frac{\mathbb{F}\Diamond_y\phi : (u,x) \in \mathcal{F} \text{ and } (u, x \circ \|y\|) \rightsquigarrow (v,z) \in \overline{\mathcal{C}}}{\langle\{\mathbb{F}\phi : (v,z)\}, \emptyset\rangle}\ \langle\mathbb{F}\Diamond_y\rangle$$

$$\frac{\mathbb{T}\Box_y\phi : (u,x) \in \mathcal{F} \text{ and } (u, x \circ \|y\|) \rightsquigarrow (v,z) \in \overline{\mathcal{C}}}{\langle\{\mathbb{T}\phi : (v,z)\}, \emptyset\rangle}\ \langle\mathbb{T}\Box_y\rangle \qquad \frac{\mathbb{F}\Box_y\phi : (u,x) \in \mathcal{F}}{\langle\{\mathbb{F}\phi : (s_i,c_i)\}, \{(u, x \circ \|y\|) \rightsquigarrow (s_i,c_i)\}\rangle}\ \langle\mathbb{F}\Box_y\rangle$$

$$\frac{\mathbb{T}\Diamond\phi : (u,x) \in \mathcal{F}}{\langle\{\mathbb{T}\phi : (s_i,c_i)\}, \{(u,x) \rightsquigarrow (s_i,c_i)\}\rangle}\ \langle\mathbb{T}\Diamond\rangle \qquad \frac{\mathbb{F}\Diamond\phi : (u,x) \in \mathcal{F} \text{ and } (u,x) \rightsquigarrow (v,y) \in \overline{\mathcal{C}}}{\langle\{\mathbb{F}\phi : (v,y)\}, \emptyset\rangle}\ \langle\mathbb{F}\Diamond\rangle$$

$$\frac{\mathbb{T}\Box\phi : (u,x) \in \mathcal{F} \text{ and } (u,x) \rightsquigarrow (v,y) \in \overline{\mathcal{C}}}{\langle\{\mathbb{T}\phi : (v,y)\}, \emptyset\rangle}\ \langle\mathbb{T}\Box\rangle \qquad \frac{\mathbb{F}\Box\phi : (u,x) \in \mathcal{F}}{\langle\{\mathbb{F}\phi : (s_i,c_i)\}, \{(u,x) \rightsquigarrow (s_i,c_i)\}\rangle}\ \langle\mathbb{F}\Box\rangle$$

$$\frac{\mathbb{T}\Diamond_\bullet\phi : (u,x) \in \mathcal{F}}{\langle\{\mathbb{T}\phi : (s_i,c_j)\}, \{(u,xc_i) \rightsquigarrow (s_i,c_j)\}\rangle}\ \langle\mathbb{T}\Diamond_\bullet\rangle \qquad \frac{\mathbb{F}\Diamond_\bullet\phi : (u,x) \in \mathcal{F} \text{ and } (u,xy) \rightsquigarrow (v,z) \in \overline{\mathcal{C}}}{\langle\{\mathbb{F}\phi : (v,z)\}, \emptyset\rangle}\ \langle\mathbb{F}\Diamond_\bullet\rangle$$

$$\frac{\mathbb{T}\Box_\bullet\phi : (u,x) \in \mathcal{F} \text{ and } (u,xy) \rightsquigarrow (v,z) \in \overline{\mathcal{C}}}{\langle\{\mathbb{T}\phi : (v,z)\}, \emptyset\rangle}\ \langle\mathbb{T}\Box_\bullet\rangle \qquad \frac{\mathbb{F}\Box_\bullet\phi : (u,x) \in \mathcal{F}}{\langle\{\mathbb{F}\phi : (s_i,c_j)\}, \{(u,xc_i) \rightsquigarrow (s_i,c_j)\}\rangle}\ \langle\mathbb{F}\Box_\bullet\rangle$$

with s_i, c_i and c_j being new label constants and $\|r\| = 1$ if $r = e$, otherwise r.

Fig. 5. Tableaux modal rules for LSM.

also suppose that $(s_1, c_1) \rightsquigarrow (s_2, c_3) \in \overline{\mathcal{C}}$. Then we can decide to apply the rule using s_2 and c_3, getting the CSS $\langle \mathcal{F} \cup \{\mathbb{T}\phi : (s_2, c_3)\}, \mathcal{C}\rangle$. Finally, we observe that the rules $\langle\mathbb{T}\Diamond_y\rangle$, $\langle\mathbb{F}\Diamond_y\rangle$, $\langle\mathbb{T}\Box_y\rangle$ and $\langle\mathbb{F}\Box_y\rangle$ use the function $\|.\|$ that converts the unit resource e into the unit resource label 1.

Definition 35 *(Closure condition).* A CSS $\langle\mathcal{F}, \mathcal{C}\rangle$ is *closed* if one of the following conditions holds:

1. $\mathbb{T}\phi : (u,x) \in \mathcal{F}$, $\mathbb{F}\phi : (u,y) \in \mathcal{F}$ and $x \sim y \in \overline{\mathcal{C}}$;
2. $\mathbb{F}I : (u,x) \in \mathcal{F}$ and $x \sim 1 \in \overline{\mathcal{C}}$;
3. $\mathbb{F}\top : (u,x) \in \mathcal{F}$;
4. $\mathbb{T}\bot : (u,x) \in \mathcal{F}$.

A CSS is *open* iff it is not closed. A tableau is closed iff all its branches are closed. A *proof* for a formula ϕ is a closed tableau for ϕ.

In other words, a proof for the formula ϕ is a closed tableau for the CSS $\langle\{\mathbb{F}\phi : (s_1, c_1)\}, \{(s_1, c_1) \rightsquigarrow (s_1, c_1)\}\rangle$.

6.3. Soundness

The soundness proof uses similar techniques than the ones used in BI labelled tableaux method [16,17]. The key point is the notion of *realizability* of a CSS $\langle\mathcal{F}, \mathcal{C}\rangle$, which means there exists a model $\mathcal{K}$ and embeddings from world labels to the world set ($\lfloor.\rfloor_w$) and resource labels to the resource set ($\lfloor.\rfloor_r$) of $\mathcal{K}$ such that if $\mathbb{T}\phi : (u,x) \in \mathcal{F}$, then $\lfloor u\rfloor_w, \lfloor x\rfloor_r \vDash_{\mathcal{K}} \phi$ and if $\mathbb{F}\phi : (u,x) \in \mathcal{F}$ then $\lfloor u\rfloor_w, \lfloor x\rfloor_r \nvDash_{\mathcal{K}} \phi$. To obtain such embedding, we consider two functions $\lfloor.\rfloor_w : \mathcal{A}_w(\mathcal{C}) \to W$ and $\lfloor.\rfloor_r : \mathcal{A}_r(\mathcal{C}) \to Res$.

We remark, by Proposition 29, that $\lfloor.\rfloor_w$ is defined on $\mathcal{A}_w(\overline{\mathcal{C}})$. Then, such $\lfloor.\rfloor_r$ functions will be implicitly extended to $\mathcal{D}_r(\mathcal{C}) \rightharpoonup Res$, that is for all $c_{i_1} \circ \ldots \circ c_{i_n} \in \mathcal{D}_r(\mathcal{C})$, $\lfloor c_{i_1} \circ \ldots \circ c_{i_n}\rfloor_r = \lfloor c_{i_1}\rfloor_r \bullet \ldots \bullet \lfloor c_{i_n}\rfloor_r$ and $\lfloor 1\rfloor_r = e$. Moreover $\lfloor x\rfloor_r$ can be undefined, because resource composition is partial.

Definition 36 *(Realization).* Let $\langle\mathcal{F}, \mathcal{C}\rangle$ be a CSS. A *realization* of $\langle\mathcal{F}, \mathcal{C}\rangle$ is a triplet $\mathfrak{R} = (\mathcal{K}, \lfloor.\rfloor_w, \lfloor.\rfloor_r)$ where $\mathcal{K} = (W, \mathcal{M}, \mathbf{R}, V)$ is a model, $\lfloor.\rfloor_w : \mathcal{A}_w(\mathcal{C}) \to W$ and $\lfloor.\rfloor_r : \mathcal{D}_r(\mathcal{C}) \to Res$, such that

- $\lfloor 1\rfloor_r = e$,
- $\lfloor.\rfloor_r$ is total: $\forall x \in \mathcal{D}_r(\mathcal{C}) \cdot \lfloor x\rfloor_r \downarrow$,
- if $r \in \Sigma_R \cap \mathcal{A}_r(\mathcal{C})$, then $\lfloor r\rfloor_r = r$,
- if $\mathbb{T}\phi : (u,x) \in \mathcal{F}$, then $\lfloor u\rfloor_w, \lfloor x\rfloor_r \vDash_{\mathcal{K}} \phi$,
- if $\mathbb{F}\phi : (u,x) \in \mathcal{F}$, then $\lfloor u\rfloor_w, \lfloor x\rfloor_r \nvDash_{\mathcal{K}} \phi$,
- if $(u,x) \rightsquigarrow (v,y) \in \mathcal{C}$, then $(\lfloor u\rfloor_w, \lfloor x\rfloor_r)\mathbf{R}(\lfloor v\rfloor_w, \lfloor y\rfloor_r)$, and
- if $x \sim y \in \mathcal{C}$, then $\lfloor x\rfloor_r = \lfloor y\rfloor_r$.

A CSS is *realizable* if there exists a realization of this CSS and a tableau is *realizable* if at least one of its branches is realizable.

Proposition 37. *Let $\langle \mathcal{F}, \mathcal{C} \rangle$ be a CSS and $\mathfrak{R} = (\mathcal{K}, \lfloor . \rfloor_w, \lfloor . \rfloor_r)$ a realization of it. The following properties hold:*

1. *For all $x \in \mathcal{D}_r(\overline{\mathcal{C}})$, $\lfloor x \rfloor_r$ is defined;*
2. *If $(u, x) \rightsquigarrow (v, y) \in \overline{\mathcal{C}}$, then $(\lfloor u \rfloor_w, \lfloor x \rfloor_r)\mathbf{R}(\lfloor v \rfloor_w, \lfloor y \rfloor_r)$;*
3. *If $x \sim y \in \overline{\mathcal{C}}$, then $\lfloor x \rfloor_r = \lfloor y \rfloor_r$.*

Proof. This proof is a direct extension of the proof of the same proposition developed in previous works [9,23]. □

Lemma 38. *The rules of the tableaux method for LSM preserve realizability.*

Proof. Let $\mathcal{T}$ a realizable tableau. By definition, $\mathcal{T}$ contains a realizable branch $\mathcal{B} = \langle \mathcal{F}, \mathcal{C} \rangle$. Let $\mathfrak{R} = (\mathcal{K}, \lfloor . \rfloor_w, \lfloor . \rfloor_r)$ be a realization of the branch $\mathcal{B}$, where $\mathcal{K} = (W, \mathcal{M}, \mathbf{R}, V)$, $\lfloor . \rfloor_w : \mathcal{A}_w(\overline{\mathcal{C}}) \to W$ and $\lfloor . \rfloor_r : \mathcal{D}_r(\overline{\mathcal{C}}) \to Res$. If we apply a rule on a labelled formula of another branch than $\mathcal{B}$, then this $\mathcal{B}$ is not modified, then $\mathcal{T}$ stays realizable. Else, we proceed by cases on the formula to which the rule is applied. We only present the cases related to modalities, the other being already checked in previous works on BBI.

