An Epistemic Separation Logic

J.R. Courtault and H. van Ditmarsch and D. Galmiche *

- Université de Lorraine, LORIA, UMR 7503, Vandoeuvre-lès-Nancy, F-54506, France
- CNRS, LORIA, UMR 7503, Vandoeuvre-lès-Nancy, F-54506, France

Abstract. We define an Epistemic Separation Logic, called ESL, that allows us to consider epistemic possible worlds as resources that can be shared or separated, in the spirit of separation logics. After studying the semantics and the expressiveness of this logic, we provide a tableau calculus with labels and resource contraints that is sound and complete and then also study countermodel extraction.

1 Introduction

The Epistemic Logic is the logic of *knowledge* and *belief*, which models and expresses properties on knowledge that have different agents [13,15,19]. The models of this logic are based on *possible worlds*, which encode all possible states/configurations of a considered system. For instance, in the case of a card game or in the muddy children problem [19], the possible worlds correspond to all card or all muddy forehead distributions. Moreover the possible worlds are very often distributions of elements (cards, muddy foreheads, lightbulb, ...) that can be considered as *resources*, which are entities that can be composed or decomposed into sub-entities. Then, two main questions arise: is it possible to enrich the Epistemic Logic models, by considering these possible worlds as such resources ? What kind of properties will we then be able to express ?
In order to model and express properties on resources, various resource logics have been proposed, such as Linear Logic (LL) [10] that focuses on resource consumption, and the logic of Bunched Implications (BI) and its variants, like Boolean BI (BBI) [18], that mainly focus on resource sharing and separation with two specific conjunctions $\wedge$ and $*$ and the corresponding implications. These logics are logical kernels of so-called separation logics with resources being memory areas [12,20], or resources being located on trees [4] and of logics modeling dynamic systems that manipulate resources [5,7].
Possible worlds being implicitly related to resources, it seems natural to extend the Epistemic Logic with separation connectives. In this paper we define such an extension, called Epistemic Separation Logic (ESL), that is a conservative extension of Epistemic Logic and also of BBI in which possible worlds are seen as resources. Let us note that we consider BBI logic in which the conjunction is distributive over the disjunction, property that does not hold in LL. Concerning the links between Epistemic Logic and resource management we can mention some works based on Linear Logic, in order to capture agent knowledge evolutions due to *epistemic actions* [3,16], but these

* Work partially supported by the ANR grant DynRes (project no. ANR-11-BS02-011) and by the EU ERC project EPS 313360. Hans van Ditmarsch is also affiliated to IMSc, Chennai, India, as research associate.

works consider the epistemic actions as resources (not the worlds). Compared with such works, our epistemic separation logic considers the possible (epistemic) worlds as resources, including sharing and separation connectives that allow us to express properties, like for instance $(A \wedge (B \vee C)) \mathrel{-\!\!*} K_a D$ that means that "the addition of a resource that satisfies the property A and also the property B or C, gives to the agent a the knowledge that D holds". Future work will be devoted to the study of other epistemic separation logics with epistemic actions [3], or updates [11].

2 An Epistemic Separation Logic

In this section we present first an Epistemic Separation Logic, called ESL, that can be seen as an extension of Boolean BI with a knowledge modality and then complete the logic with operators for knowledge change to the logic (public announcements).
We assume a finite set of agents A, and a countable set of propositional symbols Prop. The language $\mathcal{L}$ of the Epistemic Separation Logic, denoted ESL, is defined as follows:

$$\varphi ::= p \mid \bot \mid \mathrm{I} \mid \varphi \to \varphi \mid \varphi * \varphi \mid \varphi \mathrel{-\!\!*} \varphi \mid K_a \varphi$$

where a ranges over A and p over Prop. We can also define the other connectives : $\neg\varphi \equiv \varphi \to \bot$, $\top \equiv \neg\bot$, $\varphi \vee \psi \equiv \neg\varphi \to \psi$, $\varphi \wedge \psi \equiv \neg(\varphi \to \neg\psi)$ and $\widetilde{K}_a\varphi \equiv \neg K_a \neg\varphi$.
Here we consider possible worlds as resources and then we use indifferently the words *possible world* and *resource*. The *epistemic modality* $K_a\varphi$ means that the agent a knows that φ holds, and the *epistemic modality* $\widetilde{K}_a\varphi$, defined by $\widetilde{K}_a\varphi \equiv \neg K_a \neg\varphi$, means that the agent a considers that φ is possible. Finally the *multiplicative connectives* are the multiplicative conjunction $\varphi * \psi$, meaning that the possible world can be decomposed into two possible sub-worlds such that the first one satisfies φ and the second one satisfies ψ, and the multiplicative implication $\varphi \mathrel{-\!\!*} \psi$ meaning that by adding any possible world that satisfies φ we obtain a possible world that satisfies ψ. We also notice that I is the unit of $*$. A key point is the mixing of the epistemic modalities and the multiplicative connectives. For example, we can write the formula $\varphi \mathrel{-\!\!*} K_a\psi$ that expresses that any addition of a resource that satisfies φ allows the agent a to obtain the knowledge of ψ, which is an interesting property.

Definition 1 (Partial resource monoid). *A* partial resource monoid *(PRM) is a structure $\mathcal{R} = (R, \bullet, e)$ such that:*
– R is a set of resources *or* possible worlds *with $e \in R$;*
– $\bullet : R \times R \rightharpoonup R$ such that, for all $r_1, r_2, r_3 \in R$, $r_1 \bullet e \downarrow$ and $r_1 \bullet e = r_1$ (neutral element), if $r_1 \bullet r_2 \downarrow$ then $r_2 \bullet r_1 \downarrow$ and $r_1 \bullet r_2 = r_2 \bullet r_1$ (commutativity) and if $r_1 \bullet (r_2 \bullet r_3) \downarrow$ then $(r_1 \bullet r_2) \bullet r_3 \downarrow$ and $r_1 \bullet (r_2 \bullet r_3) = (r_1 \bullet r_2) \bullet r_3$ (associativity).

where $r_1 \bullet r_2 \downarrow$ means "$r_1 \bullet r_2$ is defined" and $r_1 \bullet r_2 \uparrow$ means "$r_1 \bullet r_2$ is undefined". We denote $\wp(E)$ the powerset of the set E, namely the set of sets built from E. We call e the *unit resource* and $\bullet$ the *resource composition*.

Definition 2 (Model). *A* model *is a triple $\mathcal{M} = (\mathcal{R}, \{\sim_a\}_{a \in A}, V)$ such that:*
– $\mathcal{R} = (R, \bullet, e)$ is a PRM;
– For all $a \in A$, $\sim_a \subseteq R \times R$ is an equivalence relation that is, for all $r_1, r_2, r_3 \in R$,

$r_1 \sim_a r_1$ *(reflexivity), if* $r_1 \sim_a r_2$ *then* $r_2 \sim_a r_1$ *(symmetry), if* $r_1 \sim_a r_2$ *and* $r_2 \sim_a r_3$ *then* $r_1 \sim_a r_3$ *(transitivity);.*
– $V : \mathsf{Prop} \to \wp(R)$ *is a* valuation.

If we compare these models to the Epistemic Logic models, we observe that the possible worlds are considered as resources, and they can be composed or decomposed by the function $\bullet$. Compared to the BBI models, the partial resource monoids are extended by equivalence relations on resources parametrized by agents.

