**Logics in Access Control: A Conditional Approach**

# Logics in Access Control: A Conditional Approach

Valerio Genovese[⋆][1], Laura Giordano[2], Valentina Gliozzi[3], and Gian Luca Pozzato[3]

[1] University of Luxembourg and Università di Torino - Italy valerio.genovese@uni.lu
[2] Dip. di Informatica - Università del Piemonte Orientale - Italy laura@mfn.unipmn.it
[3] Dip. di Informatica - Università di Torino - Italy {gliozzi,pozzato}@di.unito.it

**Abstract.** The paper introduces a framework based on constructive conditional logics to define axiomatization, semantics and proof methods for access control logics. We formalize the well known **says** operator as a conditional normal modality and, by considering some specific combinations of access control axioms, we define four access control logics, namely, $\mathsf{Cond}^{\mathbf{UC}}_{\mathrm{ACL}}$ , $\mathsf{Cond}^{\mathbf{U4}}_{\mathrm{ACL}}$ , $\mathsf{Cond}^{\mathbf{IC}}_{\mathrm{ACL}}$ and $\mathsf{Cond}^{\mathbf{I4}}_{\mathrm{ACL}}$ . Such logics integrate access control logics with intuitionistic conditional logics and provide a natural formulation of boolean principals. The well known "speaks for" operator introduced in the logic ABLP is defined on the top of the **says** modality. We provide a Kripke model semantics for the logics and we prove that their axiomatization is sound and complete with respect to the semantics. Also, we develop sound, complete, cut-free sequent calculi for them. For the logic $\mathsf{Cond}^{\mathbf{UC}}_{\mathrm{ACL}}$ , which (as concerns atomic principals) is slightly stronger than the logic *ICL* recently introduced by Garg and Abadi, we also provide a terminating sequent calculus, thus proving that the logic is decidable and that validity in $\mathsf{Cond}^{\mathbf{UC}}_{\mathrm{ACL}}$ is in PSPACE.

## 1 Introduction

Access control is concerned with the decision of accepting or denying a request from a *principal* (e.g., user, program) to do an operation on an object. In practice, an access control system is a product of several, often independent, distributed entities with different policies that interact in order to determine access to resources. Many formal frameworks have been proposed to specify and reason about such systems [4, 6, 18, 22, 23]. A common feature of most well-known approaches is the employment of constructive logics enriched with formulas of the form $A$ **says** $\varphi$, intuitively meaning that the principal $A$ *asserts* or *supports* $\varphi$ to hold in the system. In [2] it is shown that an intuitionistic interpretation of the modality "says" allows to avoid unexpected conclusions that are derivable when **says** is given an axiomatization in classical logic.

In [13] an access control logic, *ICL*, is defined as an extension of intuitionistic propositional logic, in which the operator **says** is given a modal interpretation in the logic S4. The treatment of the operator **says** as a modality can also be found in [7], which introduces a logical framework, FSL, based on multi-modal logic methodology.

[⋆] Valerio Genovese is supported by the National Research Fund, Luxembourg.

Even if there is some agreement on looking at the **says** construct as a modal operator, the correspondence between its axiomatization and the semantic properties associated with axioms in the Kripke semantics is mainly unexplored. In fact, some of the axioms of access control logics are non-standard in modal literature. The identification of canonical properties for well-known axioms of access control logics permits to study them separately and naturally yields completeness for logics that adopt combinations of them. This methodology is significant if we want logic to be employed to compare different access control models, because different systems adopt different axioms depending on the specific application domain.

In this paper we show that conditional logics [25] can provide a general framework to define axiomatization, semantics and proof methods for access control logics. As a starting point, we concentrate on some specific combinations of access control axioms, giving rise to four conditional access control logics: $\mathsf{Cond}_{\mathrm{ACL}}^{\mathbf{UC}}$ , $\mathsf{Cond}_{\mathrm{ACL}}^{\mathbf{U4}}$ , $\mathsf{Cond}_{\mathrm{ACL}}^{\mathbf{IC}}$ , $\mathsf{Cond}_{\mathrm{ACL}}^{\mathbf{I4}}$ . Such logics integrate access control logics with intuitionistic conditional logics. We formalize the **says** operator as a conditional normal modality so that $A$ **says** $\phi$ is regarded as a conditional implication $A \Rightarrow \phi$, meaning that proposition $\phi$ holds in all the preferred worlds for the principal $A$. From the access control point of view, the **says** operator satisfies some basic axioms of access control logics [12, 13]. The generality of this approach allows a natural formalization of boolean principals [13], that is, principals which are formed by boolean combination of atomic principals, as well as a natural encoding of the well known "speaks for" operator introduced in the logic ABLP [3, 21]. We define a Kripke semantics for the conditional access control logics, as well as sound, complete, cut-free labelled sequent calculi for them.