- $\mathbb{T}\Diamond_y \phi : (u, x) \in \mathcal{F}$.
  We have $\lfloor u \rfloor_w, \lfloor x \rfloor_r \models_{\mathcal{K}} \Diamond_y \phi$. Then, there are $w \in W$ and $r \in Res$ such that $\lfloor x \rfloor_r \bullet y \downarrow$ and $(\lfloor u \rfloor_w, \lfloor x \rfloor_r \bullet y)\mathbf{R}(w, r)$ and $w, r \models_{\mathcal{K}} \phi$. As s_i and c_i are a new label constants, $\lfloor s_i \rfloor_w$ and $\lfloor c_i \rfloor_r$ are not defined. Then we can extend $\mathfrak{R}$ such that $\lfloor s_i \rfloor_w = w$ and $\lfloor c_i \rfloor_r = r$. We also remark that the rule introduces the resource label $\|y\|$. There are three cases.
  – If $y = e$ then $\|y\| = 1$ and we have $\lfloor \|y\| \rfloor_r = \lfloor 1 \rfloor_r = e = y$.
  – If $y \neq e$ and $y \in \mathcal{A}_r(\mathcal{C})$ then $\|y\| = y$ and we have $\lfloor \|y\| \rfloor_r = \lfloor y \rfloor_r = y$.
  – If $y \neq e$ and $y \notin \mathcal{A}_r(\mathcal{C})$ then we can extend the realization by setting $\lfloor \|y\| \rfloor_r = y$.
  Thus, in all cases, we obtain a realization of $\langle \mathcal{F}, \mathcal{C} \cup \{(u, x \circ \|y\|) \rightsquigarrow (s_i, c_i)\}\rangle$, which is a realization of the new branch $\langle \mathcal{F} \cup \{\mathbb{T}\phi : (s_i, c_i)\}, \mathcal{C} \cup \{(u, x \circ \|y\|) \rightsquigarrow (s_i, c_i)\}\rangle$.
- $\mathbb{F}\Diamond_y \phi : (u, x) \in \mathcal{F}$.
  By realization, we have $\lfloor u \rfloor_w, \lfloor x \rfloor_r \not\models_{\mathcal{K}} \Diamond_\bullet \phi$. Then, by definition, for all $w \in W$ and $r \in Res$ such that $\lfloor x \rfloor_r \bullet y \downarrow$ and $(\lfloor u \rfloor_w, \lfloor x \rfloor_r \bullet y)\mathbf{R}(w, r)$, we have $w, r \not\models_{\mathcal{K}} \phi$. By rule condition, $(u, x \circ \|y\|) \rightsquigarrow (v, z) \in \overline{\mathcal{C}}$. Thus, by Proposition 37, $(\lfloor u \rfloor_w, \lfloor x \circ \|y\| \rfloor_r)\mathbf{R}(\lfloor v \rfloor_w, \lfloor z \rfloor_r)$. There are two cases.
  – If $y = e$ then $\|y\| = 1$ and we have $\lfloor \|y\| \rfloor_r = \lfloor 1 \rfloor_r = e = y$.
  – If $y \neq e$ then $\|y\| = y$ and we have $\lfloor \|y\| \rfloor_r = \lfloor y \rfloor_r = y$.
  Thus, we have $\lfloor \|y\| \rfloor_r = y$. Remarking that $\lfloor x \circ \|y\| \rfloor_r \downarrow$ and $\lfloor x \circ \|y\| \rfloor_r = \lfloor x \rfloor_r \bullet \lfloor \|y\| \rfloor_r$, we have $\lfloor v \rfloor_w, \lfloor z \rfloor_r \not\models_{\mathcal{K}} \phi$ and we can conclude that $\mathfrak{R}$ is a realization of the new branch $\langle \mathcal{F} \cup \{\mathbb{F}\phi : (v, z)\}, \mathcal{C}\rangle$.
- $\mathbb{T}\Diamond\phi : (u, x) \in \mathcal{F}$.
  We have $\lfloor u \rfloor_w, \lfloor x \rfloor_r \models_{\mathcal{K}} \Diamond\phi$. Then, there are $w \in W$ and $r \in Res$ such that $(\lfloor u \rfloor_w, \lfloor x \rfloor_r)\mathbf{R}(w, r)$ and $w, r \models_{\mathcal{K}} \phi$. As s_i and c_i are a new label constants, then $\lfloor s_i \rfloor_w$ and $\lfloor c_i \rfloor_r$ are not defined. Then we can extend $\mathfrak{R}$ such that $\lfloor s_i \rfloor_w = w$ and $\lfloor c_i \rfloor_r = r$. Then we obtain a realization of $\langle \mathcal{F}, \mathcal{C} \cup \{(u, x) \rightsquigarrow (s_i, c_i)\}\rangle$, which is a realization of the new branch $\langle \mathcal{F} \cup \{\mathbb{T}\phi : (s_i, c_i)\}, \mathcal{C} \cup \{(u, x) \rightsquigarrow (s_i, c_i)\}\rangle$.
- $\mathbb{F}\Diamond\phi : (u, x) \in \mathcal{F}$.
  By realization, we have $\lfloor u \rfloor_w, \lfloor x \rfloor_r \not\models_{\mathcal{K}} \Diamond\phi$. Then, by definition, for all $w \in W$ and $r \in Res$ such that $(\lfloor u \rfloor_w, \lfloor x \rfloor_r)\mathbf{R}(w, r)$, we have $w, r \not\models_{\mathcal{K}} \phi$. By rule condition, $(u, x) \rightsquigarrow (v, y) \in \overline{\mathcal{C}}$. Thus, by Proposition 37, $(\lfloor u \rfloor_w, \lfloor x \rfloor_r)\mathbf{R}(\lfloor v \rfloor_w, \lfloor y \rfloor_r)$. Therefore $\lfloor v \rfloor_w, \lfloor y \rfloor_r \not\models_{\mathcal{K}} \phi$ and we can conclude that $\mathfrak{R}$ is a realization of the new branch $\langle \mathcal{F} \cup \{\mathbb{F}\phi : (v, y)\}, \mathcal{C}\rangle$.
- $\mathbb{T}\Diamond_\bullet \phi : (u, x) \in \mathcal{F}$.
  We have $\lfloor u \rfloor_w, \lfloor x \rfloor_r \models_{\mathcal{K}} \Diamond_\bullet \phi$. Then, there are $w \in W$ and $s, r \in Res$ such that $\lfloor x \rfloor_r \bullet s \downarrow$ and $(\lfloor u \rfloor_w, \lfloor x \rfloor_r \bullet s)\mathbf{R}(w, r)$ and $w, r \models_{\mathcal{K}} \phi$. As s_i, c_i and c_j are a new label constants, $\lfloor s_i \rfloor_w$, $\lfloor c_i \rfloor_r$ and $\lfloor c_j \rfloor_r$ are not defined. Moreover, as $c_i \neq c_j$ then we can extend $\mathfrak{R}$ such that $\lfloor s_i \rfloor_w = w$ and $\lfloor c_i \rfloor_r = s$ and $\lfloor c_j \rfloor_r = r$. Remarking that $\lfloor x \rfloor_r \bullet \lfloor c_i \rfloor_r \downarrow$ and, by implicit extension, $\lfloor x c_i \rfloor_r = \lfloor x \rfloor_r \bullet \lfloor c_i \rfloor_r$ and $(\lfloor u \rfloor_w, \lfloor x c_i \rfloor_r)\mathbf{R}(\lfloor s_i \rfloor_w, \lfloor c_j \rfloor_r)$, we obtain a realization of $\langle \mathcal{F}, \mathcal{C} \cup \{(u, x c_i) \rightsquigarrow (s_i, c_j)\}\rangle$, which is a realization of the new branch $\langle \mathcal{F} \cup \{\mathbb{T}\phi : (s_i, c_j)\}, \mathcal{C} \cup \{(u, x c_i) \rightsquigarrow (s_i, c_j)\}\rangle$.
- $\mathbb{F}\Diamond_\bullet \phi : (u, x) \in \mathcal{F}$.
  By realization, we have $\lfloor u \rfloor_w, \lfloor x \rfloor_r \not\models_{\mathcal{K}} \Diamond_\bullet \phi$. Then, by definition, for all $w \in W$ and $s, r \in Res$ such that $\lfloor x \rfloor_r \bullet s \downarrow$ and $(\lfloor u \rfloor_w, \lfloor x \rfloor_r \bullet s)\mathbf{R}(w, r)$, we have $w, r \not\models_{\mathcal{K}} \phi$. By rule condition, $(u, xy) \rightsquigarrow (v, z) \in \overline{\mathcal{C}}$. Thus, by Proposition 37, $(\lfloor u \rfloor_w, \lfloor xy \rfloor_r)\mathbf{R}(\lfloor v \rfloor_w, \lfloor z \rfloor_r)$. Remarking that $\lfloor xy \rfloor_r \downarrow$ and $\lfloor xy \rfloor_r = \lfloor x \rfloor_r \bullet \lfloor y \rfloor_r$, by the definition of realization, we have $\lfloor v \rfloor_w, \lfloor z \rfloor_r \not\models_{\mathcal{K}} \phi$ and then $\mathfrak{R}$ is a realization of the new branch $\langle \mathcal{F} \cup \{\mathbb{F}\phi : (v, z)\}, \mathcal{C}\rangle$.
- The other cases are similar. □

Lemma 39. *Closed branches are not realizable.*

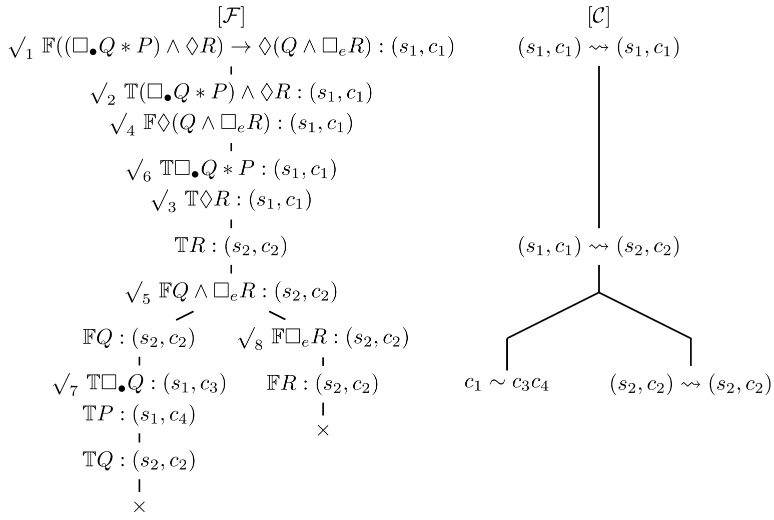
$[\mathcal{F}]$
$\surd_1\ \mathbb{F}((\Box_\bullet Q * P) \wedge \Diamond R) \rightarrow \Diamond(Q \wedge \Box_e R) : (s_1, c_1)$
$\surd_2\ \mathbb{T}(\Box_\bullet Q * P) \wedge \Diamond R : (s_1, c_1)$
$\surd_4\ \mathbb{F}\Diamond(Q \wedge \Box_e R) : (s_1, c_1)$
$\surd_6\ \mathbb{T}\Box_\bullet Q * P : (s_1, c_1)$
$\surd_3\ \mathbb{T}\Diamond R : (s_1, c_1)$
$\mathbb{T}R : (s_2, c_2)$
$\surd_5\ \mathbb{F}Q \wedge \Box_e R : (s_2, c_2)$
$\mathbb{F}Q : (s_2, c_2)$
$\surd_8\ \mathbb{F}\Box_e R : (s_2, c_2)$
$\surd_7\ \mathbb{T}\Box_\bullet Q : (s_1, c_3)$
$\mathbb{T}P : (s_1, c_4)$
$\mathbb{F}R : (s_2, c_2)$
$\times$
$\mathbb{T}Q : (s_2, c_2)$
$\times$
$[\mathcal{C}]$
$(s_1, c_1) \rightsquigarrow (s_1, c_1)$
$(s_1, c_1) \rightsquigarrow (s_2, c_2)$
$c_1 \sim c_3 c_4$
$(s_2, c_2) \rightsquigarrow (s_2, c_2)$

Fig. 6. Tableau for $((\Box_\bullet Q * P) \wedge \Diamond R) \rightarrow \Diamond(Q \wedge \Box_e R)$.

Proof. Let $\langle \mathcal{F}, \mathcal{C} \rangle$ a closed branch. We suppose that this branch is realizable. Let $\mathfrak{R} = (\mathcal{K}, \lfloor . \rfloor_W, \lfloor . \rfloor_r)$ a realization of it. There are four cases.

- $\mathbb{T}\phi : (u, x) \in \mathcal{F}$, $\mathbb{F}\phi : (u, y) \in \mathcal{F}$ and $x \sim y \in \overline{\mathcal{C}}$.
  By definition of realization and Proposition 37, we have $\lfloor u \rfloor_W, \lfloor x \rfloor_r \vDash_{\mathcal{K}} \phi$, $\lfloor u \rfloor_W, \lfloor y \rfloor_r \nvDash_{\mathcal{K}} \phi$ and $\lfloor x \rfloor_r = \lfloor y \rfloor_r$. This case is absurd.
- $\mathbb{F}I : (u, x) \in \mathcal{F}$ and $x \sim 1 \in \overline{\mathcal{C}}$.
  By definition of realization and Proposition 37, $\lfloor u \rfloor_W, \lfloor x \rfloor_r \nvDash_{\mathcal{K}} I$ and $\lfloor x \rfloor_r = e$. This case is absurd.
- $\mathbb{F}\top : (u, x) \in \mathcal{F}$.
  By definition of realization, $\lfloor u \rfloor_W, \lfloor x \rfloor_r \nvDash_{\mathcal{K}} \top$, which is absurd.
- $\mathbb{T}\bot : (u, x) \in \mathcal{F}$.
  By definition of realization, $\lfloor u \rfloor_W, \lfloor x \rfloor_r \vDash_{\mathcal{K}} \bot$, which is absurd.

As all cases are absurd, we conclude that $\langle \mathcal{F}, \mathcal{C} \rangle$ is not realizable. □

Theorem 40 *(Soundness). If there exists a proof for a formula ϕ, then ϕ is valid.*

Proof. Suppose that there exists a proof for ϕ. Then there is a closed tableau $\mathcal{T}_\phi$ for the CSS $\mathfrak{C} = \langle \{\mathbb{F}\phi : (s_1, c_1)\}, \{(s_1, c_1) \rightsquigarrow (s_1, c_1)\} \rangle$. Now suppose that ϕ is not valid. Then there is a countermodel $\mathcal{K} = (W, \mathcal{M}, \mathbf{R}, V)$, a world $w \in W$, and a resource $r \in Res$ such that $w, r \nvDash_{\mathcal{K}} \phi$. Let $\mathfrak{R} = (\mathcal{K}, \lfloor . \rfloor_W, \lfloor . \rfloor_r)$ such that $\lfloor s_1 \rfloor_W = w$, $\lfloor c_1 \rfloor_r = r$ and $\lfloor 1 \rfloor_r = e$. Note that $\mathfrak{R}$ is a realization of $\mathfrak{C}$. By Lemma 38, $\mathcal{T}_\phi$ is realizable. By Lemma 39, $\mathcal{T}_\phi$ cannot be closed. But, this is absurd because $\mathcal{T}_\phi$ is a proof and then a closed tableau. Therefore ϕ is valid. □

6.4. Tableaux examples

We first build a tableau for formula $\phi \equiv ((\Box_\bullet Q * P) \wedge \Diamond R) \rightarrow \Diamond(Q \wedge \Box_e R)$.

By Definition 34, $[\langle \{\mathbb{F}\phi : (s_1, c_1)\}, \{(s_1, c_1) \rightsquigarrow (s_1, c_1)\} \rangle]$ is a tableau for ϕ. In order to represent tableaux, we use the following representation:

$[\mathcal{F}]$	$[\mathcal{C}]$
$\mathbb{F}((\Box_\bullet Q * P) \wedge \Diamond R) \rightarrow \Diamond(Q \wedge \Box_e R) : (s_1, c_1)$	$(s_1, c_1) \rightsquigarrow (s_1, c_1)$

The column on left represents the sets of labelled formulæ of the CSS of the tableau ($[\mathcal{F}]$) and the column on the right represents the constraint sets of the CSS of the tableau ($[\mathcal{C}]$). Applying rules on this tableau, we obtain the tableau of Fig. 6 for ϕ. We decorate a labelled formula with $\surd_i$ to show that we apply a rule on this formula at step i.

We give more details about the rule applications at steps 3, 7, and 8. At step 3, we apply a rule on the labelled formula $\mathbb{T}\Diamond R : (s_1, c_1)$. To apply the rule $\langle \mathbb{T}\Diamond \rangle$, we have to choose a new world label (s_2) and a new resource label (c_2). Then, the rule introduces in the branch the labelled formula $\mathbb{T}R : (s_2, c_2)$ and the constraint $(s_1, c_1) \rightsquigarrow (s_2, c_2)$.