Definition 3 (Forcing relation, validity). *Let* $\mathcal{M} = (\mathcal{R}, \{\sim_a\}_{a\in A}, V)$ *be a model. The forcing relation* $\vDash_{\mathcal{M}} \subseteq R \times \mathcal{L}$ *is defined by structural induction, for all* $r \in R$*, as follows:*

$r \vDash_{\mathcal{M}} p$	*iff*	$r \in V(p)$
$r \vDash_{\mathcal{M}} \top$	*always*	
$r \vDash_{\mathcal{M}} \bot$	*never*	
$r \vDash_{\mathcal{M}} \mathrm{I}$	*iff*	$r = e$
$r \vDash_{\mathcal{M}} \neg\varphi$	*iff*	$r \nvDash_{\mathcal{M}} \varphi$
$r \vDash_{\mathcal{M}} \varphi \wedge \psi$	*iff*	$r \vDash_{\mathcal{M}} \varphi$ *and* $r \vDash_{\mathcal{M}} \psi$
$r \vDash_{\mathcal{M}} \varphi \vee \psi$	*iff*	$r \vDash_{\mathcal{M}} \varphi$ *or* $r \vDash_{\mathcal{M}} \psi$
$r \vDash_{\mathcal{M}} \varphi \to \psi$	*iff*	$r \vDash_{\mathcal{M}} \varphi$ *implies* $r \vDash_{\mathcal{M}} \psi$
$r \vDash_{\mathcal{M}} \varphi * \psi$	*iff*	$\exists r_1, r_2 \in R \cdot r_1 \bullet r_2 \downarrow$ *and* $r = r_1 \bullet r_2$ *and* $r_1 \vDash_{\mathcal{M}} \varphi$ *and* $r_2 \vDash_{\mathcal{M}} \psi$
$r \vDash_{\mathcal{M}} \varphi \mathrel{-\!\!*} \psi$	*iff*	$\forall r' \in R \cdot (r \bullet r' \downarrow$ *and* $r' \vDash_{\mathcal{M}} \varphi) \Rightarrow r \bullet r' \vDash_{\mathcal{M}} \psi$
$r \vDash_{\mathcal{M}} K_a\varphi$	*iff*	$\forall r' \in R \cdot r \sim_a r' \Rightarrow r' \vDash_{\mathcal{M}} \varphi$
$r \vDash_{\mathcal{M}} \widetilde{K}_a\varphi$	*iff*	$\exists r' \in R \cdot r \sim_a r'$ *and* $r' \vDash_{\mathcal{M}} \varphi$

We say that a formula φ *is* valid*, denoted* $\vDash \varphi$*, if and only if* $r \vDash_{\mathcal{M}} \varphi$ *for all resources* r *of all models* $\mathcal{M}$*.*

Moreover we can show that Epistemic Separation Logic (ESL) is a conservative extension of Epistemic Logic and also a conservative extension of BBI.

Now we aim at extending the language definition of ESL with the connectives $[\varphi]\psi$ and $\langle\varphi\rangle\psi \equiv \neg[\varphi]\neg\psi$ that are dynamic epistemic modalities of Public Announcement Logic (PAL) [17,22], $[\varphi]\psi$ meaning that "after the truthful public announcement φ, ψ is true", and $\langle\varphi\rangle\psi$ meaning that "φ can be truthfully announced and ψ is true after it".
The peculiarity of PAL, and of other dynamic epistemic logics, is that this modality is standardly interpreted by a model transformation and not by an internal step in a given model, corresponding to an arrow in a given accessibility relation. The formula $[\varphi]\psi$ is true in a state of a given model, if and only if on condition that φ is true in that state, in the model restriction to the states where φ is true, the postcondition ψ is true in that state. In PAL terminology, where R is a set of words, $r \models_{\mathcal{M}} [\varphi]\psi$ iff if $r \models_{\mathcal{M}} \varphi$ then $r \models_{\mathcal{M}|\varphi} \psi$ where $\mathcal{M}|\varphi = (R', \{\sim'_a\}_{a\in A}, V')$ such that $R' = \{r \in R \mid r \models_{\mathcal{M}} \varphi\}$, for each $a \in A$, $\sim'_a = \sim_a \cap (R' \times R')$, and for each $p \in P$, $V'(p) = V(p) \cap R'$.
This standard semantics for public announcement logic is unsuitable in our setting, because it does not preserve monoids. For example, given a unit $e \in R$, a public announcement $\neg\mathrm{I}$ will restrict the resource set R of the monoid $\mathcal{R}$ to $R \setminus \{e\}$ that is no longer a monoid. Such restrictions on R cannot preserve the associativity of $\bullet$.

Two alternative semantics for public announcement logic are as follows. In a first approach [9] we do not restrict the domain to worlds where the announcement formula φ is true, but we restrict the accessibility relation (for all agents) to those pairs ending in worlds where φ is true. In a second approach [21] we do not restrict the domain but only refine the accessibility relation, i.e., we separate the submodel consisting of the φ worlds from the submodel consisting of the $\neg\varphi$ worlds. All semantics are equivalent in the sense that in a world satisfying the announcement, the same formulae in the logic are true (they are bisimilar), but the two alternatives have the advantage that the entire domain of the original model is preserved and therefore they preserve monoids. The refinement approach seems most suitable in our setting, as we focus on the incorporation of reliable information, i.e., truthful announcements.

Definition 4 (Extension of forcing relation). *Let $\mathcal{M} = (\mathcal{R}, \{\sim_a\}_{a\in A}, V)$ be a model. The forcing relation $\vDash_{\mathcal{M}} \subseteq R \times \mathcal{L}$ is extended, for public annoucements, as follows: $r \vDash_{\mathcal{M}} [\varphi]\psi$ iff if $r \vDash_{\mathcal{M}} \varphi$ then $r \vDash_{\mathcal{M}|\varphi} \psi$ and $r \vDash_{\mathcal{M}} \langle\varphi\rangle\psi$ iff $r \vDash_{\mathcal{M}} \varphi$ and $r \vDash_{\mathcal{M}|\varphi} \psi$ where $\mathcal{M}|\varphi = (\mathcal{R}', \{\sim'_a\}_{a\in A}, V')$, called the* update *of $\mathcal{M}$ by the public announcement φ, is defined by: $\mathcal{R}' = \mathcal{R}$, $\sim'_a = \sim_a \cap \{(r,s) \mid r \vDash_{\mathcal{M}} \varphi \text{ iff } s \vDash_{\mathcal{M}} \varphi\}$ and $V' = V$.*

The reader may note the difference with the more standard public announcement semantics given above. Moreover we observe that in the forcing relation there is no interaction between the epistemic aspects and resource aspects: the clauses for $*$ and $-\!\!*$ do not refer to the equivalence relation that encodes the epistemic modality, and the clauses for knowledge K_a and its dual do not refer to resource composition or decomposition that encode the resource modalities. We think that ESL is equally expressive as ESL with public announcements but this point will be fixed in future work.

3 Modelling with Epistemic Separation Logic

First we develop an example that emphasizes some key points about modelling with ESL. We consider two agents that enter in a library to borrow books. We suppose that they are not allowed to take out more than two books (only zero, one or two books) and they must tell the book references to the librarian who will fetch their. We also suppose that the books asked by the agents are always available and that each agent does not know which books and how many books are asked by the other. The librarian says to the agents: "Before telling me the book references I would like to say that I cannot carry more than two books. Could you tell me, at first, if I will be able to carry all the books that you want or if I need to use a book trolley ?".

As a first step, we build a model of this situation with ESL. We define the set of agents $A = \{A_1, A_2\}$, where A_i is the i^{th} agent and a PRM that deals with the possible worlds $\mathcal{R} = (R, \bullet, e)$. Then we define the set of resources $R = \{(i,j) \mid i,j \in \{0,1,2\}\}$, where (i,j) encodes "the agent A_1 wants i books and the agent A_2 wants j books", and we recall that an agent cannot borrow more than two books. Thereby, for instance, $(2,0)$ represents A_1 that wants two books and A_2 that wants no book.

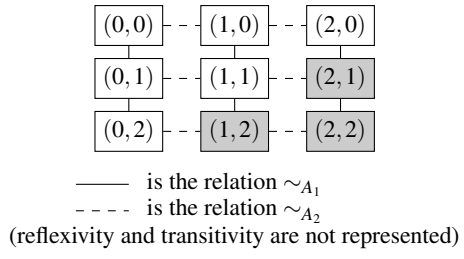


Fig. 1. Knowledge of the agents before the discussion. Grey means "cannot be carried".