For the logic $\mathsf{Cond}_{\mathrm{ACL}}^{\mathbf{UC}}$ , which is slightly stronger (as concerns atomic principals) than the logic *ICL* introduced in [13], we are also able to obtain a decision procedure and a complexity upper bound, namely that the problem of deciding validity in $\mathsf{Cond}_{\mathrm{ACL}}^{\mathbf{UC}}$ is decidable in PSPACE. This is in agreement with [13], which provides a PSPACE complexity result for the logic *ICL*.

The paper is structured as follows. In Section 2 we introduce the axiomatization of the intuitionistic conditional logics $\mathsf{Cond}_{\mathrm{ACL}}^{\mathbf{UC}}$ , $\mathsf{Cond}_{\mathrm{ACL}}^{\mathbf{U4}}$ , $\mathsf{Cond}_{\mathrm{ACL}}^{\mathbf{IC}}$ and $\mathsf{Cond}_{\mathrm{ACL}}^{\mathbf{I4}}$ , and we compare them with existing approaches. In Section 3 we describe the semantics of the logics. In Section 4 we show that the axiomatization is sound and complete with respect to the semantics. In Section 5 we define cut-free sequent calculi for the access control logics and we prove their soundness and completeness. For the logic $\mathsf{Cond}_{\mathrm{ACL}}^{\mathbf{UC}}$ we also show that the calculus can be turned into a terminating one by adopting some restrictions on the application of some rules: this allows us to show that the logic $\mathsf{Cond}_{\mathrm{ACL}}^{\mathbf{UC}}$ is decidable and to give a complexity upper bound for it. Section 6 contains the conclusions and a discussion of related work. This work is an extended and revised version of the work presented in [15].

## 2 Conditional Access Control Logics: the Axiom System

In this section, we introduce the conditional intuitionistic logics for access control by defining their axiomatizations. The formulation of the "says" modality as a conditional operator allows boolean principals to be modelled in a natural way, since in a conditional formula $A$ **says** $\phi$, both $A$ and $\phi$ are formulas. For instance, we can write $A \wedge B$ **says** $\phi$ to mean that principals $A$ and $B$ jointly say that $\phi$, and $A \vee B$ **says** $\phi$ to mean that principals $A$ and $B$ independently say that $\phi$. Indeed, conditional logics provide a natural generalization of multimodal logics to the case when modalities are labelled by formulas. In the following, we will regard atomic principals as atomic propositions, distinct from all the other propositions of the language and we define boolean principals as boolean formulas obtained by combining atomic principals with conjunctions and disjunctions. We will assume the propositions representing principals to have a truth value in the semantics, where a principal $A$ is true in a world $w$ if the world $w$ is *visible* to $A$. The notion of visibility we introduce is similar to the notion of visibility introduced in [12] and in [13]. Visibility is used, for each principal $A$, to identify those states of affairs (worlds) among which preferred $A$ worlds are selected. Following [13], we informally interpret proposition $A$ as "$A$ is happy", and we mean that $A$ *is happy in those worlds* $w$ *which are visible to* $A$.

We define the language $\mathcal{L}$ of the access control logics. Let $ATM$ be a set of atomic propositions, including a set $\mathcal{A}$ of propositions called *atomic principals*. We define a *(boolean) principal* to be a boolean combination of the atomic principals in $\mathcal{A}$ containing only the connectives $\wedge$ and $\vee$.

The formulas of $\mathcal{L}$ are defined inductively as follows: if $P \in ATM$, then $P \in \mathcal{L}$; $\bot \in \mathcal{L}$, where $\bot$ is a proposition which is always false; if $\varphi$, $\varphi_1$ and $\varphi_2$ are formulas of $\mathcal{L}$ and $A$ is a principal, then $\varphi_1 \wedge \varphi_2$, $\varphi_1 \vee \varphi_2$, $\varphi_1 \rightarrow \varphi_2$, and $A$ **says** $\varphi$ are formulas of $\mathcal{L}$. In the following, we will denote principals by $A, B, C, \ldots$ while we will use greek letters for arbitrary formulas. As usual, we introduce the following precedence among connectives: $\wedge, \vee,$ **says** $, \rightarrow$. As an example, $A$ **says** $\varphi \rightarrow A \wedge B$ **says** $\varphi$ is a formula of $\mathcal{L}$, to be read as $(A$ **says** $\varphi) \rightarrow ((A \wedge B)$ **says** $\varphi)$. The intended meaning of the formula $A$ **says** $\varphi$ is that *principal* $A$ *says that* $\varphi$, namely, "the principal $A$ asserts or supports $\varphi$" [13].

In the following we introduce the axiomatization of the logic $\mathsf{Cond}_{\mathrm{ACL}}^{\mathbf{UC}}$ , first. Then, we present the axiomatization of the other logics by changing some characterizing access control axioms.