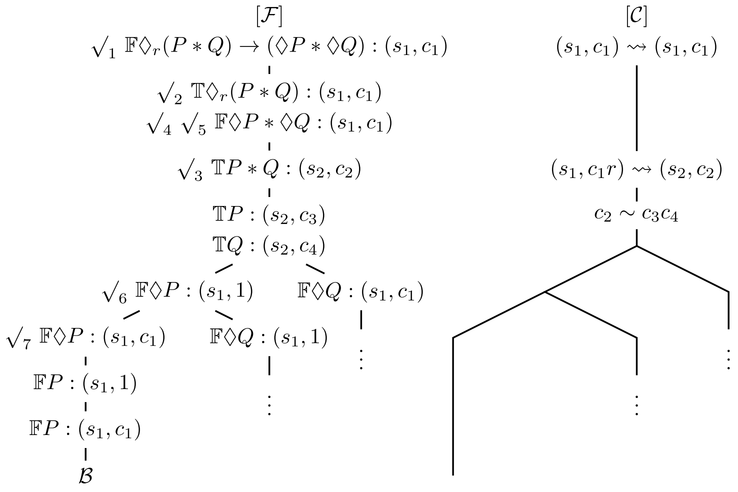
$[\mathcal{F}]$
$\surd_1\ \mathbb{F}\Diamond_r(P*Q)\rightarrow(\Diamond P*\Diamond Q):(s_1,c_1)$
$\surd_2\ \mathbb{T}\Diamond_r(P*Q):(s_1,c_1)$
$\surd_4\ \surd_5\ \mathbb{F}\Diamond P*\Diamond Q:(s_1,c_1)$
$\surd_3\ \mathbb{T}P*Q:(s_2,c_2)$
$\mathbb{T}P:(s_2,c_3)$
$\mathbb{T}Q:(s_2,c_4)$
$\surd_6\ \mathbb{F}\Diamond P:(s_1,1)$
$\mathbb{F}\Diamond Q:(s_1,c_1)$
$\surd_7\ \mathbb{F}\Diamond P:(s_1,c_1)$
$\mathbb{F}\Diamond Q:(s_1,1)$
$\mathbb{F}P:(s_1,1)$
$\mathbb{F}P:(s_1,c_1)$
$\mathcal{B}$
$[\mathcal{C}]$
$(s_1,c_1)\rightsquigarrow(s_1,c_1)$
$(s_1,c_1r)\rightsquigarrow(s_2,c_2)$
$c_2\sim c_3c_4$

Fig. 7. Tableau for $\Diamond_r(P*Q)\rightarrow(\Diamond P*\Diamond Q)$.

Concerning step 7, we apply the rule $\langle\mathbb{T}\Box_\bullet\rangle$ on the labelled formula $\mathbb{T}\Box_\bullet Q:(s_1,c_3)$. Then we have to choose v, y and z such that $(s_1,c_3y)\rightsquigarrow(v,z)\in\overline{\mathcal{C}}$. We have $(s_1,c_3c_4)\rightsquigarrow(s_2,c_2)\in\overline{\mathcal{C}}$; indeed,

$$\dfrac{(s_1,c_1)\rightsquigarrow(s_2,c_2)\qquad c_1\sim c_3c_4\qquad \dfrac{(s_1,c_1)\rightsquigarrow(s_2,c_2)}{c_2\sim c_2}\langle k_{r_2}\rangle}{(s_1,c_3c_4)\rightsquigarrow(s_2,c_2)}\langle k_a\rangle$$

Thus it is possible to apply this rule choosing $v=s_2$, $y=c_4$ and $z=c_2$, adding to the branch the labelled formula $\mathbb{T}Q:(s_2,c_2)$.

For step 8, we apply the rule $\langle\mathbb{F}\Box_y\rangle$ on the labelled formula $\mathbb{F}\Box_e R:(s_2,c_2)$. This rule introduces the labelled formula $\mathbb{F}R:(s_2,c_2)$ and the constraint $(s_2,c_2\circ\|e\|)\rightsquigarrow(s_2,c_2)$, which is equivalent to $(s_2,c_2)\rightsquigarrow(s_2,c_2)$ because $\|e\|=1$ and because 1 is the unit of $\circ$.

Finally, we observe that the tableau's branches are closed (denoted $\times$), so this tableau is a proof for the formula $((\Box_\bullet Q*P)\wedge\Diamond R)\rightarrow\Diamond(Q\wedge\Box_e R)$. Therefore, by Theorem 40, the formula is valid.

We consider another example of tableau for the formula $\Diamond_r(P*Q)\rightarrow(\Diamond P*\Diamond Q)$. By applying tableaux rules, we obtain the tableau of Fig. 7 with branches that are not closed.

6.5. Countermodel extraction

We present a countermodel extraction method that will be used to show the completeness of the tableaux calculus with respect to the model-theoretic semantics defined in Section 2. The method consists in transforming the reachability constraint set and the resource constraint set of a branch $\langle\mathcal{F},\mathcal{C}\rangle$ into a model $\mathcal{K}$ such that if $\mathbb{T}\phi:(u,x)\in\mathcal{F}$, then $u,[x]\vDash_{\mathcal{K}}\phi$ and, if $\mathbb{F}\phi:(u,x)\in\mathcal{F}$, then $u,[x]\nvDash_{\mathcal{K}}\phi$, where $[x]$ is the equivalence class of x.

The first step is to *saturate* the labelled formula of the branch (also known as 'obtaining a Hintikka CSS').

Definition 41 *(Hintikka CSS).* A CSS $\langle\mathcal{F},\mathcal{C}\rangle$ is a *Hintikka CSS* iff, for any formulæ $\phi,\psi\in\mathcal{L}$, any world label $u\in L_w$, any resource label $x,y\in L_r$, and any resource symbol $r\in\Sigma_R$, we have the following:

1. $\mathbb{T}\phi:(u,x)\notin\mathcal{F}$ or $\mathbb{F}\phi:(u,y)\notin\mathcal{F}$ or $x\sim y\notin\overline{\mathcal{C}}$,
2. $\mathbb{F}I:(u,x)\notin\mathcal{F}$ or $x\sim 1\notin\overline{\mathcal{C}}$,
3. $\mathbb{F}\top:(u,x)\notin\mathcal{F}$,
4. $\mathbb{T}\bot:(u,x)\notin\mathcal{F}$,
5. if $\mathbb{T}I:(u,x)\in\mathcal{F}$, then $x\sim 1\in\overline{\mathcal{C}}$,
6. if $\mathbb{T}\neg\phi:(u,x)\in\mathcal{F}$, then $\mathbb{F}\phi:(u,x)\in\mathcal{F}$,
7. if $\mathbb{F}\neg\phi:(u,x)\in\mathcal{F}$, then $\mathbb{T}\phi:(u,x)\in\mathcal{F}$,
8. if $\mathbb{T}\phi\wedge\psi:(u,x)\in\mathcal{F}$, then $\mathbb{T}\phi:(u,x)\in\mathcal{F}$ and $\mathbb{T}\psi:(u,x)\in\mathcal{F}$,
9. if $\mathbb{F}\phi\wedge\psi:(u,x)\in\mathcal{F}$, then $\mathbb{F}\phi:(u,x)\in\mathcal{F}$ or $\mathbb{F}\psi:(u,x)\in\mathcal{F}$,
10. if $\mathbb{T}\phi\vee\psi:(u,x)\in\mathcal{F}$, then $\mathbb{T}\phi:(u,x)\in\mathcal{F}$ or $\mathbb{T}\psi:(u,x)\in\mathcal{F}$,
11. if $\mathbb{F}\phi\vee\psi:(u,x)\in\mathcal{F}$, then $\mathbb{F}\phi:(u,x)\in\mathcal{F}$ and $\mathbb{F}\psi:(u,x)\in\mathcal{F}$,

12. if $\mathbb{T}\phi \to \psi : (u, x) \in \mathcal{F}$, then $\mathbb{F}\phi : (u, x) \in \mathcal{F}$ or $\mathbb{T}\psi : (u, x) \in \mathcal{F}$,
13. if $\mathbb{F}\phi \to \psi : (u, x) \in \mathcal{F}$, then $\mathbb{T}\phi : (u, x) \in \mathcal{F}$ and $\mathbb{F}\psi : (u, x) \in \mathcal{F}$,
14. if $\mathbb{T}\phi * \psi : (u, x) \in \mathcal{F}$, then there are $y, z \in L_r$ such that $x \sim yz \in \overline{\mathcal{C}}$ and $\mathbb{T}\phi : (u, y) \in \mathcal{F}$ and $\mathbb{T}\psi : (u, z) \in \mathcal{F}$,
15. if $\mathbb{F}\phi * \psi : (u, x) \in \mathcal{F}$, then, for all $y, z \in L_r$, $x \sim yz \in \overline{\mathcal{C}} \Rightarrow \mathbb{F}\phi : (u, y) \in \mathcal{F}$ or $\mathbb{F}\psi : (u, z) \in \mathcal{F}$,
16. if $\mathbb{T}\phi \mathrel{-\!\!*} \psi : (u, x) \in \mathcal{F}$, then, for all $y \in L_r$, $xy \in \mathcal{D}_r(\overline{\mathcal{C}}) \Rightarrow \mathbb{F}\phi : (u, y) \in \mathcal{F}$ or $\mathbb{T}\psi : (u, xy) \in \mathcal{F}$,
17. if $\mathbb{F}\phi \mathrel{-\!\!*} \psi : (u, x) \in \mathcal{F}$, then there are $y \in L_r$ such that $xy \in \mathcal{D}_r(\overline{\mathcal{C}})$ and $\mathbb{T}\phi : (u, y) \in \mathcal{F}$ and $\mathbb{F}\psi : (u, xy) \in \mathcal{F}$,
18. if $\mathbb{T}\Diamond_r\phi : (u, x) \in \mathcal{F}$, then there are $v \in L_W$ and $z \in L_r$ such that $(u, x \circ \|r\|) \rightsquigarrow (v, z) \in \overline{\mathcal{C}}$ and $\mathbb{T}\phi : (v, z) \in \mathcal{F}$,
19. if $\mathbb{F}\Diamond_r\phi : (u, x) \in \mathcal{F}$, then, for all $v \in L_W$ and for all $z \in L_r$, $(u, x \circ \|r\|) \rightsquigarrow (v, z) \in \overline{\mathcal{C}} \Rightarrow \mathbb{F}\phi : (v, z) \in \mathcal{F}$,
20. if $\mathbb{T}\Box_r\phi : (u, x) \in \mathcal{F}$, then, for all $v \in L_W$ and for all $z \in L_r$, $(u, x \circ \|r\|) \rightsquigarrow (v, z) \in \overline{\mathcal{C}} \Rightarrow \mathbb{T}\phi : (v, z) \in \mathcal{F}$, and
21. if $\mathbb{F}\Box_r\phi : (u, x) \in \mathcal{F}$, then there are $v \in L_W$ and $z \in L_r$ such that $(u, x \circ \|r\|) \rightsquigarrow (v, z) \in \overline{\mathcal{C}}$ and $\mathbb{F}\phi : (v, z) \in \mathcal{F}$.
22. if $\mathbb{T}\Diamond\phi : (u, x) \in \mathcal{F}$, then there are $v \in L_W$ and $y \in L_r$ such that $(u, x) \rightsquigarrow (v, y) \in \overline{\mathcal{C}}$ and $\mathbb{T}\phi : (v, y) \in \mathcal{F}$,
23. if $\mathbb{F}\Diamond\phi : (u, x) \in \mathcal{F}$ then, for all $v \in L_W$ and for all $y \in L_r$, $(u, x) \rightsquigarrow (v, y) \in \overline{\mathcal{C}} \Rightarrow \mathbb{F}\phi : (v, y) \in \mathcal{F}$
24. if $\mathbb{T}\Box\phi : (u, x) \in \mathcal{F}$, then, for all $v \in L_W$ and for all $y \in L_r$, $(u, x) \rightsquigarrow (v, y) \in \overline{\mathcal{C}} \Rightarrow \mathbb{T}\phi : (v, y) \in \mathcal{F}$,
25. if $\mathbb{F}\Box\phi : (u, x) \in \mathcal{F}$, then there are $v \in L_W$ and $y \in L_r$ such that $(u, x) \rightsquigarrow (v, y) \in \overline{\mathcal{C}}$ and $\mathbb{F}\phi : (v, y) \in \mathcal{F}$,
26. if $\mathbb{T}\Diamond_\bullet\phi : (u, x) \in \mathcal{F}$, then there are $v \in L_W$ and $y, z \in L_r$, $(u, xy) \rightsquigarrow (v, z) \in \overline{\mathcal{C}}$ and $\mathbb{T}\phi : (v, z) \in \mathcal{F}$,
27. if $\mathbb{F}\Diamond_\bullet\phi : (u, x) \in \mathcal{F}$, then, for all $v \in L_W$ and for all $y, z \in L_r$, $(u, xy) \rightsquigarrow (v, z) \in \overline{\mathcal{C}} \Rightarrow \mathbb{F}\phi : (v, z) \in \mathcal{F}$,
28. if $\mathbb{T}\Box_\bullet\phi : (u, x) \in \mathcal{F}$, then, for all $v \in L_W$ and for all $y, z \in L_r$, $(u, xy) \rightsquigarrow (v, z) \in \overline{\mathcal{C}} \Rightarrow \mathbb{T}\phi : (v, z) \in \mathcal{F}$,
29. if $\mathbb{F}\Box_\bullet\phi : (u, x) \in \mathcal{F}$, then there are $v \in L_W$ and $y, z \in L_r$ such that $(u, xy) \rightsquigarrow (v, z) \in \overline{\mathcal{C}}$ and $\mathbb{F}\phi : (v, z) \in \mathcal{F}$.

This definition is an extension of the similar definition given in previous works [9,23] with the conditions from (18) to (29) that correspond to the treatment of the modalities. Note that the conditions (1), (2), (3), and (4) certify that a Hintikka CSS is not closed and the other conditions certify that all labelled formulæ of a Hintikka CSS are saturated.