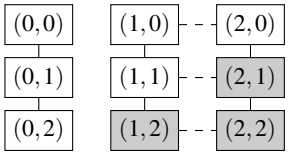


Fig. 2. Update of the model after the first public announcement: $K_{A_1}\neg \mathrm{I}$

The resource composition $\bullet$ is defined by:

$$(i_1, j_1) \bullet (i_2, j_2) = \begin{cases} \uparrow & \text{if } i_1 + i_2 > 2 \text{ or } j_1 + j_2 > 2 \\ (i_1 + i_2, j_1 + j_2) & \text{otherwise} \end{cases}$$

We remind that $\uparrow$ means "is not defined" and we note that $(0,0)$ is the unit of resource composition and then $e = (0,0)$.

Let us now illustrate the resource composition. We assume that A_1 wants to borrow one book and the other agent wants no book, then we represent the global borrow request by the resource, or possible world, $(1,0)$. Now, if A_2 wants two more books, then we have the final borrow request $(1,0) \bullet (0,2) = (1,2)$. Moreover, if A_2 wants one more book then it is not allowed: we have $(1,2) \bullet (0,1) \uparrow$, that expresses that A_2 cannot borrow more than two books.

Now, we have to build a model $\mathcal{M} = (\mathcal{R}, \{\sim_a\}_{a \in A}, V)$ and then we define two equivalence relations, that are $\sim_{A_1}$ and $\sim_{A_2}$. For instance, we expect $(1,0) \sim_{A_2} (2,0)$ because if A_2 wants no book then, as A_2 has no information about how many books are wanted by A_1 and as he has only information about how many books he wants, then he must consider, from his point of view, that A_1 might want one book or A_1 might want two books. In the other hand, we also expect to have, for instance, $(1,0) \not\sim_{A_2} (1,1)$, because it is not consistent, from the point of view of A_2, that he wants no book and one book.

Therefore, we give the following definitions, for all $i_1, i_2, j_1, j_2 \in \{0,1,2\}$:

$$\begin{array}{ll} (i_1, j_1) \sim_{A_1} (i_2, j_2) & \text{iff} \quad i_1 = i_2 \\ (i_1, j_1) \sim_{A_2} (i_2, j_2) & \text{iff} \quad j_1 = j_2 \end{array}$$

Finally, we consider the set of propositional symbols $\mathsf{Prop} = \{P_1, P_2, C\}$ and the valuation V, such that $V(P_1) = \{(1,0)\}$, $V(P_2) = \{(0,1)\}$ and $V(C) = \{(i,j) \mid i + j \leqslant 2\}$. Thus we have $r \in V(P_i)$ if and only if r is the borrow such that the agent A_i wants one and only one book and the other agent wants no book and $r \in V(C)$ means that the librarian can carry the books of r (the agents want at maximum two books).

A graphical representation of our model is given in Fig. 1, where grey vertices correspond to requests which do not satisfy C.

After the construction of the model of Fig. 1, we illustrate the use of ESL connectives in our model. Concerning propositional symbols, we have for instance $(0,1) \vDash_{\mathcal{M}} P_2$,

because $(0,1) \in V(P_2)$, which expresses that only one book is wanted and this book is wanted by A_2. But, we have $(0,2) \not\models_{\mathcal{M}} P_2$ and $(1,1) \not\models_{\mathcal{M}} P_2$. Concerning the propositional symbol C, we have for instance $(1,1) \models_{\mathcal{M}} C$ which expresses that the librarian can carry the two books asked by the agents, but $(1,2) \not\models_{\mathcal{M}} C$ that means that the librarian cannot carry the books (because the agents want more than two books).
Being a conservative extension of the Epistemic Logic, ESL can express properties on the agent knowledge. For instance, we have $(0,1) \models_{\mathcal{M}} K_{A_1} C$, because for all $r \in R$ such that $(0,1) \sim_{A_1} r$, we have $r \models_{\mathcal{M}} C$. It means that if we consider that A_1 wants no book and A_2 wants one book, then the agent A_1 knows that the librarian can carry the books. Concerning the modality $\widetilde{K}_a$ we have $(1,2) \models_{\mathcal{M}} \widetilde{K}_{A_1} C$, because $(1,2) \sim_{A_1} (1,1)$ and $(1,1) \models_{\mathcal{M}} C$. It means that if A_1 wants one book and A_2 wants two books then A_1 considers that it is possible that the librarian can carry the books.
Being also a conservative extension of BBI, ESL can express sharing and separation properties. Concerning the formula I, we have $r \models_{\mathcal{M}} \mathrm{I}$ iff $r = e = (0,0)$. In other words the formula I expresses that the agents want no book. About sharing and separation expressed in ESL, as $(0,0) \models_{\mathcal{M}} K_{A_1} C$ and $(0,0) \models_{\mathcal{M}} K_{A_2} C$ then we have $(0,0) \models_{\mathcal{M}} K_{A_1} C \wedge K_{A_2} C$. The conjunction $\wedge$ expresses sharing such that $K_{A_1} C$ and $K_{A_2} C$ share the resource $(0,0)$. The other conjunction $*$ expresses separation. As $(2,0) = (1,0) \bullet (1,0)$ and $(1,0) \models_{\mathcal{M}} P_1$ and $(1,0) \models_{\mathcal{M}} P_1$ then $(2,0) \models_{\mathcal{M}} P_1 * P_1$. This is a separation property because $(2,0)$ is separated (or decomposed) into two sub-resources. We remark that $P_1 * P_1$ means that A_1 wants two books (and the other agent wants no book) and the connective $*$ allows us to count resources. For instance, $P_1 * P_2 * P_2$ means that A_1 wants one book and A_2 wants two books.
The multiplicative implication $-\!\!*$ allows us to express a property on the resource obtained after the addition of another resource. For instance $(1,1) \models_{\mathcal{M}} P_1 -\!\!* \neg C$, because if we add a resource that satisfies P_1 to the resource $(1,1)$ then we obtain a resource that satisfies $\neg C$. Indeed we only have $(1,0) \models_{\mathcal{M}} P_1$ and then $(1,1) \bullet (1,0) = (2,1)$ and $(2,1) \models_{\mathcal{M}} \neg C$. Therefore, $(1,1) \models_{\mathcal{M}} P_1 -\!\!* \neg C$, that means that if A_1 and A_2 want one book then if A_1 wants one more book then the librarian cannot carry the books.

After the librarian asks to the agents if he will be able to carry the wanted books, we suppose that the agents have the following discussion:
1. A_1: "I know that I do not want no book."
2. A_2: "I know that I want at least one book, and A_1 wants also at least one book."
3. A_1: "I know that I am allowed to borrow one more book."
4. A_2: "I know that you can carry our books. Moreover, I also know that we want one book each other."

The previous sentences numbered by i are public announcements, which will be denoted Υ_i. We now show the evolution of the model of Fig. 1 after each announcement.
Firstly, A_1 says (announces) that he knows that the agents do not want no book, which is expressed by the formula $\Upsilon_1 = K_{A_1} \neg \mathrm{I}$. We observe that we have, $(i,j) \models_{\mathcal{M}} K_{A_1} \neg \mathrm{I}$ if and only if $(i,j) \not\sim_{A_1} (0,0)$. Then the update of our model by the public announcement $K_{A_1} \neg \mathrm{I}$ is the model $\mathcal{M} | K_{A_1} \neg \mathrm{I}$ which is given in Fig. 2.
Starting from the model $\mathcal{M} | K_{A_1} \neg \mathrm{I}$ which is given in Fig. 2 and assuming that the agents

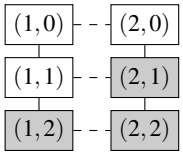


Fig. 3.

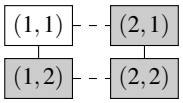


Fig. 4.

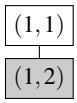


Fig. 5.

Fig. 6.

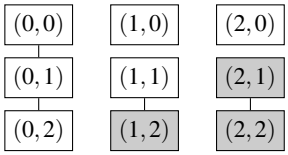


Fig. 7. The model updated after all public announcements ($\mathcal{M}|\Upsilon_1|\Upsilon_2|\Upsilon_3$)

never lie, the worlds $(0, j)$, where $j \in \{0,1,2\}$, cannot be the solution of our problem because these words do not force the public announcement. We call "solution of our problem" any world that allows the agents to do the announcements without lying. Thus, the solution is one of the possible worlds of Fig. 3.