In order to extract a countermodel from a Hintikka CSS, we must build equivalence classes. The equivalence class of $x \in \mathcal{D}_r(\overline{\mathcal{C}})$, denoted $[x]$, is the set $[x] = \{y \in L_r \mid x \sim y \in \overline{\mathcal{C}}\}$. We also denote by $\mathcal{D}_r(\overline{\mathcal{C}})/\sim\; = \{[x] \mid x \in \mathcal{D}_r(\overline{\mathcal{C}})\}$ the set of all equivalence classes of $\mathcal{D}_r(\overline{\mathcal{C}})$. We highlight that $\sim$ is an equivalence relation, because it is reflexive (by Corollary 27), symmetric (by rule $\langle s_r\rangle$) and transitive (by rule $\langle t_r\rangle$).

Now, we give the definition of a function Ω that extracts a countermodel from a Hintikka CSS.

Definition 42 *(Function Ω).* Let $\langle \mathcal{F}, \mathcal{C}\rangle$ be a Hintikka CSS. The function Ω associates to $\langle \mathcal{F}, \mathcal{C}\rangle$ a 4-tuple $\Omega(\langle \mathcal{F}, \mathcal{C}\rangle) = (W, \mathcal{M}, \mathbf{R}, V)$, where $\mathcal{M} = (Res, \bullet, e)$, such that

- $W = \mathcal{A}_W(\mathcal{C})$,
- $Res = \mathcal{D}_r(\overline{\mathcal{C}})/\sim$,
- $e = [1]$,
- $[x] \bullet [y] = \begin{cases} \uparrow & \text{if } x \circ y \notin \mathcal{D}_r(\overline{\mathcal{C}}) \\ [x \circ y] & \text{otherwise,} \end{cases}$
- $(u, [x])\mathbf{R}(v, [y])$ iff $(u, x) \rightsquigarrow (v, y) \in \overline{\mathcal{C}}$, and
- $(u, [x]) \in V(p)$ iff $\exists y \in L_r$ such that $y \sim x \in \overline{\mathcal{C}}$ and $\mathbb{T}p : (u, y) \in \mathcal{F}$.

For all $r \in \Sigma_R$ such that $\|r\| \in \mathcal{D}_r(\overline{\mathcal{C}})$, we have that $[\![r]\!] = [\|r\|]$. Moreover, we consider that, for all $r \in \Sigma_R$ such that $\|r\| \notin \mathcal{D}_r(\overline{\mathcal{C}})$, we have $[\![r]\!]$ is not defined (is not a resource). Note that our definition is well-formed for the case in which $r = e \in \Sigma_R$. Indeed, as $\|e\| = 1$ and $1 \in \mathcal{D}_r(\overline{\mathcal{C}})$ by the rule $\langle 1\rangle$, then $[\![e]\!] = [\|e\|] = [1] = e$.

Lemma 43. *Let $\langle \mathcal{F}, \mathcal{C}\rangle$ be a Hintikka CSS. $\Omega(\langle \mathcal{F}, \mathcal{C}\rangle)$ is a model.*

Proof. We must show that $\Omega(\langle \mathcal{F}, \mathcal{C}\rangle) = (W, \mathcal{M}, \mathbf{R}, V)$, where $\mathcal{M} = (Res, \bullet, e)$, is a model.

- We show that $\mathcal{M} = (Res, \bullet, e)$ is a PRM.
  – $1 \in \mathcal{D}_r(\overline{\mathcal{C}})$, by rule $\langle 1\rangle$, so $[1] \in Res$. Moreover, as $e = [1]$, then $e \in Res$.
  – $\bullet : Res \times Res \rightharpoonup Res$ is well-defined, associative, commutative and e is its unit.
    ∗ We show that $\bullet$ is well-defined. Let $x, x', y, y' \in \mathcal{D}_r(\overline{\mathcal{C}})$ such that $x \sim x' \in \overline{\mathcal{C}}$ and $y \sim y' \in \overline{\mathcal{C}}$. We show that $[x] \bullet [y] = [x'] \bullet [y']$. There are two cases.
      · $[x] \bullet [y] \uparrow$. In this case, $xy \notin \mathcal{D}_r(\overline{\mathcal{C}})$. We suppose that $x'y' \in \mathcal{D}_r(\overline{\mathcal{C}})$. By Corollary 28, we have $x'y' \sim xy \in \overline{\mathcal{C}}$. Then $xy \in \mathcal{D}_r(\overline{\mathcal{C}})$, which is absurd. Thus $x'y' \notin \mathcal{D}_r(\overline{\mathcal{C}})$. Therefore $[x'] \bullet [y'] \uparrow$.
      · $[x] \bullet [y] \downarrow$. In this case, $xy \in \mathcal{D}_r(\overline{\mathcal{C}})$. Moreover, by definition of Ω, $[x] \bullet [y] = [xy]$. By Corollary 28, we have $xy \sim x'y' \in \overline{\mathcal{C}}$. Then $[x'] \bullet [y'] \downarrow$ (because $x'y' \in \mathcal{D}_r(\overline{\mathcal{C}})$) and $[xy] = [x'y']$. By definition of Ω, $[x'] \bullet [y'] = [x'y']$. Therefore $[x] \bullet [y] = [xy] = [x'y'] = [x'] \bullet [y']$.
    ∗ Neutral element. Let $r \in Res$. Then there is $x \in \mathcal{D}_r(\overline{\mathcal{C}})$ such that $r = [x]$. Then, by definition of Ω and as 1 is the unit of $\circ$, we have $r \bullet e = [x] \bullet [1] = [x \circ 1] = [x] = r$.

- $*$ Commutativity. Let $r_1, r_2 \in Res$ such that $r_1 \bullet r_2 \downarrow$. Then there are $xy \in \mathcal{D}_r(\overline{\mathcal{C}})$ such that $r_1 = [x]$ and $r_2 = [y]$. By commutativity of $\circ$, we have $r_1 \bullet r_2 = [x] \bullet [y] = [x \circ y] = [y \circ x] = [y] \bullet [x] = r_2 \bullet r_1$.
- $*$ The proof of associativity is similar ($\circ$ is associative).

- We show that $\mathbf{R} \subseteq (W \times Res) \times (W \times Res)$ is reflexive and transitive.
  - Reflexivity. Let $w \in W$ and $r \in Res$. By definition of Ω, $w \in \mathcal{A}_w(\mathcal{C})$ and there is $x \in \mathcal{D}_r(\overline{\mathcal{C}})$ such that $r = [x]$. By Proposition 29, $w \in \mathcal{A}_w(\overline{\mathcal{C}})$. By Corollary 27, we have $(w, 1) \rightsquigarrow (w, 1) \in \overline{\mathcal{C}}$ and $x \sim x \in \overline{\mathcal{C}}$. Then, by rule $\langle r_{a_1} \rangle$, $(w, x) \rightsquigarrow (w, x) \in \overline{\mathcal{C}}$. Thus, we have $(w, r)\mathbf{R}(w, r)$.
  - Transitivity. Let $w_1, w_2, w_3 \in W$ and $r_1, r_2, r_3 \in Res$ such that $(w_1, r_1)\mathbf{R}(w_2, r_2)$ and $(w_2, r_2)\mathbf{R}(w_3, r_3)$. By definition of Ω, there are $x, y, z \in \mathcal{D}_r(\overline{\mathcal{C}})$ such that $r_1 = [x]$, $r_2 = [y]$, $r_3 = [z]$, $(w_1, x) \rightsquigarrow (w_2, y) \in \overline{\mathcal{C}}$ and $(w_2, y) \rightsquigarrow (w_3, z) \in \overline{\mathcal{C}}$. By rule $\langle t_a \rangle$, $(w_1, x) \rightsquigarrow (w_3, z) \in \overline{\mathcal{C}}$. Thus $(w_1, r_1)\mathbf{R}(w_3, r_3)$. □

Lemma 44. *Let $\langle \mathcal{F}, \mathcal{C} \rangle$ be a Hintikka CSS and $\mathcal{K} = \Omega(\langle \mathcal{F}, \mathcal{C} \rangle) = (W, \mathcal{M}, \mathbf{R}, V)$, where $\mathcal{M} = (Res, \bullet, e)$. For all formulæ $\phi \in \mathcal{L}$, all $u \in \mathcal{A}_w(\mathcal{C})$, and all $x \in \mathcal{D}_r(\overline{\mathcal{C}})$, we have*

1. *if $\mathbb{F}\phi : (u, x) \in \mathcal{F}$, then $u, [x] \not\models_{\mathcal{K}} \phi$, and*
2. *if $\mathbb{T}\phi : (u, x) \in \mathcal{F}$, then $u, [x] \models_{\mathcal{K}} \phi$.*

Proof. The properties (1) and (2) are proved simultaneously by structural induction on ϕ.

- Base cases.
  - Case $\mathbb{F}p : (u, x) \in \mathcal{F}$ such that $p \in Prop$. We suppose that $u, [x] \models_{\mathcal{K}} p$. Then $(u, [x]) \in V(p)$. By definition Ω, there is a resource label y such that $y \sim x \in \overline{\mathcal{C}}$ and $\mathbb{T}p : (u, y) \in \mathcal{F}$. By condition (1) of Definition 41, $\langle \mathcal{F}, \mathcal{C} \rangle$ is not a Hintikka CSS. This is absurd, so $u, [x] \not\models_{\mathcal{K}} p$.
  - Case $\mathbb{T}p : (u, x) \in \mathcal{F}$ such that $p \in Prop$. By property by (P_{css}), $x \sim x \in \overline{\mathcal{C}}$. Then, by definition of Ω, $(u, [x]) \in V(p)$. Thus $u, [x] \models_{\mathcal{K}} p$.
  - Case $\mathbb{F}\bot : (u, x) \in \mathcal{F}$. We have $u, [x] \not\models_{\mathcal{K}} \bot$, by definition.
  - Case $\mathbb{T}\bot : (u, x) \in \mathcal{F}$. As $\langle \mathcal{F}, \mathcal{C} \rangle$ is a Hintikka CSS, by condition (4) of Definition 41, this case is absurd.
  - Case $\mathbb{F}I : (u, x) \in \mathcal{F}$. We suppose that $u, [x] \models_{\mathcal{K}} I$. Then $[x] = e$, and, by definition of Ω, we have $[x] = [1]$. Therefore $x \sim 1 \in \overline{\mathcal{C}}$. Then, by condition (2) of Definition 41, $\langle \mathcal{F}, \mathcal{C} \rangle$ is not a Hintikka CSS. Being absurd, we can conclude that $u, [x] \not\models_{\mathcal{K}} I$.
  - Case $\mathbb{T}I : (u, x) \in \mathcal{F}$. By condition (5) of Definition 41, $x \sim 1 \in \overline{\mathcal{C}}$. Then, by definition of Ω, $[x] = [1] = e$. Therefore $u, [x] \models_{\mathcal{K}} I$.
  - The other base cases are similar.
- Inductive step. We suppose that properties (1) and (2) hold for formulæ ϕ and ψ (IH). We only develop the cases about modalities.
  - Case $\mathbb{F}\Diamond_r\phi : (u, x) \in \mathcal{F}$. Let $w \in W$ and $s \in Res$ such that $[x] \bullet r \downarrow$ and $(u, [x] \bullet r)\mathbf{R}(w, s)$. We recall that, because of our abuse of notation, we are supposing that $[x] \bullet \llbracket r \rrbracket \downarrow$ and $(u, [x] \bullet \llbracket r \rrbracket)\mathbf{R}(w, s)$. We remark that $r \in \Sigma_R$. As $[x] \bullet \llbracket r \rrbracket \downarrow$ then $\llbracket r \rrbracket$ is defined and so $\llbracket r \rrbracket = [\|r\|]$. Then, by definition of Ω, there is a resource label y such that $y \in \mathcal{D}_r(\overline{\mathcal{C}})$, $s = [y]$ and $(u, x \circ \|r\|) \rightsquigarrow (w, y) \in \overline{\mathcal{C}}$. Thus, by condition (19) of Definition 41, $\mathbb{F}\phi : (w, y) \in \mathcal{F}$. Then, by the induction hypothesis, $w, s \not\models_{\mathcal{K}} \phi$. Therefore $u, [x] \not\models_{\mathcal{K}} \Diamond_r\phi$.
  - Case $\mathbb{T}\Diamond_r\phi : (u, x) \in \mathcal{F}$. By condition (18) of Definition 41, there is a world label v and one resource label z such that $(u, x \circ \|r\|) \rightsquigarrow (v, z) \in \overline{\mathcal{C}}$ and $\mathbb{T}\phi : (v, z) \in \mathcal{F}$. Remarking that $\|r\| \in \mathcal{D}_r(\overline{\mathcal{C}})$ then $\llbracket r \rrbracket = [\|r\|]$. Then, by the induction hypothesis and the definition of Ω, $[x] \bullet \llbracket r \rrbracket \downarrow$, $(u, [x] \bullet \llbracket r \rrbracket)\mathbf{R}(v, [z])$ and $v, [z] \models_{\mathcal{K}} \phi$. Therefore $u, [x] \models_{\mathcal{K}} \Diamond_r\phi$.
  - Case $\mathbb{F}\Diamond\phi : (u, x) \in \mathcal{F}$. Let $w \in W$ and $r \in Res$ such that $(u, [x])\mathbf{R}(w, r)$. By definition of Ω, there is resource label y such that $y \in \mathcal{D}_r(\overline{\mathcal{C}})$, $r = [y]$ and $(u, x) \rightsquigarrow (w, y) \in \overline{\mathcal{C}}$. Thus, by condition (23) of Definition 41, $\mathbb{F}\phi : (w, y) \in \mathcal{F}$. Then, by the induction hypothesis, $w, r \not\models_{\mathcal{K}} \phi$. Therefore $u, [x] \not\models_{\mathcal{K}} \Diamond\phi$.
  - Case $\mathbb{T}\Diamond\phi : (u, x) \in \mathcal{F}$. By condition (22) of Definition 41, there is a world label v and a resource label y such that $(u, x) \rightsquigarrow (v, y) \in \overline{\mathcal{C}}$ and $\mathbb{T}\phi : (v, y) \in \mathcal{F}$. Then, by the induction hypothesis and definition of Ω, there is a world v and a resource $[y]$ such that $(u, [x])\mathbf{R}(v, [y])$ and $v, [y] \models_{\mathcal{K}} \phi$. Therefore $u, [x] \models_{\mathcal{K}} \Diamond\phi$.
  - Case $\mathbb{F}\Diamond_\bullet\phi : (u, x) \in \mathcal{F}$. Let $w \in W$ and $r, r' \in Res$ such that $[x] \bullet r \downarrow$ and $(u, [x] \bullet r)\mathbf{R}(w, r')$. By definition of Ω, there are two resource labels y and z such that $xy \in \mathcal{D}_r(\overline{\mathcal{C}})$, $z \in \mathcal{D}_r(\overline{\mathcal{C}})$, $r = [y]$, $r' = [z]$ and $(u, xy) \rightsquigarrow (w, z) \in \overline{\mathcal{C}}$. Thus, by condition (27) of Definition 41, $\mathbb{F}\phi : (w, z) \in \mathcal{F}$. Then, by the induction hypothesis, $w, r' \not\models_{\mathcal{K}} \phi$. Therefore $u, [x] \not\models_{\mathcal{K}} \Diamond_\bullet\phi$.
  - Case $\mathbb{T}\Diamond_\bullet\phi : (u, x) \in \mathcal{F}$. By condition (26) of Definition 41, there is a world label v and two resource labels y and z such that $(u, xy) \rightsquigarrow (v, z) \in \overline{\mathcal{C}}$ and $\mathbb{T}\phi : (v, z) \in \mathcal{F}$. We remark that $xy \in \mathcal{D}_r(\overline{\mathcal{C}})$. Then, by the induction hypothesis and definition of Ω, $[x] \bullet [y] \downarrow$, $(u, [x] \bullet [y])\mathbf{R}(v, [z])$ and $v, [z] \models_{\mathcal{K}} \phi$. Therefore $u, [x] \models_{\mathcal{K}} \Diamond_\bullet\phi$.
  - The other cases are similar. □

Lemma 45. *Let $\langle \mathcal{F}, \mathcal{C} \rangle$ be a Hintikka CSS such that $\mathbb{F}\phi : (u, x) \in \mathcal{F}$. The formula ϕ is not valid and $\Omega(\langle \mathcal{F}, \mathcal{C} \rangle)$ is a countermodel of ϕ.*

Proof. Let $\langle \mathcal{F}, \mathcal{C} \rangle$ be a Hintikka CSS such that $\mathbb{F}\phi : (u, x) \in \mathcal{F}$. Let $\mathcal{K} = \Omega(\langle \mathcal{F}, \mathcal{C} \rangle)$. By Lemma 43, $\mathcal{K}$ is a model. As $\langle \mathcal{F}, \mathcal{C} \rangle$ is a CSS, by (P_{css}) and Proposition 29, $u \in \mathcal{A}_w(\mathcal{C})$ and $x \in \mathcal{D}_r(\overline{\mathcal{C}})$. Thus, by Lemma 44, we have $u, [x] \not\models_{\mathcal{K}} \phi$. Therefore $\mathcal{K}$ is a countermodel of the formula ϕ and we can conclude that ϕ is not valid. □

If we consider the tableau for the formula $\Diamond_r(P * Q) \to (\Diamond P * \Diamond Q)$ in Fig. 7, it contains a branch (denoted $\mathcal{B}$) which is a Hintikka CSS. By Lemma 45, $\Diamond_r(P * Q) \to (\Diamond P * \Diamond Q)$ is not valid and $\Omega(\mathcal{B})$ is a countermodel for this formula.

We extract this countermodel, using Definition 42.
We have $\mathcal{K} = \Omega(\mathcal{B}) = (W, \mathcal{M}, \mathbf{R}, V)$, where $\mathcal{M} = (Res, \bullet, e)$, such that

- $W = \mathcal{A}_w(\mathcal{C}) = \{s_1, s_2\}$,
- $Res = \mathcal{D}_r(\overline{\mathcal{C}})/\sim = \{e, [c_1], [c_2], [c_3], [c_4], r, [c_1 r]\}$, where $e = [1]$, $[c_2] = [c_3 c_4]$ and $[\![r]\!] = [\|r\|] = [r]$ (recall that we abuse notation and write r for $[\![r]\!]$),
- $\bullet$ is defined by

$\bullet$	e	$[c_1]$	$[c_2]$	$[c_3]$	$[c_4]$	r	$[c_1 r]$
e	e	$[c_1]$	$[c_2]$	$[c_3]$	$[c_4]$	r	$[c_1 r]$
$[c_1]$	$[c_1]$	$\uparrow$	$\uparrow$	$\uparrow$	$\uparrow$	$[c_1 r]$	$\uparrow$
$[c_2]$	$[c_2]$	$\uparrow$	$\uparrow$	$\uparrow$	$\uparrow$	$\uparrow$	$\uparrow$
$[c_3]$	$[c_3]$	$\uparrow$	$\uparrow$	$\uparrow$	$[c_2]$	$\uparrow$	$\uparrow$
$[c_4]$	$[c_4]$	$\uparrow$	$\uparrow$	$[c_2]$	$\uparrow$	$\uparrow$	$\uparrow$
r	r	$[c_1 r]$	$\uparrow$	$\uparrow$	$\uparrow$	$\uparrow$	$\uparrow$
$[c_1 r]$	$[c_1 r]$	$\uparrow$	$\uparrow$	$\uparrow$	$\uparrow$	$\uparrow$	$\uparrow$

- Concerning the reachability relation, we have $(s_1, [c_1 r])\mathbf{R}(s_2, [c_2])$ and $(w, r)\mathbf{R}(w, r)$, for all $w \in W$ and $r \in Res$, and
- $V(P) = \{(s_2, [c_3])\}$ and $V(Q) = \{(s_2, [c_4])\}$.

It is easy to check that it is a countermodel of $\Diamond_r(P * Q) \to (\Diamond P * \Diamond Q)$. We remark that it is also a countermodel of the formula $\Diamond_\bullet(P * Q) \to (\Diamond P * \Diamond Q)$.

6.6. *Completeness*

The proof of completeness for LSM is an extension of the one developed for BBI [23] and detailed for a modal extension in [9]. It consists in constructing a Hintikka CSS from a CSS which can be closed. To construct this Hintikka CSS, we use a fair strategy and a oracle and then we start by giving some definitions of [9,23] extended for dealing with our new modalities.

Definition 46 *(Fair strategy).* A *fair strategy* is a labelled sequence of formulæ $(\mathbb{S}_i \mathcal{X}_i : (u_i, x_i))_{i \in \mathbb{N}}$ in $\{\mathbb{T}, \mathbb{F}\} \times \mathcal{L} \times L_w \times L_r$ such that all labelled formulæ occur infinitely many times in this sequence; that is, $\{i \in \mathbb{N} \mid \mathbb{S}_i \mathcal{X}_i : (u_i, x_i) \equiv \mathbb{S}\mathcal{X} : (u, x)\}$ is infinite for any $\mathbb{S}\mathcal{X} : (u, x) \in \{\mathbb{T}, \mathbb{F}\} \times \mathcal{L} \times L_w \times L_r$.

Proposition 47. *There exists a fair strategy.*

Proof. Let $X = \{\mathbb{T}, \mathbb{F}\} \times \mathcal{L} \times L_w \times L_r$ the set of all labelled formulæ. As Prop is countable, $\mathcal{L}$ is countable. Moreover, L_w and L_r are countable (remember that γ_R is countable). Therefore, X is countable. Then $\mathbb{N} \times X$ is countable and there exists a surjective function $\varphi : \mathbb{N} \longrightarrow \mathbb{N} \times X$. Let $p : \mathbb{N} \times X \longrightarrow X$ defined by $p(i, x) = x$ and $u = p \circ \varphi$. We show that u is a fair strategy by showing that for any $x \in X$, $u^{-1}(\{x\})$ is infinite. Let $x \in X$. $u^{-1}(\{x\}) = \varphi^{-1}(p^{-1}(\{x\}))$. But $p^{-1}(\{x\}) = \{(i, x) | i \in \mathbb{N}\}$ so $p^{-1}(x)$ is infinite. As φ is surjective, $\varphi^{-1}(p^{-1}(\{x\}))$ is also infinite. □

Definition 48. Let $\mathcal{P}$ be a set of CSSs.

1. $\mathcal{P}$ is $\preccurlyeq$*-closed* if $\langle \mathcal{F}, \mathcal{C} \rangle \in \mathcal{P}$ holds whenever $\langle \mathcal{F}, \mathcal{C} \rangle \preccurlyeq \langle \mathcal{F}', \mathcal{C}' \rangle$ and $\langle \mathcal{F}', \mathcal{C}' \rangle \in \mathcal{P}$ holds.
2. $\mathcal{P}$ is of *finite character* if $\langle \mathcal{F}, \mathcal{C} \rangle \in \mathcal{P}$ holds whenever $\langle \mathcal{F}_f, \mathcal{C}_f \rangle \in \mathcal{P}$ holds for every $\langle \mathcal{F}_f, \mathcal{C}_f \rangle \preccurlyeq_f \langle \mathcal{F}, \mathcal{C} \rangle$.
3. $\mathcal{P}$ is *saturated* if for any $\langle \mathcal{F}, \mathcal{C} \rangle \in \mathcal{P}$ and any instance

$$\frac{cond(\mathcal{F}, \mathcal{C})}{\langle \mathcal{F}_1, \mathcal{C}_1 \rangle \ \mid \ \ldots \ \mid \ \langle \mathcal{F}_k, \mathcal{C}_k \rangle}$$

of a rule of Figs. 4 and 5, if $cond(\mathcal{F}, \mathcal{C})$ is fulfilled then $\langle \mathcal{F} \cup \mathcal{F}_i, \mathcal{C} \cup \mathcal{C}_i \rangle \in \mathcal{P}$ for at least one $i \in \{1, \ldots, k\}$.

Definition 49 *(Oracle).* An *oracle* is a set of non-closed CSSs which is $\preccurlyeq$-closed, of finite character, and saturated.

Lemma 50. *There exists an oracle which contains every finite CSS for which there is no closed tableau.*

Proof. The proof is an adaptation for our modalities of the similar proof proposed in [9,23] which is already an adaptation of proof of completeness of tableaux for first-order logic [15]. The proof developed in [9] gives all the necessary notions to derive this proof in detail. □

In order to show the completeness of our tableau calculus, we consider a formula φ for which there exists no proof and we show that there exists a countermodel for this formula.

We denote by $\mathcal{T}_0$ the initial tableau for φ. Then, we have

1. $\mathcal{T}_0 = [\langle\{\mathbb{F}\varphi : (s_1, c_1)\}, \{(s_1, c_1) \leadsto (s_1, c_1)\}\rangle]$, and
2. $\mathcal{T}_0$ cannot be closed.

Now, we present a way to obtain a Hintikka CSS that will allow us to conclude to the completeness. By Lemma 50, there exists an oracle that contains every finite CSS for which there exists no closed tableau. We denote by $\mathcal{P}$ this oracle.

By Proposition 47, there exists a fair strategy. We denote by $\mathcal{S}$ this strategy and $\mathbb{S}_i X_i : (u_i, x_i)$ the i^{th} formula of $\mathcal{S}$. As $\mathcal{T}_0$ cannot be closed, its unique branch belongs to the oracle, that is $\langle\{\mathbb{F}\varphi : (s_1, c_1)\}, \{(s_1, c_1) \leadsto (s_1, c_1)\}\rangle \in \mathcal{P}$.

Now we build a sequence $\langle \mathcal{F}_i, \mathcal{C}_i\rangle_{i \geqslant 0}$ as follows:

- $\langle \mathcal{F}_0, \mathcal{C}_0\rangle = \langle\{\mathbb{F}\varphi : (s_1, c_1)\}, \{(s_1, c_1) \leadsto (s_1, c_1)\}\rangle$;
- If $\langle \mathcal{F}_i \cup \{\mathbb{S}_i X_i : (u_i, x_i)\}, \mathcal{C}_i\rangle \notin \mathcal{P}$, then we have $\langle \mathcal{F}_{i+1}, \mathcal{C}_{i+1}\rangle = \langle \mathcal{F}_i, \mathcal{C}_i\rangle$;
- If $\langle \mathcal{F}_i \cup \{\mathbb{S}_i X_i : (u_i, x_i)\}, \mathcal{C}_i\rangle \in \mathcal{P}$, then we have $\langle \mathcal{F}_{i+1}, \mathcal{C}_{i+1}\rangle = \langle \mathcal{F}_i \cup \{\mathbb{S}_i X_i : (u_i, x_i)\} \cup F_e, \mathcal{C}_i \cup \mathcal{C}_e\rangle$ such that F_e and $\mathcal{C}_e$ are determined by:

$\mathbb{S}_i$	F_i	F_e	$\mathcal{C}_e$
$\mathbb{T}$	I	$\emptyset$	$\{x_i \sim 1\}$
$\mathbb{T}$	$\phi * \psi$	$\{\mathbb{T}\phi : (u_i, \mathfrak{b}), \mathbb{T}\psi : (u_i, \mathfrak{c})\}$	$\{x_i \sim \mathfrak{b}\mathfrak{c}\}$
$\mathbb{F}$	$\phi \mathrel{-\!\!*} \psi$	$\{\mathbb{T}\phi : (u_i, \mathfrak{b}), \mathbb{F}\psi : (u_i, x_i\mathfrak{b})\}$	$\{x_i\mathfrak{b} \sim x_i\mathfrak{b}\}$
$\mathbb{T}$	$\Diamond_r\phi$	$\{\mathbb{T}\phi : (\mathfrak{a}, \mathfrak{b})\}$	$\{(s_i, x_i \circ \Vert r\Vert) \leadsto (\mathfrak{a}, \mathfrak{b})\}$
$\mathbb{F}$	$\Box_r\phi$	$\{\mathbb{F}\phi : (\mathfrak{a}, \mathfrak{b})\}$	$\{(s_i, x_i \circ \Vert r\Vert) \leadsto (\mathfrak{a}, \mathfrak{b})\}$
$\mathbb{T}$	$\Diamond\phi$	$\{\mathbb{T}\phi : (\mathfrak{a}, \mathfrak{b})\}$	$\{(s_i, x_i) \leadsto (\mathfrak{a}, \mathfrak{b})\}$
$\mathbb{F}$	$\Box\phi$	$\{\mathbb{F}\phi : (\mathfrak{a}, \mathfrak{b})\}$	$\{(s_i, x_i) \leadsto (\mathfrak{a}, \mathfrak{b})\}$
$\mathbb{T}$	$\Diamond_\bullet\phi$	$\{\mathbb{T}\phi : (\mathfrak{a}, \mathfrak{c})\}$	$\{(s_i, x_i\mathfrak{b}) \leadsto (\mathfrak{a}, \mathfrak{c})\}$
$\mathbb{F}$	$\Box_\bullet\phi$	$\{\mathbb{F}\phi : (\mathfrak{a}, \mathfrak{c})\}$	$\{(s_i, x_i\mathfrak{b}) \leadsto (\mathfrak{a}, \mathfrak{c})\}$
Otherwise		$\emptyset$	$\emptyset$

with $\mathfrak{a} = s_{i+2}$, $\mathfrak{b} = c_{2i+2}$ and $\mathfrak{c} = c_{2i+3}$.