Then, A_2 announces that he knows that A_1 wants at less one book, and also himself wants at less one book. Such property is expressed by the formula $\Upsilon_2 = K_{A_2}((P_1 * \top) \wedge (P_2 * \top))$. We have $(i, j) \vDash_{\mathcal{M}|\Upsilon_1} K_{A_2}((P_1 * \top) \wedge (P_2 * \top))$ iff $i \geq 1$ and $j \geq 1$. Then, focusing on the possible worlds satisfying the formula, the solution is one of the resources of Fig. 4. A_1 announces that he knows that he is allowed to borrow one more book, which is captured by the formula $\Upsilon_3 = K_{A_1} \neg (P_1 \multimap \bot)$. Indeed, we have $(i, j) \vDash_{\mathcal{M}|\Upsilon_1|\Upsilon_2} P_1 \multimap \bot$ if and only if for all $r \in R$ such that $(i, j) \bullet r \downarrow$ and $r \vDash_{\mathcal{M}|\Upsilon_1|\Upsilon_2} P_1$, we have $(i, j) \bullet r \vDash_{\mathcal{M}|\Upsilon_1|\Upsilon_2} \bot$. As r can only be $(1,0)$ (because $r \vDash_{\mathcal{M}|\Upsilon_1|\Upsilon_2} P_1$) and no resource satisfies $\bot$, we necessarily have $(i, j) \bullet (1,0) \uparrow$, that means that A_1 cannot borrow one more book. Then the negation ($\neg$) of the formula $(P_1 \multimap \bot)$ means A_1 can borrow one more book. Finally, ignoring all possible worlds that do not satisfy the formula $K_{A_1} \neg (P_1 \multimap \bot)$, we obtain the worlds of the Fig. 5.

Finally, A_2 says that he knows that the librarian can carry the books. The only possible world which satisfies the formula $K_{A_2} C$ is $(1,1)$, which is the solution of our problem: A_1 wants one book and A_2 wants also one book. Moreover, A_2 knows it, that is expressed by $K_{A_2}(C \wedge (P_1 * P_2))$. Considering this last sentence as a public announcement ($\Upsilon_4 = K_{A_2}(C \wedge (P_1 * P_2))$), and ignoring the worlds that do not satisfy it, we obtain the world of Fig. 6. The model updated by the public announcements with all worlds represented ($\mathcal{M}|\Upsilon_1|\Upsilon_2|\Upsilon_3$) is given in Fig. 7. We also can write $(1,1) \vDash_{\mathcal{M}} \langle \Upsilon_1 \rangle \langle \Upsilon_2 \rangle \langle \Upsilon_3 \rangle K_{A_2}(C \wedge (P_1 * P_2))$, that expresses that after all announcements, A_2 knows that the librarian can carry the books and also knows the quantity of books wanted being each agent. We remark that $(1,1)$ is the only world satisfying the formula and the public announcements are expressed using $\langle \Upsilon_i \rangle$ rather than $[\Upsilon_i]$ because we assume that the agents are in a true and fair view.

Let us now reason once more about the entire model and not about the situation $(1,1)$. We show how to combine epistemic and separating connectives and then to provide new modalities. For instance we have

– $K_a(\varphi * \psi)$, that means that the agent a knows that the resource (the possible world) can be decomposed into two sub-resources that respectively satisfy φ and ψ. Back to the example, $K_{A_1}(P_1 * P_1 * P_2)$ expresses that A_1 knows that he wants two books and A_2 wants one book.

– $K_a(\varphi \mathrel{-\!\!*} \psi)$, that means that the agent a knows that by the addition of a resource satisfying φ one obtains a resource satisfying ψ. Back to the example, $K_{A_1}((P_1 \vee P_2) \mathrel{-\!\!*} \neg C)$ expresses that A_1 knows that if an agent orders one more book then the librarian cannot carry the books.

– $\varphi * K_a\psi$, that means that without a resource satisfying φ, the agent a could have the knowledge that ψ holds. Back to the example, $P_2 * K_{A_2}C$ expresses that wanting one book less, the agent A_2 gets the knowledge that the librarian can carry the books.

– $\varphi \mathrel{-\!\!*} K_a\psi$, that means that the addition of a resource satisfying φ allows the agent a to obtain the knowledge that ψ holds. Back to the example, $P_1 \mathrel{-\!\!*} K_{A_1}\neg C$ expresses that choosing to borrow one more book gives to A_1 the knowledge that the librarian cannot carry the books.

We remark that the two last expressions allow us to express a property that involves a kind of change of mind, namely "if the agent wants one book less" and "if the agent chooses to borrow one more book". The use of such formulae that can be seen as new epistemic modalities will be studied in futur work.

4 A Tableaux Calculus for Epistemic Separation Logic

In this section, we present a tableaux calculus for ESL, in the spirit of the tableaux calculus for BI and BBI [8,14], with extraction of countermodels in case of non validity of a formula. Its extension to deal with public annoucements will be studied in next works and compared to related works [1].

We first introduce labels and constraints that respectively correspond to resources and the equality and the equivalence relations on resources and agents.

Definition 5 (Resource labels). *L_r is a set of* resource labels *built from a constant* 1*, an infinite countable set of constants $\gamma_r = \{c_1, c_2, \ldots\}$ and a function denoted $\circ$:*

$$X ::= 1 \mid c_i \mid X \circ X, \text{ where } c_i \in \gamma_r.$$

Moreover $\circ$ is a function on L_r that is associative, commutative and 1 is its unit.

We denote xy the resource label $x \circ y$. A resource label can be viewed as a word where the letter order is not taken into account. We say that x is a *resource sublabel* of y if and only if there exists z such that $x \circ z = y$. The set of resource sublabels of x is denoted $\mathcal{E}(x)$.

Definition 6 (Constraints). *A* resource constraint *is an expression of the form $x \simeq y$ where x and y are resource labels. A* agent constraint *is an expression of the form $x =_u y$ where x and y are resource labels and u belongs to the set of agents A.*

Rules for resource constraints

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

$$\frac{x \simeq y \qquad yk \simeq yk}{xk \simeq yk}\ \langle c_r\rangle \qquad \frac{x =_u y}{x \simeq x}\ \langle k_r\rangle$$

Rules for agent constraints

$$\frac{x \simeq x}{x =_u x}\ \langle r_a\rangle \qquad \frac{x =_u y}{y =_u x}\ \langle s_a\rangle \qquad \frac{x =_u y \qquad y =_u z}{x =_u z}\ \langle t_a\rangle \qquad \frac{x =_u y \qquad x \simeq k}{k =_u y}\ \langle k_a\rangle$$

Fig. 8. Rules for constraint closure, for all $u \in A$

We call *set of constraints* any set $\mathcal{C}$ that contains resource constraints and agent constraints. For instance, $\mathcal{C} = \{c_1 \simeq c_2, c_2 \simeq c_3, c_4 =_b c_1\}$ is a set of constraints.

Definition 7 (Domain). *Let $\mathcal{C}$ be a constraint set. The (resource)* domain *of $\mathcal{C}$ is the set of all resource sublabels that appear in $\mathcal{C}$, that is:*

$$\mathcal{D}_r(\mathcal{C}) = \bigcup_{x \simeq y \in \mathcal{C}} (\mathcal{E}(x) \cup \mathcal{E}(y)) \cup \bigcup_{x =_u y \in \mathcal{C}} (\mathcal{E}(x) \cup \mathcal{E}(y))$$

Definition 8 (Alphabet). *Let $\mathcal{C}$ be a constraint set. The (resource)* alphabet *of $\mathcal{C}$ is the set of resource constants that appear in $\mathcal{C}$. In particular, $\mathcal{A}_r(\mathcal{C}) = \gamma_r \cap \mathcal{D}_r(\mathcal{C})$.*

We remark that 1 is not a label constant ($1 \notin \gamma_r$) and then $1 \notin \mathcal{A}_r(\mathcal{C})$. But $1 \in \mathcal{D}_r(\mathcal{C})$, for any set of constraints $\mathcal{C} \neq \emptyset$, because $1 \in \mathcal{E}(x)$ holds for all resource labels x.
Now we introduce rules for constraint closure that allow us to capture the properties of the models into the calculus.