Proposition 51. *For any $i \in \mathbb{N}$, the following properties hold:*

1. $\mathbb{F}\varphi : (s_1, c_1) \in \mathcal{F}_i$ *and* $(s_1, c_1) \leadsto (s_1, c_1) \in \mathcal{C}_i$*;*
2. $\mathcal{F}_i \subseteq \mathcal{F}_{i+1}$ *and* $\mathcal{C}_i \subseteq \mathcal{C}_{i+1}$*;*
3. $\langle \mathcal{F}_i, \mathcal{C}_i\rangle_{i \geqslant 0} \in \mathcal{P}$*;*
4. $\mathcal{A}_w(\mathcal{C}_i) \subseteq \{s_1, s_2, \ldots, s_{i+1}\}$*;*
5. $\mathcal{A}_r(\mathcal{C}_i) \subseteq \{c_1, c_2, \ldots, c_{2i+1}\} \cup \Sigma_R$.

Proof. Given in Appendix A. □

The limit CSS $\langle \mathcal{F}_\infty, \mathcal{C}_\infty\rangle$ of the sequence $\langle \mathcal{F}_i, \mathcal{C}_i\rangle_{i \geqslant 0}$ is defined by

$$\mathcal{F}_\infty = \bigcup_{i \geqslant 0} \mathcal{F}_i \quad \text{and} \quad \mathcal{C}_\infty = \bigcup_{i \geqslant 0} \mathcal{C}_i.$$

Proposition 52. *The following properties hold:*

1. $\langle \mathcal{F}_\infty, \mathcal{C}_\infty\rangle \in \mathcal{P}$*;*
2. *For all labelled formulæ $\mathbb{S}\phi : (u, x)$, if $\langle \mathcal{F}_\infty \cup \{\mathbb{S}\phi : (u, x)\}, \mathcal{C}_\infty\rangle \in \mathcal{P}$, then $\mathbb{S}\phi : (u, x) \in \mathcal{F}_\infty$.*

Proof. Given in Appendix B. □

Lemma 53. *The limit CSS is a Hintikka CSS.*

Proof. By Property 1 of Proposition 52, $\langle \mathcal{F}_\infty, \mathcal{C}_\infty \rangle \in \mathcal{P}$. We verify that all conditions of Definition 41 hold. Here we only give the conditions about modalities.

- We suppose that $\mathbb{T}\Diamond_r\phi : (u, x) \in \mathcal{F}_\infty$. By same arguments to that of condition 5, there is $k \in \mathbb{N}$ such that
  – the kth formula of our fair strategy is $\mathbb{T}\Diamond_r\phi : (u, x)$,
  – $\mathbb{T}\Diamond_r\phi : (u, x) \in \mathcal{F}_k$, and
  – $\langle \mathcal{F}_k, \mathcal{C}_k \rangle \in \mathcal{P}$.
  Then, by construction of the limit CSS, $\langle \mathcal{F}_{k+1}, \mathcal{C}_{k+1} \rangle = \langle \mathcal{F}_k \cup \{\mathbb{T}\phi : (\mathfrak{a}, \mathfrak{b})\}, \mathcal{C}_k \cup \{(u, x \circ \|r\|) \rightsquigarrow (\mathfrak{a}, \mathfrak{b})\}\rangle$, where $\mathfrak{a} = s_{k+2}$ and $\mathfrak{b} = c_{2k+2}$. Then $(u, x \circ \|r\|) \rightsquigarrow (\mathfrak{a}, \mathfrak{b}) \in \overline{\mathcal{C}_\infty}$ and $\mathbb{T}\phi : (\mathfrak{a}, \mathfrak{b}) \in \mathcal{F}_\infty$. Therefore condition (18) of Definition 41 holds.
- We suppose that $\mathbb{F}\Diamond_r\phi : (u, x) \in \mathcal{F}_\infty$. Let $v \in L_w$ and $y \in L_r$ such that $(u, x \circ \|r\|) \rightsquigarrow (v, y) \in \overline{\mathcal{C}_\infty}$. As $\mathcal{P}$ is saturated then $\langle \mathcal{F}_\infty \cup \{\mathbb{F}\phi : (v, y)\}, \mathcal{C}_\infty \rangle \in \mathcal{P}$, by rule $\langle \mathbb{F}\Diamond_\bullet \rangle$. By Property 2 of Proposition 52, $\mathbb{F}\phi : (v, y) \in \mathcal{F}_\infty$. Therefore the condition (19) of Definition 41 holds.
- Id. condition (20).
- Id. condition (21).
- Suppose that $\mathbb{T}\Diamond\phi : (u, x) \in \mathcal{F}_\infty$. By same arguments to that of condition 5, there is $k \in \mathbb{N}$ such that
  – the kth formula of our fair strategy is $\mathbb{T}\Diamond\phi : (u, x)$,
  – $\mathbb{T}\Diamond\phi : (u, x) \in \mathcal{F}_k$, and
  – $\langle \mathcal{F}_k, \mathcal{C}_k \rangle \in \mathcal{P}$.
  Then, by construction of the limit CSS, $\langle \mathcal{F}_{k+1}, \mathcal{C}_{k+1} \rangle = \langle \mathcal{F}_k \cup \{\mathbb{T}\phi : (\mathfrak{a}, \mathfrak{b})\}, \mathcal{C}_k \cup \{(u, x) \rightsquigarrow (\mathfrak{a}, \mathfrak{b})\}\rangle$, where $\mathfrak{a} = s_{k+2}$ and $\mathfrak{b} = c_{2k+2}$. Then $(u, x) \rightsquigarrow (\mathfrak{a}, \mathfrak{b}) \in \overline{\mathcal{C}_\infty}$ and $\mathbb{T}\phi : (\mathfrak{a}, \mathfrak{b}) \in \mathcal{F}_\infty$. Therefore condition (22) of Definition 41 holds.
- Suppose that $\mathbb{F}\Diamond\phi : (u, x) \in \mathcal{F}_\infty$. Let $v \in L_w$ and $y \in L_r$ such that $(u, x) \rightsquigarrow (v, y) \in \overline{\mathcal{C}_\infty}$. As $\mathcal{P}$ is saturated then $\langle \mathcal{F}_\infty \cup \{\mathbb{F}\phi : (v, y)\}, \mathcal{C}_\infty \rangle \in \mathcal{P}$, by rule $\langle \mathbb{F}\Diamond \rangle$. By Property 2 of Proposition 52, $\mathbb{F}\phi : (v, y) \in \mathcal{F}_\infty$. Therefore condition (23) of Definition 41 holds.
- Id. condition (24).
- Id. condition (25).
- Suppose that $\mathbb{T}\Diamond_\bullet\phi : (u, x) \in \mathcal{F}_\infty$. By same arguments as for condition 5, there is $k \in \mathbb{N}$ such that
  – the kth formula of our fair strategy is $\mathbb{T}\Diamond_\bullet\phi : (u, x)$,
  – $\mathbb{T}\Diamond_\bullet\phi : (u, x) \in \mathcal{F}_k$, and
  – $\langle \mathcal{F}_k, \mathcal{C}_k \rangle \in \mathcal{P}$.
  Then, by construction of the limit CSS, $\langle \mathcal{F}_{k+1}, \mathcal{C}_{k+1} \rangle = \langle \mathcal{F}_k \cup \{\mathbb{T}\phi : (\mathfrak{a}, \mathfrak{c})\}, \mathcal{C}_k \cup \{(u, x\mathfrak{b}) \rightsquigarrow (\mathfrak{a}, \mathfrak{c})\}\rangle$, where $\mathfrak{a} = s_{k+2}$, $\mathfrak{b} = c_{2k+2}$ and $\mathfrak{c} = c_{2k+3}$. Then $(u, x\mathfrak{b}) \rightsquigarrow (\mathfrak{a}, \mathfrak{c}) \in \overline{\mathcal{C}_\infty}$ and $\mathbb{T}\phi : (\mathfrak{a}, \mathfrak{c}) \in \mathcal{F}_\infty$. Therefore condition (26) of Definition 41 holds.
- Suppose that $\mathbb{F}\Diamond_\bullet\phi : (u, x) \in \mathcal{F}_\infty$. Let $v \in L_w$ and $y, z \in L_r$ such that $(u, xy) \rightsquigarrow (v, z) \in \overline{\mathcal{C}_\infty}$. As $\mathcal{P}$ is saturated then $\langle \mathcal{F}_\infty \cup \{\mathbb{F}\phi : (v, z)\}, \mathcal{C}_\infty \rangle \in \mathcal{P}$, by rule $\langle \mathbb{F}\Diamond_\bullet \rangle$. By Property 2 of Proposition 52, $\mathbb{F}\phi : (v, z) \in \mathcal{F}_\infty$. Therefore condition (27) of Definition 41 holds.
- Id. condition (28).
- Id. condition (29). □

Theorem 54 *(Completeness). Let φ be a formula. If φ is valid, then there exits a proof for φ.*

Proof. We suppose that there is no proof for the formula φ. We show that φ is not valid. The method that we have presented here allows us to build a limit CSS $\langle \mathcal{F}_\infty, \mathcal{C}_\infty \rangle$ that is, by Lemma 53, a Hintikka CSS. By Property 1 of Proposition 51, $\mathbb{F}\varphi : (s_1, c_1) \in \mathcal{F}_i$, for any $i \geqslant 0$. By definition of limit CSS, $\mathbb{F}\varphi : (s_1, c_1) \in \mathcal{F}_\infty$. Then, by Lemma 45, φ is not valid. □

7. Conclusion

We have defined and studied an extension of the modal logic S4, called LSM, that introduces the notion of resource, and corresponding separating modalities, in its models. This logic directly and naturally supports reasoning about the manipulation of resources by a system. The resource semantics upon which LSM is based is that of BI [30,33,16,17], further informed by the treatment of modality considered in [6,5,8].

We have proposed a model-theoretic semantics for LSM and have given a labelled tableaux calculus that is proved sound and complete. Moreover, we provide a countermodel extraction method in case for non-valid formulæ.

We have considered a range of examples — essentially classic distributed systems examples — that can be described naturally in LSM. Specifically, we have considered mutual exclusion, producer–consumer systems, and timed Petri nets. These examples illustrate the use and expressiveness of the separating modalities. They serve to illustrate the relative natural expressiveness of the modalities which, although all definable in terms of the basic resource-shifted $\Diamond_r$ and $\Box_r$, are convenient for the illustrated modelling examples.

There are many promising directions for future work that we intend to pursue. We summarize them here in order to support some of the initial choices made here. We begin with the core theoretical topics.

- Formulation of the evident intuitionistic variants of LSM and exploration of its logical theory (cf. [17,36]).
- Formulation and exploration of first- (and, perhaps, higher-) order systems based on LSM (cf. [6,4,5]).
- Systematic exploration of the structure of multi-dimensional models. Here we have considered a two-dimensional set-up that employs a simple pairing of worlds. More generally, one might consider, with or without the resource interpretation, n-dimensional models in which worlds may combined using the evident notion of bunching.
- Integration of the systems considered in this paper and in our proposed further work into a general co-algebraic perspective.

Considering applications, in particular those in program analysis and verification, we can consider the relationship between our work and concurrent separation logic [27]. Concurrent separation logic is built upon the resource semantics of bunched logic and handles concurrent processes in the style of Hoare logic. We conjecture that our treatment of resource semantics can be used to support concurrent separation logic too.

We remark that, in general, there is a more-or-less straightforward relationship between Hoare-style presentations of program logics and logically more standard presentations based on a satisfaction relation between a model and a propositional formula. Hoare-style systems are based on assertions of the form

$$\{\,\phi\,\}\,C\,\{\,\psi\,\},$$

for logical formulæ ϕ and ψ and program commands C, with essentially Hilbert-type proof-systems, whereas more standard semantic presentations are formulated along the lines of

$$w \models_{\mathcal{M}} \phi,$$

where $\mathcal{M}$ is a model and w is a choice of world. In establishing the relationship between this view and Hoare-style presentations, we take a model with worlds given by program states (S, T, etc.) and consider how states evolve as programs perform actions C by executing commands; that is, $S \xrightarrow{C} T$. To see how this works we need to consider how such commands generate logical modalities. Define

$$S \models_{\mathcal{M}} [C]\phi \text{ iff for every evolution } S \xrightarrow{C} T,\ T \models_{\mathcal{M}} \phi,$$

which asserts that the program must have property ϕ after executing command c provided that whenever C evolves S to T, the state T has property ϕ. Thus, a Hoare-style assertion, $\{\,\phi\,\}\,C\,\{\,\psi\,\}$, in which the command C evolves the program state from S to T essentially corresponds to a semantic assertion

$$S \models_{\mathcal{M}} \phi \to [C]\psi.$$

Reynolds' Separation Logic [35], which employs a Hoare-style presentation, and Ishtiaq and O'Hearn's Pointer Logic [22], which employs a semantic presentation, enrich this view of reasoning about programs by introducing the BI's concept of resource semantics in order to reason about mutable data structures.

In concurrent separation logic, the rule for the concurrent product of $n \geq 2$ commands has the form

$$\frac{\{\,\phi_1\,\}\,C_1\,\{\,\psi_1\,\}\ldots\{\,\phi_n\,\}\,C_n\,\{\,\psi_n\,\}}{\{\,\phi_1 * \ldots * \phi_n\,\}\,C_1 \times \cdots \times C_n\,\{\,\psi_1 * \ldots * \psi_n\,\}},$$

where no variable free in ϕ_i or ψ_i is changed in C_j when $j \neq i$. In the resource–process calculi considered in [6,4,5], the multiplicative conjunction is also intimately connected to the concurrent product:

$$\begin{array}{lll} R, E \models \phi_1 * \phi_2 & \text{iff} & \text{there exist } R_1, E_1, R_2, E_2 \text{ such that} \\ & & R, E \sim R_1 \otimes R_2, E_1 \times E_2 \text{ and} \\ & & R_1, E_1 \models \phi_1 \text{ and } R_2, E_2 \models \phi_2. \end{array}$$

Here we employ two-dimensional worlds in order to make assertions about the states of systems in which resources and processes co-evolve according to an operational semantics based on judgements of the form $R, E \xrightarrow{a} R', E'$, understood as asserting that the process E evolves by performing action a relative to available resources R so as to become the process E' with available resources R'.

This example suggests that it would be interesting, and possibly of value for program analysis and verification, to consider classes of models in which some of the dimensions of the model are generated by the operational semantics of a programming language. Such models will have associated action modalities (cf. [6,4,5,8]).

Acknowledgements

This work has been partially supported by the UK EPSRC research grant EP/H008373/2.

Appendix A. Proof of Proposition 51

Proposition 51. *For any $i \in \mathbb{N}$, the following properties hold:*

1. $\mathbb{F}\varphi : (s_1, c_1) \in \mathcal{F}_i$ *and* $(s_1, c_1) \rightsquigarrow (s_1, c_1) \in \mathcal{C}_i$*;*
2. $\mathcal{F}_i \subseteq \mathcal{F}_{i+1}$ *and* $\mathcal{C}_i \subseteq \mathcal{C}_{i+1}$*;*
3. $\langle \mathcal{F}_i, \mathcal{C}_i \rangle_{i \geqslant 0} \in \mathcal{P}$*;*
4. $\mathcal{A}_w(\mathcal{C}_i) \subseteq \{s_1, s_2, \ldots, s_{i+1}\}$*;*
5. $\mathcal{A}_r(\mathcal{C}_i) \subseteq \{c_1, c_2, \ldots, c_{2i+1}\} \cup \Sigma_R$.

Proof.

1. This property holds for $i = 0$. As $\langle \mathcal{F}_{i+1}, \mathcal{C}_{i+1} \rangle$ is an extension ($\cup$) of $\langle \mathcal{F}_i, \mathcal{C}_i \rangle$, this property also holds for all $i \geqslant 0$.
2. This property holds because $\langle \mathcal{F}_{i+1}, \mathcal{C}_{i+1} \rangle$ is an extension ($\cup$) of $\langle \mathcal{F}_i, \mathcal{C}_i \rangle$.

(3, 4, 5) We prove the Properties 3, 4, and 5 simultaneously by induction on i.v

The base case ($i = 0$) clearly holds, as $\langle \mathcal{F}_0, \mathcal{C}_0 \rangle = \langle \{\mathbb{F}\varphi : (s_1, c_1)\}, \{(s_1, c_1) \rightsquigarrow (s_1, c_1)\} \rangle$, then we remark that Properties 4 and 5 hold and Property 3 holds by hypothesis.

Now we prove the inductive case. We suppose that the Properties 3, 4, and 5 hold for $i = n$ (IH). We show that they hold for $i = n + 1$.

- If $\langle \mathcal{F}_n \cup \{\mathbb{S}_n \mathcal{X}_n : (u_n, x_n)\}, \mathcal{C}_n \rangle \notin \mathcal{P}$, then $\langle \mathcal{F}_{n+1}, \mathcal{C}_{n+1} \rangle = \langle \mathcal{F}_n, \mathcal{C}_n \rangle$. Then Properties 3, 4, and 5 hold by the induction hypothesis.
- If $\langle \mathcal{F}_n \cup \{\mathbb{S}_n \mathcal{X}_n : (u_n, x_n)\}, \mathcal{C}_n \rangle \in \mathcal{P}$ then it is a CSS (the elements of $\mathcal{P}$ are CSS, by definition). Then, by (P_{css}), $(u_n, 1) \rightsquigarrow (u_n, 1) \in \overline{\mathcal{C}_n}$ and $x_n \sim x_n \in \overline{\mathcal{C}_n}$. Thus, we have $u_n \in \mathcal{A}_w(\overline{\mathcal{C}_n})$ and $\gamma_R \cap \mathcal{E}(x_n) \subseteq \mathcal{A}_r(\overline{\mathcal{C}_n})$. Therefore, by Proposition 29, $u_n \in \mathcal{A}_w(\mathcal{C}_n)$ and $\gamma_R \cap \mathcal{E}(x_n) \subseteq \mathcal{A}_r(\mathcal{C}_n)$ **(1)**. There are ten cases.
  - If $\mathbb{S}_n = \mathbb{T}$ and $\mathcal{X}_n = I$. In this case, $\langle \mathcal{F}_{n+1}, \mathcal{C}_{n+1} \rangle = \langle \mathcal{F}_n \cup \{\mathbb{S}_n \mathcal{X}_n : (u_n, x_n)\}, \mathcal{C}_n \cup \{x_n \sim 1\} \rangle$. By saturation of $\mathcal{P}$, applying the rule $\langle \mathbb{T}I \rangle$, we have $\langle \mathcal{F}_{n+1}, \mathcal{C}_{n+1} \rangle \in \mathcal{P}$. Then Property 3 holds. By **(1)**, we remark that $\mathcal{A}_w(\mathcal{C}_{n+1}) = \mathcal{A}_w(\mathcal{C}_n)$ and $\mathcal{A}_r(\mathcal{C}_{n+1}) = \mathcal{A}_r(\mathcal{C}_n)$. Then, by the induction hypothesis, Properties 4 and 5 hold.
  - Case $\mathbb{S}_n = \mathbb{T}$ and $\mathcal{X}_n = \phi * \psi$. $\langle \mathcal{F}_{n+1}, \mathcal{C}_{n+1} \rangle = \langle \mathcal{F}_n \cup \{\mathbb{S}_n \mathcal{X}_n : (u_n, x_n)\} \cup \{\mathbb{T}\phi : (u_n, c_{2n+2}), \mathbb{T}\psi : (u_n, c_{2n+3})\}, \mathcal{C}_n \cup \{x \sim c_{2n+2}c_{2n+3}\} \rangle$. By the induction hypothesis, $c_{2n+2} \notin \mathcal{A}_r(\mathcal{C}_n)$ and $c_{2n+3} \notin \mathcal{A}_r(\mathcal{C}_n)$, and they are new resource label constants. Moreover, as $\langle \mathcal{F}_n \cup \{\mathbb{S}_n \mathcal{X}_n : (u_n, x_n)\}, \mathcal{C}_n \rangle \in \mathcal{P}$ then, by saturation for rule $\langle \mathbb{T}* \rangle$ and using the labels c_{2n+2} and c_{2n+3}, $\langle \mathcal{F}_{n+1}, \mathcal{C}_{n+1} \rangle \in \mathcal{P}$. Thus property 3 holds. Moreover, by **(1)** and (IH), $\mathcal{A}_w(\mathcal{C}_{n+1}) = \mathcal{A}_w(\mathcal{C}_n)$ and $\mathcal{A}_r(\mathcal{C}_{n+1}) = \mathcal{A}_r(\mathcal{C}_n) \cup \{c_{2n+2}, c_{2n+3}\}$. Therefore, Properties 4 and 5 hold by the induction hypothesis.
  - Case $\mathbb{S}_n = \mathbb{F}$ and $\mathcal{X}_n = \phi \mathrel{-\!\!*} \psi$. $\langle \mathcal{F}_{n+1}, \mathcal{C}_{n+1} \rangle = \langle \mathcal{F}_n \cup \{\mathbb{S}_n \mathcal{X}_n : (u_n, x_n)\} \cup \{\mathbb{T}\phi : (u_n, c_{2n+2}),\ \mathbb{F}\psi : (u_n, x_n c_{2n+2})\}, \mathcal{C}_n \cup \{x_n c_{2n+2} \sim x_n c_{2n+2}\} \rangle$. By the induction hypothesis, $c_{2n+2} \notin \mathcal{A}_r(\mathcal{C}_n)$, then it is new resource label constant. As $\langle \mathcal{F}_n \cup \{\mathbb{S}_n \mathcal{X}_n : (u_n, x_n)\}, \mathcal{C}_n \rangle \in \mathcal{P}$, by saturation for rule $\langle \mathbb{F}\mathrel{-\!\!*} \rangle$ and using the label c_{2n+2}, $\langle \mathcal{F}_{n+1}, \mathcal{C}_{n+1} \rangle \in \mathcal{P}$. Thus property 3 holds. Moreover, by **(1)**, we have $\mathcal{A}_w(\mathcal{C}_{n+1}) = \mathcal{A}_w(\mathcal{C}_n)$ and $\mathcal{A}_r(\mathcal{C}_{n+1}) = \mathcal{A}_r(\mathcal{C}_n) \cup \{c_{2n+2}\}$. Therefore, Properties 4 and 5 hold by the induction hypothesis.
  - Case $\mathbb{S}_n = \mathbb{T}$ and $\mathcal{X}_n = \Diamond_r \phi$. In this case, $\langle \mathcal{F}_{n+1}, \mathcal{C}_{n+1} \rangle = \langle \mathcal{F}_n \cup \{\mathbb{S}_n \mathcal{X}_n : (u_n, x_n)\} \cup \{\mathbb{T}\phi : (s_{n+2}, c_{2n+2})\}, \mathcal{C}_n \cup \{(u_n, x_n \circ \|r\|) \rightsquigarrow (s_{n+2}, c_{2n+2})\} \rangle$. By the induction hypothesis, $s_{n+2} \notin \mathcal{A}_w(\mathcal{C}_n)$ and $c_{2n+2} \notin \mathcal{A}_r(\mathcal{C}_n)$, and they are new world and resource label constants. As $\langle \mathcal{F}_n \cup \{\mathbb{S}_n \mathcal{X}_n : (u_n, x_n)\}, \mathcal{C}_n \rangle \in \mathcal{P}$, by saturation for rule $\langle \mathbb{T}\Diamond_y \rangle$ and using the labels s_{n+2} and c_{2n+2}, $\langle \mathcal{F}_{n+1}, \mathcal{C}_{n+1} \rangle \in \mathcal{P}$. Thus Property 3 holds. Moreover, by **(1)**, $\mathcal{A}_w(\mathcal{C}_{n+1}) = \mathcal{A}_w(\mathcal{C}_n) \cup \{s_{n+2}\}$ and $\mathcal{A}_r(\mathcal{C}_{n+1}) = \mathcal{A}_r(\mathcal{C}_n) \cup \{c_{2n+2}\}$. Therefore, Properties 4 and 5 hold by the induction hypothesis.
  - Case $\mathbb{S}_n = \mathbb{F}$ and $\mathcal{X}_n = \Box_r \phi$. This case is similar.
  - Case $\mathbb{S}_n = \mathbb{T}$ and $\mathcal{X}_n = \Diamond \phi$. In this case, $\langle \mathcal{F}_{n+1}, \mathcal{C}_{n+1} \rangle = \langle \mathcal{F}_n \cup \{\mathbb{S}_n \mathcal{X}_n : (u_n, x_n)\} \cup \{\mathbb{T}\phi : (s_{n+2}, c_{2n+2})\}, \mathcal{C}_n \cup \{(u_n, x_n) \rightsquigarrow (s_{n+2}, c_{2n+2})\} \rangle$. By the induction hypothesis, $s_{n+2} \notin \mathcal{A}_w(\mathcal{C}_n)$ and $c_{2n+2} \notin \mathcal{A}_r(\mathcal{C}_n)$, then they are new world and resource label constants. As $\langle \mathcal{F}_n \cup \{\mathbb{S}_n \mathcal{X}_n : (u_n, x_n)\}, \mathcal{C}_n \rangle \in \mathcal{P}$, by saturation for rule $\langle \mathbb{T}\Diamond \rangle$ and using the labels s_{n+2} and c_{2n+2}, $\langle \mathcal{F}_{n+1}, \mathcal{C}_{n+1} \rangle \in \mathcal{P}$. Thus property 3 holds. Moreover, by **(1)**, $\mathcal{A}_w(\mathcal{C}_{n+1}) = \mathcal{A}_w(\mathcal{C}_n) \cup \{s_{n+2}\}$ and $\mathcal{A}_r(\mathcal{C}_{n+1}) = \mathcal{A}_r(\mathcal{C}_n) \cup \{c_{2n+2}\}$. Therefore, Properties 4 and 5 hold by the induction hypothesis.
  - Case $\mathbb{S}_n = \mathbb{F}$ and $\mathcal{X}_n = \Box \phi$. This case is similar.
  - Case $\mathbb{S}_n = \mathbb{T}$ and $\mathcal{X}_n = \Diamond_{\bullet} \phi$. In this case, $\langle \mathcal{F}_{n+1}, \mathcal{C}_{n+1} \rangle = \langle \mathcal{F}_n \cup \{\mathbb{S}_n \mathcal{X}_n : (u_n, x_n)\} \cup \{\mathbb{T}\phi : (s_{n+2}, c_{2n+3})\}, \mathcal{C}_n \cup \{(u_n, x_n c_{2n+2}) \rightsquigarrow (s_{n+2}, c_{2n+3})\} \rangle$. By the induction hypothesis, $s_{n+2} \notin \mathcal{A}_w(\mathcal{C}_n)$, $c_{2n+2} \notin \mathcal{A}_r(\mathcal{C}_n)$ and $c_{2n+3} \notin \mathcal{A}_r(\mathcal{C}_n)$, then they are new world and resource label constants. As $\langle \mathcal{F}_n \cup \{\mathbb{S}_n \mathcal{X}_n : (u_n, x_n)\}, \mathcal{C}_n \rangle \in \mathcal{P}$, by saturation for rule $\langle \mathbb{T}\Diamond_{\bullet} \rangle$ and using the labels s_{n+2}, c_{2n+2} and c_{2n+3}, $\langle \mathcal{F}_{n+1}, \mathcal{C}_{n+1} \rangle \in \mathcal{P}$. Thus property 3 holds. Moreover, by **(1)**, $\mathcal{A}_w(\mathcal{C}_{n+1}) = \mathcal{A}_w(\mathcal{C}_n) \cup \{s_{n+2}\}$ and $\mathcal{A}_r(\mathcal{C}_{n+1}) = \mathcal{A}_r(\mathcal{C}_n) \cup \{c_{2n+2}, c_{2n+3}\}$. Therefore, Properties 4 and 5 hold by the induction hypothesis.
  - Case $\mathbb{S}_n = \mathbb{F}$ and $\mathcal{X}_n = \Box_{\bullet} \phi$. This case is similar.