Definition 9 (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. 8 such that $\mathcal{C} \subseteq \overline{\mathcal{C}}$.*

There are six rules ($\langle 1\rangle$, $\langle s_r\rangle$, $\langle d_r\rangle$, $\langle t_r\rangle$, $\langle c_r\rangle$ and $\langle k_r\rangle$) that produce resource constraints and four rules ($\langle r_a\rangle$, $\langle s_a\rangle$, $\langle t_a\rangle$ and $\langle k_a\rangle$) that produce agent constraints. We note that u, introduced in the rule $\langle r_a\rangle$, must belong to the set of agents A (else $x =_u x$ would not be an agent constraint). For instance, if $\mathcal{C} = \{c_1 \simeq c_2, c_2 \simeq c_3, c_1 =_b c_4\}$, we have $c_3 =_b c_4 \in \overline{\mathcal{C}}$ because of the following proof:

$$\frac{c_1 =_b c_4 \qquad \dfrac{c_1 \simeq c_2 \qquad c_2 \simeq c_3}{c_1 \simeq c_3}\ \langle t_r\rangle}{c_3 =_b c_4}\ \langle k_a\rangle$$

Proposition 1. *The following rules can be derived from the rules of constraint closure:*

$$\frac{xk \simeq y}{x \simeq x}\ \langle p_l\rangle \qquad \frac{x \simeq yk}{y \simeq y}\ \langle p_r\rangle \qquad \frac{xk =_u y}{x \simeq x}\ \langle q_l\rangle \qquad \frac{x =_u yk}{y =_u y}\ \langle q_r\rangle$$

$$\frac{x \eqsim_u y \qquad x \simeq x' \qquad y \simeq y'}{x' \eqsim_u y'} \langle w_a \rangle$$

Corollary 1. *Let $\mathcal{C}$ be a set of constraints and u an agent of A. We have $x \in \mathcal{D}_r(\overline{\mathcal{C}})$ if and only if $x \simeq x \in \overline{\mathcal{C}}$ iff $x \eqsim_u x \in \overline{\mathcal{C}}$.*

Proposition 2. *Let $\mathcal{C}$ a set of constraints. We have $\mathcal{A}_r(\mathcal{C}) = \mathcal{A}_r(\overline{\mathcal{C}})$.*

Now, we can define a labelled tableaux calculus for ESL in the spirit of previous works for BI [8] and BBI [14].

Definition 10. *A* labelled formula *is a 3-uplet $(S, \varphi, x) \in \{\mathbb{T}, \mathbb{F}\} \times \mathcal{L} \times L_r$ written $\mathbb{S}\varphi : x$. A* constrained set of statements *(CSS) is a pair $\langle \mathcal{F}, \mathcal{C} \rangle$, where $\mathcal{F}$ is a set of labelled formulae and $\mathcal{C}$ is a set of constraints, satisfying the property:*

$$\text{if } \mathbb{S}\varphi : x \in \mathcal{F} \text{ then } x \simeq x \in \overline{\mathcal{C}} \quad (P_{css})$$

A CSS $\langle \mathcal{F}, \mathcal{C} \rangle$ is finite *if $\mathcal{F}$ and $\mathcal{C}$ are finite.*
The relation $\preccurlyeq$ is defined by $\langle \mathcal{F}, \mathcal{C} \rangle \preccurlyeq \langle \mathcal{F}', \mathcal{C}' \rangle$ iff $\mathcal{F} \subseteq \mathcal{F}'$ and $\mathcal{C} \subseteq \mathcal{C}'$. We denote $\langle \mathcal{F}_f, \mathcal{C}_f \rangle \preccurlyeq_f \langle \mathcal{F}, \mathcal{C} \rangle$ 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.

Fig. 9 presents the rules of tableaux calculus for ESL. Let us note that "c_i and c_j are new label constants" means $c_i \neq c_j \in \gamma_r \setminus \mathcal{A}_r(\mathcal{C})$. In this tableaux calculus we encode tableaux as lists of CSS and denote $\oplus$ the concatenation of lists. Then we have $[e_3; e_1] \oplus [e_1; e_2; e_5] = [e_3; e_1; e_1; e_2; e_5]$.

Definition 11 (Tableau). *Let $\langle \mathcal{F}_0, \mathcal{C}_0 \rangle$ be a finite CSS. A* tableau *for $\langle \mathcal{F}_0, \mathcal{C}_0 \rangle$ is a list of CSS, called* branches*, inductively built according the following rules:*

1. *The one branch 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*

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

is an instance of a rule of Fig. 9 for which $cond\langle \mathcal{F}, \mathcal{C} \rangle$ 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 $\langle \{\mathbb{F}\varphi : c_1\}, \{c_1 \simeq c_1\} \rangle$.*

From the rules of Fig. 9, we remark that a new CSS obtained after an application of a rule verifies the property (P_{css}) of Definition 10 (in particular by Corollary 1).
In this tableaux calculus, we have two particular set of rules. The first set is composed by the rules $\langle \mathbb{T}\mathrm{I} \rangle$, $\langle \mathbb{T}* \rangle$, $\langle \mathbb{F}{-\!\!*} \rangle$, $\langle \mathbb{F}K \rangle$ and $\langle \mathbb{T}\widetilde{K} \rangle$. They introduce new label constants (c_i and c_j) and new constraints, except for $\langle \mathbb{T}\mathrm{I} \rangle$ that only introduces a new constraint. For instance when we apply the rule $\langle \mathbb{F}K \rangle$ on the labelled formula $\mathbb{F}K_a\varphi : c_3$ that belongs to a CSS $\langle \mathcal{F}, \mathcal{C} \rangle$, we have to choose a new resource label which does not appear in

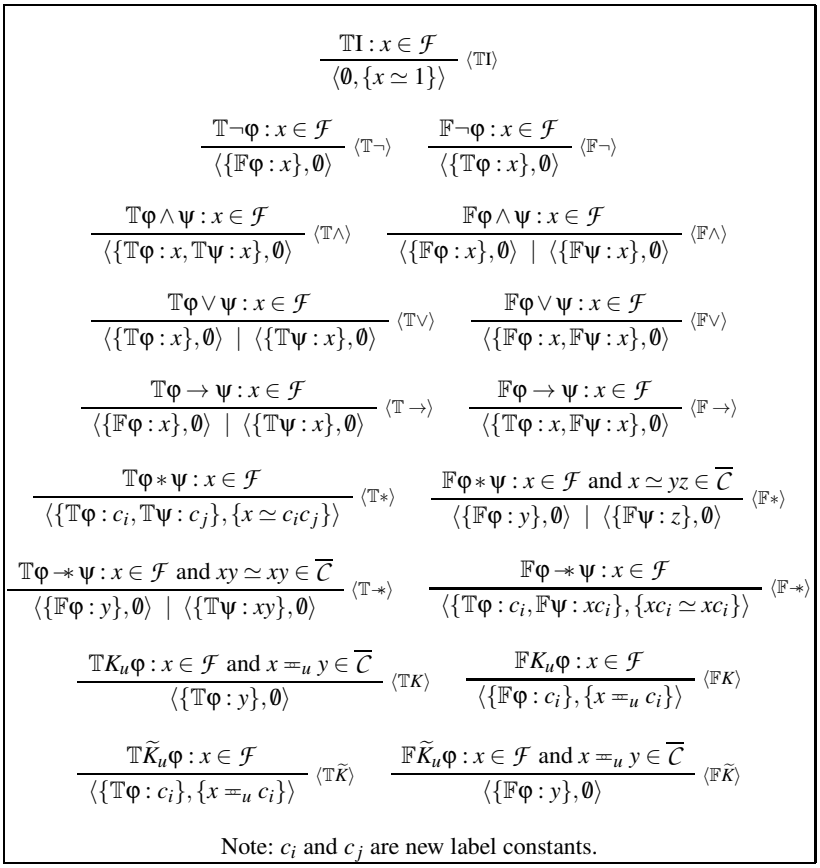


Fig. 9. Rules of tableaux calculus for ESL

$\mathcal{C}$. If we assume that $c_5 \in \gamma_r \setminus \mathcal{A}_r(\mathcal{C})$ then we can apply the rule, getting the new CSS $\langle \mathcal{F} \cup \{\mathbb{F}\varphi : c_5\}, \mathcal{C} \cup \{c_3 =\!\!=_a c_5\} \rangle$. We remark the new agent constraint $c_3 =\!\!=_a c_5$ added to the set of constraints. The second set is composed by the rules $\langle \mathbb{F}* \rangle$, $\langle \mathbb{T}-\!\!* \rangle$, $\langle \mathbb{T}K \rangle$, $\langle \mathbb{F}\widetilde{K} \rangle$. They have a condition on the closure of constraints. In order to apply one of these rules we have to choose a label which satisfies the condition and then apply the rule using it. Otherwise, we cannot apply the rule. For instance if $\langle \mathcal{F}, \mathcal{C} \rangle$ is a CSS such that $\mathbb{T}K_b\varphi : c_2 \in \mathcal{F}$ then the application of the rule $\langle \mathbb{T}K \rangle$ depends of the choice of a resource label x such that $c_2 =\!\!=_b x \in \overline{\mathcal{C}}$. If we assume that $c_2 =\!\!=_b c_3 \in \overline{\mathcal{C}}$ then we can apply the rule getting the CSS $\langle \mathcal{F} \cup \{\mathbb{T}\varphi : c_3\}, \mathcal{C} \rangle$.

Definition 12 (Closure condition). *A CSS $\langle \mathcal{F}, \mathcal{C} \rangle$ is* closed *if one of the following conditions holds: 1. $\mathbb{T}\varphi : x \in \mathcal{F}$, $\mathbb{F}\varphi : y \in \mathcal{F}$ and $x \simeq y \in \overline{\mathcal{C}}$, 2. $\mathbb{F}\mathbf{I} : x \in \mathcal{F}$ and $x \simeq 1 \in \overline{\mathcal{C}}$, 3. $\mathbb{F}\top : x \in \mathcal{F}$ and 4. $\mathbb{T}\bot : x \in \mathcal{F}$. A CSS is* open *if it is not closed.*
A tableau for φ is closed *if all its branches are closed and a* tableau proof *for φ is a closed tableau for φ.*

Theorem 1 (Soundness). *Let* φ *be a ESL formula. If there exists a tableau proof for* φ *then* φ *is valid.*

Proof. The proof is based on similar techniques than the ones used for the soundness proof of BI tableaux method [8]. The key point consists in considering the notion of *realizability* of a CSS $\langle \mathcal{F}, \mathcal{C} \rangle$, meaning that there exist a model $\mathcal{M}$ and an embedding $(|.|)$ from the resource labels to the resource set of $\mathcal{M}$ such that if $\mathbb{T}\varphi : x \in \mathcal{F}$ then $|x| \vDash_{\mathcal{M}} \varphi$ and if $\mathbb{F}\varphi : x \in \mathcal{F}$ then $|x| \nvDash_{\mathcal{M}} \varphi$.

Let us consider the formula $\varphi \equiv K_a((P \mathrel{-\!\!*} Q) * K_b(P \wedge R)) \rightarrow K_a \widetilde{K}_b Q$. We first initialize a tableau for φ with $[\langle \{\mathbb{F}\varphi : c_1\}, \{c_1 \simeq c_1\} \rangle]$. and introduce the following representation:

$$\begin{array}{cc} [\mathcal{F}] & [\mathcal{C}] \\ \mathbb{F}K_a((P \mathrel{-\!\!*} Q) * K_b(P \wedge R)) \rightarrow K_a \widetilde{K}_b Q : c_1 & c_1 \simeq c_1 \end{array}$$

The column on left-hand side represents the labelled formula sets of the CSS of the tableau ($[\mathcal{F}]$) and the column on right-hand side represents the constraint sets of the CSS of ($[\mathcal{C}]$). By applying rules on this tableau, we obtain the tableau for φ that is given in Fig. 10. We decorate a labelled formula with $\surd_i$ to show that we apply a rule on this formula at step i. Let us give more details about rule applications at steps 2 and 6.
The step 2 consists in applying the rule $\langle \mathbb{F}K_a \rangle$ on the labelled formula $\mathbb{F}K_a \widetilde{K}_b Q : c_1$. Then in order to apply this rule we have to choose a new resource constant (c_2). Then we can apply the rule introducing, in the branch, the labelled formula $\mathbb{F}\widetilde{K}_b Q : c_2$ and the agent constraint $c_1 =\!\!\!=_a c_2$. The step 6 consists in applying the rule $\langle \mathbb{T}K_b \rangle$ on the labelled formula $\mathbb{T}K_b(P \wedge R) : c_4$. Then we have to choose y such that $c_4 =\!\!\!=_b y \in \overline{\mathcal{C}}$. We have $c_4 =\!\!\!=_b c_4 \in \overline{\mathcal{C}}$, indeed

$$\dfrac{\dfrac{\dfrac{\dfrac{c_2 \simeq c_3c_4}{c_3c_4 \simeq c_2}\langle s_r \rangle \qquad c_2 \simeq c_3c_4}{c_3c_4 \simeq c_3c_4}\langle t_r \rangle}{c_4 \simeq c_4}\langle d_r \rangle}{c_4 =\!\!\!=_b c_4}\langle r_a \rangle$$

Therefore we can choose $y = c_4$ and apply the rule, adding to the branch the labelled formula $\mathbb{T}P \wedge R : c_4$. Finally, we observe that the tableau branches are closed (denoted $\times$). In particular, the branch on the right-hand side is closed because $\mathbb{T}Q : c_3c_4$, $\mathbb{F}Q : c_2$ and $c_3c_4 \simeq c_2 \in \overline{\mathcal{C}}$. In conclusion, we have a closed tableau proof for the formula $K_a((P \mathrel{-\!\!*} Q) * K_b(P \wedge R)) \rightarrow K_a \widetilde{K}_b Q$ and then by Theorem 1 this formula is valid.

Moreover we propose a countermodel extraction method, adapted from [14], that consists in transforming the sets of resource and agent constraint of a branch $\langle \mathcal{F}, \mathcal{C} \rangle$ into a model $\mathcal{M}$ such that if $\mathbb{T}\varphi : x \in \mathcal{F}$ then $[x] \vDash_{\mathcal{M}} \varphi$ and if $\mathbb{F}\varphi : x \in \mathcal{F}$ then $[x] \nvDash_{\mathcal{M}} \varphi$, where $[x]$ is the equivalence class of x,
First we have to define when a CSS $\langle \mathcal{F}, \mathcal{C} \rangle$ is a *Hintikka CSS*.

Definition 13 (Hintikka CSS). *A CSS* $\langle \mathcal{F}, \mathcal{C} \rangle$ *is a* Hintikka CSS *iff for any formula* $\varphi, \psi \in \mathcal{L}$ *and any resource label* $x, y \in L_r$ *and any agent* $u \in A$*:*

1. $\mathbb{T}\varphi : x \notin \mathcal{F}$ *or* $\mathbb{F}\varphi : y \notin \mathcal{F}$ *or* $x \simeq y \notin \overline{\mathcal{C}}$