- In the last case, $\langle \mathcal{F}_{i+1}, \mathcal{C}_{i+1} \rangle = \langle \mathcal{F}_i \cup \{\mathbb{S}_i \mathcal{X}_i : (u_i, x_i)\}, \mathcal{C}_i \rangle$. By hypothesis, $\langle \mathcal{F}_i \cup \{\mathbb{S}_i \mathcal{X}_i : (u_i, x_i)\}, \mathcal{C}_i \rangle \in \mathcal{P}$, then Property 3 holds. Properties 4 and 5 hold by the induction hypothesis, because $\mathcal{A}_w(\mathcal{C}_{n+1}) = \mathcal{A}_w(\mathcal{C}_n)$ and $\mathcal{A}_r(\mathcal{C}_{n+1}) = \mathcal{A}_r(\mathcal{C}_n)$. □

Appendix B. Proof of Proposition 52

Proposition 52. *The following properties hold:*

1. $\langle \mathcal{F}_\infty, \mathcal{C}_\infty \rangle \in \mathcal{P}$;
2. *For all labelled formulæ* $\mathbb{S}\phi : (u, x)$, *if* $\langle \mathcal{F}_\infty \cup \{\mathbb{S}\phi : (u, x)\}, \mathcal{C}_\infty \rangle \in \mathcal{P}$, *then* $\mathbb{S}\phi : (u, x) \in \mathcal{F}_\infty$.

Proof. We prove that $\langle \mathcal{F}_\infty, \mathcal{C}_\infty \rangle$ is a CSS, meaning that it satisfies properties (P_{css}). Let $\mathbb{S}\phi : (u, x) \in \mathcal{F}_\infty$. We show that $(u, 1) \rightsquigarrow (u, 1) \in \overline{\mathcal{C}_\infty}$ and $x \sim x \in \overline{\mathcal{C}_\infty}$. By definition of $\mathcal{F}_\infty$, there is i such that $\mathbb{S}\phi : (u, x) \in \mathcal{F}_i$. By Property 3 of Proposition 51, $\langle \mathcal{F}_i, \mathcal{C}_i \rangle \in \mathcal{P}$. Then $\langle \mathcal{F}_i, \mathcal{C}_i \rangle$ is a CSS and, by (P_{css}), $(u, 1) \rightsquigarrow (u, 1) \in \overline{\mathcal{C}_i}$ and $x \sim x \in \overline{\mathcal{C}_i}$. Thus $(u, 1) \rightsquigarrow (u, 1) \in \overline{\mathcal{C}_\infty}$ and $x \sim x \in \overline{\mathcal{C}_\infty}$. We now prove properties (1) and (2).

1. Let $\langle \mathcal{F}_f, \mathcal{C}_f \rangle \preccurlyeq_f \langle \mathcal{F}_\infty, \mathcal{C}_\infty \rangle$. As $\mathcal{F}_f$ and $\mathcal{C}_f$ are finite and as the sequence $\langle \mathcal{F}_i, \mathcal{C}_i \rangle_{i \geqslant 0}$ is increasing by Property 2 of Proposition 51, there is $j \in \mathbb{N}$ such that $\langle \mathcal{F}_f, \mathcal{C}_f \rangle \preccurlyeq \langle \mathcal{F}_j, \mathcal{C}_j \rangle$. By Property 3 of Proposition 51, $\langle \mathcal{F}_j, \mathcal{C}_j \rangle \in \mathcal{P}$. As $\mathcal{P}$ is $\preccurlyeq$-closed, we have $\langle \mathcal{F}_f, \mathcal{C}_f \rangle \in \mathcal{P}$. Thus for all $\langle \mathcal{F}_f, \mathcal{C}_f \rangle \preccurlyeq_f \langle \mathcal{F}_\infty, \mathcal{C}_\infty \rangle$, we have $\langle \mathcal{F}_f, \mathcal{C}_f \rangle \in \mathcal{P}$. Therefore $\langle \mathcal{F}_\infty, \mathcal{C}_\infty \rangle \in \mathcal{P}$, because $\mathcal{P}$ is of finite character.
2. Let $\mathbb{S}\phi : (u, x)$ such that $\langle \mathcal{F}_\infty \cup \{\mathbb{S}\phi : (u, x)\}, \mathcal{C}_\infty \rangle \in \mathcal{P}$. By property (P_{css}), $(u, 1) \rightsquigarrow (u, 1) \in \overline{\mathcal{C}_\infty}$ and $x \sim x \in \overline{\mathcal{C}_\infty}$. By compactness (Lemma 30), there are $\mathcal{C}_{f1} \subseteq \mathcal{C}_\infty$ and $\mathcal{C}_{f2} \subseteq \mathcal{C}_\infty$ such that $\mathcal{C}_{f1}$ and $\mathcal{C}_{f2}$ are finite and $(u, 1) \rightsquigarrow (u, 1) \in \overline{\mathcal{C}_{f1}}$ and $x \sim x \in \overline{\mathcal{C}_{f2}}$. As the sequence is increasing, by Property 2 of Proposition 51, there are $j_1, j_2 \in \mathbb{N}$ such that $\mathcal{C}_{f1} \subseteq \mathcal{C}_{j_1}$ and $\mathcal{C}_{f2} \subseteq \mathcal{C}_{j_2}$. Let $j = max(j_1, j_2)$. As the sequence is increasing, we have $\mathcal{C}_{f1} \subseteq \mathcal{C}_j$ and $\mathcal{C}_{f2} \subseteq \mathcal{C}_j$. As $\mathbb{S}\phi : (u, x)$ occurs infinitely many times in our fair strategy $\mathcal{S}$, there is $k \geqslant j$ such that $\mathbb{S}_k F_k : (u_k, x_k) = \mathbb{S}\phi : (u, x)$. Moreover, $\mathcal{C}_j \subseteq \mathcal{C}_k$. Then $(u, 1) \rightsquigarrow (u, 1) \in \overline{\mathcal{C}_k}$ and $x \sim x \in \overline{\mathcal{C}_k}$. Thus $\langle \mathcal{F}_k \cup \{\mathbb{S}\phi : (u, x)\}, \mathcal{C}_k \rangle$ is a CSS (satisfies the property (P_{css})) and $\langle \mathcal{F}_k \cup \{\mathbb{S}\phi : (u, x)\}, \mathcal{C}_k \rangle \preccurlyeq \langle \mathcal{F}_\infty \cup \{\mathbb{S}\phi : (u, x)\}, \mathcal{C}_\infty \rangle$, by definition of limit CSS. As $\mathcal{P}$ is $\preccurlyeq$-closed, $\langle \mathcal{F}_k \cup \{\mathbb{S}\phi : (u, x)\}, \mathcal{C}_k \rangle \in \mathcal{P}$. By construction of $\langle \mathcal{F}_{k+1}, \mathcal{C}_{k+1} \rangle$, $\mathbb{S}\phi : (u, x) \in \mathcal{F}_{k+1}$. Therefore $\mathbb{S}\phi : (u, x) \in \mathcal{F}_\infty$. □

References

[1] B. Berthomieu, M. Diaz, Modeling and verification of time dependent systems using time Petri nets, IEEE Trans. Softw. Eng. 17 (3) (1991) 259–273.

[2] P. Blackburn, M. de Rijke, Y. Venema, Modal Logic, Cambridge University Press, New York, NY, USA, 2001.

[3] B.F. Chellas, Modal Logic: An Introduction, Cambridge University Press, 1980.

[4] M. Collinson, B. Monahan, D. Pym, A logical and computational theory of located resource, J. Logic Comput. 19 (b) (2009) 1207–1244, Advance access published on 22 July, 2009. http://dx.doi.org/10.1093/logcom/exp021.

[5] M. Collinson, B. Monahan, D. Pym, A Discipline of Mathematical Systems Modelling, College Publications, 2012.

[6] M. Collinson, D. Pym, Algebra and logic for resource-based systems modelling, Math. Structures Comput. Sci. 19 (5) (2009) 959–1027.

[7] M. Collinson, B. Monahan, D. Pym, Semantics for structured systems modelling and simulation, in: Simutools 2010, ACM Digital Library and EU Digital Library, 2010.

[8] J.R. Courtault, D. Galmiche, A modal BI logic for dynamic resource properties, in: Logical Foundations of Computer Science, LFCS 2013, San Diego, CA, in: LNCS, vol. 7734, 2013, pp. 134–148.

[9] J.R. Courtault, D. Galmiche, A modal separation logic for resource dynamics, J. Logic Comput. (2015), http://dx.doi.org/10.1093/logcom/exv031.

[10] J.-R. Courtault, H. van Ditmarsch, D. Galmiche, An epistemic separation logic, in: 22nd Int. Workshop on Logic, Language, Information, and Computation, WoLLIC 2015, Bloomington, USA, in: LNCS, vol. 9160, 2015, pp. 156–173.

[11] M. Dunn, G. Restall, Relevance logic, in: Handbook of Philosophical Logic, Kluwer, 2002.

[12] E.A. Emerson, E.M. Clarke, Using branching time temporal logic to synthesize synchronization skeletons, Sci. Comput. Program. 2 (3) (1982) 241–266.

[13] U. Engberg, G. Winskel, Petri nets as models of linear logic, in: CAAP 90, Copenhagen, Denmark, in: LNCS, vol. 431, May 1990, pp. 144–161.

[14] U. Engberg, G. Winskel, Completeness results for linear logic on Petri nets, Ann. Pure Appl. Logic 86 (1997) 101–135.

[15] M. Fitting, First-Order Logic and Automated Theorem Proving, Texts and Monographs in Computer Science, Springer Verlag, 1990.

[16] D. Galmiche, D. Méry, D. Pym, Resource Tableaux (extended abstract), in: 16th Int. Workshop on Computer Science Logic, CSL 2002, Edinburgh, Scotland, in: LNCS, vol. 2471, September 2002, pp. 183–199.

[17] D. Galmiche, D. Méry, D. Pym, The semantics of BI and resource tableaux, Math. Structures Comput. Sci. 15 (6) (2005) 1033–1088.

[18] D. Galmiche, D. Méry, Tableaux and resource graphs for separation logic, J. Logic Comput. 20 (1) (2010) 189–231.

[19] J.Y. Girard, Linear logic, Theoret. Comput. Sci. 50 (1) (1987) 1–102.

[20] A. Herzig, A simple separation logic, in: Int. Workshop on Logic, Language, Information, and Computation, WoLLIC 2013, Darmstadt, Germany, in: LNCS, vol. 8071, 2013, pp. 168–178.

[21] M. Hennessy, G. Plotkin, On observing nondeterminism and concurrency, in: Proceedings of the 7th ICALP, in: Lecture Notes in Computer Science, vol. 85, Springer-Verlag, 1980, pp. 299–309.

[22] S. Ishtiaq, P. O'Hearn, BI as an assertion language for mutable data structures, in: 28th ACM Symposium on Principles of Programming Languages, POPL 2001, London, UK, 2001, pp. 14–26.

[23] D. Larchey-Wendling, The formal proof of the strong completeness of partial monoidal Boolean BI, J. Logic Comput. (2014), http://dx.doi.org/10.1093/logcom/exu031.

[24] P.M. Merlin, A study of the recoverability of computing systems, PhD thesis, University of California, Irvine, 1974.

[25] R. Milner, Communication and Concurrency, Prentice–Hall, Inc., Upper Saddle River, NJ, USA, 1989.

[26] P. O'Hearn, On bunched typing, J. Funct. Programming 13 (4) (2003) 747–796.

[27] P. O'Hearn, Resources, concurrency, and local reasoning, Theoret. Comput. Sci. 375 (1–3) (May 2007) 271–307.

[28] P. O'Hearn, J. Reynolds, H. Yang, Local reasoning about programs that alter data structures, in: 15th Int. Workshop on Computer Science Logic, CSL 2001, Paris, France, in: LNCS, vol. 2142, 2001, pp. 1–19.

[29] P. O'Hearn, H. Yang, Petri net semantics of bunched implications, Manuscript, 14 October 1999, at http://www0.cs.ucl.ac.uk/staff/p.ohearn/papers/petri.ps, 1999.

[30] P. O'Hearn, D. Pym, The logic of bunched implications, Bull. Symbolic Logic 5 (2) (1999) 215–244.

[31] A. Pnueli, The temporal logic of programs, in: Proceedings of the 18th Annual Symposium on Foundations of Computer Science, SFCS '77, IEEE Computer Society, Washington, DC, USA, 1977, pp. 46–57.

[32] D.J. Pym, C. Tofts, Systems modelling via resources and processes: philosophy, calculus, semantics, and logic, Electron. Notes Theor. Comput. Sci. 172 (2007) 545–587.

[33] D. Pym, P. O'Hearn, H. Yang, Possible worlds and resources: the semantics of BI, Theoret. Comput. Sci. 315 (1) (2004) 257–305, Erratum: p. 285, l.-12: ", for some P', $Q \equiv P; P'$" should be "$P \vdash Q$".

[34] G. Restall, An Introduction to Substructural Logics, Routledge, 1999.

[35] J. Reynolds, Separation logic: a logic for shared mutable data structures, in: IEEE Symposium on Logic in Computer Science, Copenhagen, Denmark, July 2002, pp. 55–74.

[36] A. Simpson, The proof theory and semantics of intuitionistic modal logic, PhD thesis, University of Edinburgh, 1994.

[37] C. Stirling, Modal and Temporal Properties of Processes, Springer Verlag, 2001.

[38] H. van Ditmarsch, W. van der Hoek, B. Kooi, Dynamic Epistemic Logic, Springer Publishing Company, 2007.