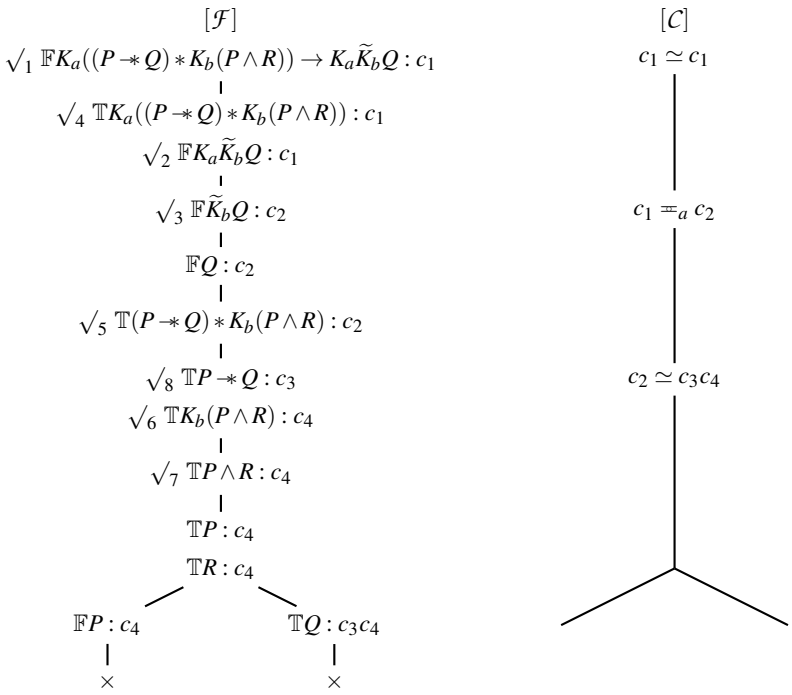


Fig. 10. Tableau for $K_a((P \multimap\!\!* Q) * K_b(P \wedge R)) \to K_a\widetilde{K}_bQ$

2. $\mathbb{F}\mathbf{I} : x \notin \mathcal{F}$ *or* $x \simeq 1 \notin \overline{\mathcal{C}}$
3. $\mathbb{F}\top : x \notin \mathcal{F}$
4. $\mathbb{T}\bot : x \notin \mathcal{F}$
5. *If* $\mathbb{T}\mathbf{I} : x \in \mathcal{F}$ *then* $x \simeq 1 \in \overline{\mathcal{C}}$
6. *If* $\mathbb{T}\neg\varphi : x \in \mathcal{F}$ *then* $\mathbb{F}\varphi : x \in \mathcal{F}$
7. *If* $\mathbb{F}\neg\varphi : x \in \mathcal{F}$ *then* $\mathbb{T}\varphi : x \in \mathcal{F}$
8. *If* $\mathbb{T}\varphi \wedge \psi : x \in \mathcal{F}$ *then* $\mathbb{T}\varphi : x \in \mathcal{F}$ *and* $\mathbb{T}\psi : x \in \mathcal{F}$
9. *If* $\mathbb{F}\varphi \wedge \psi : x \in \mathcal{F}$ *then* $\mathbb{F}\varphi : x \in \mathcal{F}$ *or* $\mathbb{F}\psi : x \in \mathcal{F}$
10. *If* $\mathbb{T}\varphi \vee \psi : x \in \mathcal{F}$ *then* $\mathbb{T}\varphi : x \in \mathcal{F}$ *or* $\mathbb{T}\psi : x \in \mathcal{F}$
11. *If* $\mathbb{F}\varphi \vee \psi : x \in \mathcal{F}$ *then* $\mathbb{F}\varphi : x \in \mathcal{F}$ *and* $\mathbb{F}\psi : x \in \mathcal{F}$
12. *If* $\mathbb{T}\varphi \to \psi : x \in \mathcal{F}$ *then* $\mathbb{F}\varphi : x \in \mathcal{F}$ *or* $\mathbb{T}\psi : x \in \mathcal{F}$
13. *If* $\mathbb{F}\varphi \to \psi : x \in \mathcal{F}$ *then* $\mathbb{T}\varphi : x \in \mathcal{F}$ *and* $\mathbb{F}\psi : x \in \mathcal{F}$
14. *If* $\mathbb{T}\varphi * \psi : x \in \mathcal{F}$ *then* $\exists y,z \in L_r$, $x \simeq yz \in \overline{\mathcal{C}}$ *and* $\mathbb{T}\varphi : y \in \mathcal{F}$ *and* $\mathbb{T}\psi : z \in \mathcal{F}$
15. *If* $\mathbb{F}\varphi * \psi : x \in \mathcal{F}$ *then* $\forall y,z \in L_r$, $x \simeq yz \in \overline{\mathcal{C}} \Rightarrow \mathbb{F}\varphi : y \in \mathcal{F}$ *or* $\mathbb{F}\psi : z \in \mathcal{F}$
16. *If* $\mathbb{T}\varphi \multimap\!\!* \psi : x \in \mathcal{F}$ *then* $\forall y \in L_r$, $xy \in \mathcal{D}_r(\overline{\mathcal{C}}) \Rightarrow \mathbb{F}\varphi : y \in \mathcal{F}$ *or* $\mathbb{T}\psi : xy \in \mathcal{F}$
17. *If* $\mathbb{F}\varphi \multimap\!\!* \psi : x \in \mathcal{F}$ *then* $\exists y \in L_r$, $xy \in \mathcal{D}_r(\overline{\mathcal{C}})$ *and* $\mathbb{T}\varphi : y \in \mathcal{F}$ *and* $\mathbb{F}\psi : xy \in \mathcal{F}$
18. *If* $\mathbb{T}K_u\varphi : x \in \mathcal{F}$ *then* $\forall y \in L_r$, $x =_u y \in \overline{\mathcal{C}} \Rightarrow \mathbb{T}\varphi : y \in \mathcal{F}$
19. *If* $\mathbb{F}K_u\varphi : x \in \mathcal{F}$ *then* $\exists y \in L_r$, $x =_u y \in \overline{\mathcal{C}}$ *and* $\mathbb{F}\varphi : y \in \mathcal{F}$
20. *If* $\mathbb{T}\widetilde{K}_u\varphi : x \in \mathcal{F}$ *then* $\exists y \in L_r$, $x =_u y \in \overline{\mathcal{C}}$ *and* $\mathbb{T}\varphi : y \in \mathcal{F}$

21. If $\mathbb{F}\widetilde{K}_u\varphi : x \in \mathcal{F}$ *then* $\forall y \in L_r$, $x =_u y \in \overline{C} \Rightarrow \mathbb{F}\varphi : y \in \mathcal{F}$

In this definition, the four first conditions certify that a Hintikka CSS is not closed and the other that all labelled formulae of a Hintikka CSS are fulfilled [14].
In order to extract a countermodel from a Hintikka CSS, we manipulate equivalence classes. The equivalence class of $x \in \mathcal{D}_r(\overline{C})$, denoted $[x]$, is the set $[x] = \{y \in L_r \mid x \simeq y \in \overline{C}\}$. We also denote $\mathcal{D}_r(\overline{C})/\simeq = \{[x] \mid x \in \mathcal{D}_r(\overline{C})\}$ the set of all equivalence classes of $\mathcal{D}_r(\overline{C})$. We observe that $\simeq$ is an equivalence relation, because it is is reflexive (by Corollary 1), symmetric (by rule $\langle s_r \rangle$) and transitive (by rule $\langle t_r \rangle$). Then we define a function Ω that allows us to extract a countermodel from a Hintikka CSS.

Definition 14 (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 3-uplet* $\Omega(\langle \mathcal{F}, \mathcal{C} \rangle) = (\mathcal{R}, \{\sim_a\}_{a \in A}, V)$, *where* $\mathcal{R} = (R, \bullet, e)$, *such that:*

- $R = \mathcal{D}_r(\overline{C})/\simeq$
- $e = [1]$
- $[x] \bullet [y] = \begin{cases} \uparrow & \text{if } xy \notin \mathcal{D}_r(\overline{C}) \\ [xy] & \text{otherwise} \end{cases}$
- *For all* $a \in A$, $[x] \sim_a [y]$ *iff* $x =_a y \in \overline{C}$
- $[x] \in V(p)$ *iff* $\exists y \in L_r$ *such that* $y \simeq x \in \overline{C}$ *and* $\mathbb{T}p : y \in \mathcal{F}$

Lemma 1. *Let* $\langle \mathcal{F}, \mathcal{C} \rangle$ *be a Hintikka CSS such that* $\mathbb{F}\varphi : x \in \mathcal{F}$. *The formula* φ *is not valid and* $\Omega(\langle \mathcal{F}, \mathcal{C} \rangle)$ *is a countermodel of* φ.

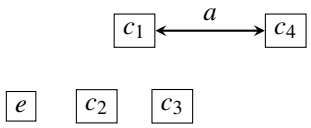
If we consider $A = \{a, b\}$ and the formula $(K_a P * K_a Q) \rightarrow K_a(P * Q)$. By application of the tableau rules, we obtain a tableau (see Fig. below) that contains a branch (denoted $\mathcal{B}$) which is a Hintikka CSS. By Lemma 1, $(K_a P * K_a Q) \rightarrow K_a(P * Q)$ is not valid and $\Omega(\mathcal{B})$ allows us to extract a countermodel using Definition 14.

We have $\mathcal{M} = \Omega(\mathcal{B}) = (\mathcal{R}, \{\sim_a\}_{a \in A}, V)$, where $\mathcal{R} = (R, \bullet, e)$, such that:

- $R = \mathcal{D}_r(\overline{C})/\simeq = \{e, [c_1], [c_2], [c_3], [c_4]\}$, where $e = [1]$ and $[c_1] = [c_2 c_3]$.
- The resource composition:

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

- The equivalence relation, where the reflexivity is not represented:



- $V(P) = \{[c_2]\}$ and $V(Q) = \{[c_3]\}$

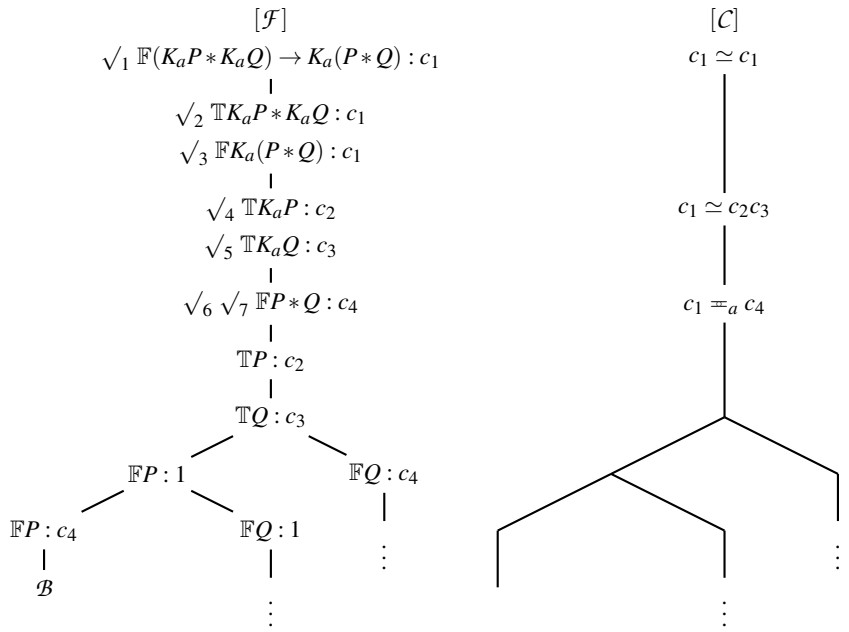


Fig. 11. Tableau $(K_aP * K_aQ) \to K_a(P * Q)$

Theorem 2 (Completeness). *Let* φ *be a ESL formula. If* φ *is valid then there exists a tableau proof for* φ.

Proof. The proof is an extension of the proof for BBI [14] to the epistemic connectives. It consists in building a Hintikka CSS from a formula for which there is no tableau proof, by using a fair strategy, that is a sequence of labelled formulae in which all labelled formulae occur infinitely many times, and an oracle, that is a set of non closed CSS with some specific properties. Then assuming there is no tableau proof for φ, we build a special CSS, that is a Hintikka CSS, and deduce from it that φ is not valid.

5 Conclusion

We have defined a new logic, called Epistemic Separation Logic (ESL), with possible worlds considered as resources, introducing the sharing and the separation on these worlds, and then we have extended it with public announcements. Moreover we propose a tableau calculus with labels and resource graphs and we show its soundness and the completeness. A countermodel extraction method is also given.
Future work will be devoted to the study of a calculus for ESL with public announcements and also of another ESL extensions that deal with epistemic actions [2,3]. Extensions with other modalities dealing with dynamic resources [6,7] will also be studied.

References

1. P. Balbiani, H. van Ditmarsch, A. Herzig, and T. de Lima. Tableaux for public announcement logics. *Journal of Logic and Computation*, 20(1):55–76, 2010.
2. A. Baltag, B. Coecke, and M. Sadrzadeh. Algebra and sequent calculus for epistemic actions. *Electronic Notes in Theoretical Computer Science*, 126:27 – 52, 2005.
3. A. Baltag, B. Coecke, and M. Sadrzadeh. Epistemic actions as resources. *Journal of Logic and Computation*, 17(3):555–585, 2006.
4. N. Biri and D. Galmiche. A Separation Logic for Resource Distribution. In *23rd Conference on Foundations of Software Technology and Theoretical Computer Science, FSTTCS'03, LNCS 2914*, pages 23–37, December 2003. Mumbai, India.
5. M. Collinson and D. Pym. Algebra and logic for resource-based systems modelling. *Mathematical Structures in Computer Science*, 19(5):959–1027, 2009.
6. J.R. Courtault and D. Galmiche. A modal extension of Boolean BI for resource transformations. In *Int. Workshop on Logics for Resources, Processes, and Programs, LRPP'13*, Nancy, France, 2013.
7. J.R. Courtault and D. Galmiche. A Modal BI Logic for Dynamic Resource Properties. In *Logical Foundations of Computer Science, LFCS 2013, LNCS 7734*, pages 134–148, 2013. San Diego, CA.
8. D. Galmiche, D. Méry, and D. Pym. The semantics of BI and Resource Tableaux. *Math. Struct. in Comp. Science*, 15(6):1033–1088, 2005.
9. J.D. Gerbrandy. *Bisimulations on Planet Kripke*. PhD thesis, University of Amsterdam, 1999. ILLC Dissertation Series DS-1999-01.
10. J.Y. Girard. Linear logic. *Theoretical Computer Science*, 50(1):1–102, 1987.
11. A. Herzig. A simple separation logic. In *Logic, Language, Information, and Computation - 20th International Workshop, WoLLIC 2013, LNCS 8071*, pages 168–178, Darmstadt, Germany, 2013.
12. S. Ishtiaq and P. O'Hearn. BI as an assertion language for mutable data structures. In *28th ACM Symposium on Principles of Programming Languages, POPL 2001*, pages 14–26, London, UK, 2001.
13. J.-J.Meyer and W. Van Der Hoek. *Epistemic Logic for AI and Computer Science*. Tracts in Theoretical Computer Science 41. Cambridge University Press, New York, NY, USA, 1995.
14. D. Larchey-Wendling. The formal strong completeness of partial monoidal Boolean BI. *Journal of Logic and Computation, first published online June 2, 2014 doi:10.1093/logcom/exu031*, 2014.
15. W. Lenzen. Recent work in epistemic logic. *Acta Philosophia Fennica*, 30:1–219, 1978.
16. M. Marion and M. Sadrzadeh. Reasoning about Knowledge in Linear Logic: Modalities and Complexity. In *Logic, Epistemology, and the Unity of Science*, pages 327–350. Kluwer Academic Publishers, 2003.
17. J.A. Plaza. Logics of public communications. In *Proc. of the 4th ISMIS*, pages 201–216. Oak Ridge National Laboratory, 1989.
18. D.J. Pym. *The Semantics and Proof Theory of the Logic of Bunched Implications*, volume 26 of *Applied Logic Series*. Kluwer Academic Publishers, 2002.
19. Y. Moses R. Fagin, J. Halpern and M. Vardi. *Reasoning About Knowledge*. MIT Press, Cambridge MA, 1995.
20. J. Reynolds. Separation logic: A logic for shared mutable data structures. In *IEEE Symposium on Logic in Computer Science*, pages 55–74, Copenhagen, Danemark, July 2002.
21. J. van Benthem and F. Liu. Dynamic logic of preference upgrade. *Journal of Applied Non-Classical Logics*, 17(2):157–182, 2007.
22. H. van Ditmarsch, W. van der Hoek, and B. Kooi. *Dynamic Epistemic Logic*. Springer Publishing Company, 2007.