The axiomatization of $\mathsf{Cond}_{\mathrm{ACL}}^{\mathbf{UC}}$ contains few basic axioms for access control logics [2, 13], as well as additional axioms governing the behavior of boolean principals. Because we privilege the modularity of the approach, we are interested in considering each axiom separately. As a consequence, the resulting axiomatization might be redundant.

### 2.1 Basic Axioms

The *axiom system* of $\mathsf{Cond}_{\mathrm{ACL}}^{\mathbf{UC}}$ contains the following axioms and inference rules, which are intended to capture the basic properties of the **says** operator.

(FALSE) $\bot \rightarrow \gamma$
(THEN-1) $\alpha \rightarrow (\beta \rightarrow \alpha)$
(THEN-2) $(\alpha \rightarrow (\beta \rightarrow \gamma)) \rightarrow ((\alpha \rightarrow \beta) \rightarrow (\alpha \rightarrow \gamma))$
(AND-1) $\alpha \wedge \beta \rightarrow \alpha$
(AND-2) $\alpha \wedge \beta \rightarrow \beta$

(AND-3) $\alpha \rightarrow (\beta \rightarrow (\alpha \wedge \beta))$
(OR-1) $\alpha \rightarrow \alpha \vee \beta$
(OR-2) $\beta \rightarrow \alpha \vee \beta$
(OR-3) $(\alpha \rightarrow \beta) \rightarrow ((\gamma \rightarrow \beta) \rightarrow (\alpha \vee \gamma \rightarrow \beta))$
(K) $A\ \textbf{says}\ (\alpha \rightarrow \beta) \rightarrow (A\ \textbf{says}\ \alpha \rightarrow A\ \textbf{says}\ \beta)$
(UNIT) $\alpha \rightarrow (A\ \textbf{says}\ \alpha)$
(C) $A\ \textbf{says}\ (A\ \textbf{says}\ \alpha \rightarrow \alpha)$
(MP) If $\vdash \alpha$ and $\vdash \alpha \rightarrow \beta$ then $\vdash \beta$
(RCEA) If $\vdash A \leftrightarrow B$ then $\vdash (A\ \textbf{says}\ \gamma) \leftrightarrow (B\ \textbf{says}\ \gamma)$
(RCK) If $\vdash \alpha \rightarrow \beta$ then $\vdash (A\ \textbf{says}\ \alpha) \rightarrow (A\ \textbf{says}\ \beta)$

**Definition 1.** *We say that a formula $\alpha$ is a theorem of the logic, and write $\vdash \alpha$ if there is a derivation of $\alpha$ from the above axioms and rules. We say that $\alpha$ can be derived from a set of formulas $\Gamma$, and write $\Gamma \vdash \alpha$, if there are $\gamma_1, \ldots \gamma_n$ ($n \geq 0$) in $\Gamma$ such that $\vdash \gamma_1 \wedge \ldots \wedge \gamma_n \rightarrow \alpha$.*

The definition of derivability above is taken from [8] (Definition 2.14). The axioms and rules (FALSE), (THEN-1), (THEN-2), (AND-1), (AND-2), (AND-3), (OR-1), (OR-2), (OR-3), and (MP) are axioms and rules of intuitionistic logic. The rule (MP) is modus ponens. (RCK) and (RCEA) are standard inference rules for conditional logics. (RCK) plays the role of the rule of Necessitation (if $\vdash \phi$ then $\vdash \Box\phi$) in modal/multimodal logic and is derivable in both *ICL* [13] and DTL$_0$ [12]. (RCEA) makes the formulas $A$ **says** $\phi$ and $B$ **says** $\phi$ equivalent when the principals $A$ and $B$ are equivalent (i.e. if the worlds visible to $A$ are the same as the worlds visible to $B$, then principals $A$ and $B$ support the same formulas). (UNIT) and (K) are the characterizing axioms of the logic *ICL* [13] and other access control logics [1, 14, 29]. The axiom (K) belongs to the axiomatization of all normal modal logics and it is derivable in "normal" conditional logics. Intuitively, (K) expresses that **says** is closed under logical consequence, while (UNIT) is a stronger form of necessitation which states, for every formula $\alpha$, that if $\alpha$ holds, then $\alpha$ is supported by every principal. Axiom (C) has been included in the axiomatization of the logic DTL$_0$ in [12] and it comes from doxastic logic [30]. Intuitively, (C) means that every principal says that all its statements are true.

The choice of the above axioms is meaningful in the context of access control. However, other axioms have been proposed in the literature and different access control logics have been defined through their combination. In particular, in alternative to (C) and (UNIT), weaker axioms have been proposed, namely, (C4) and (I):

(C4) $(A\ \textbf{says}\ (A\ \textbf{says}\ \alpha)) \rightarrow (A\ \textbf{says}\ \alpha)$
(I) $(A\ \textbf{says}\ \alpha) \rightarrow (B\ \textbf{says}\ A\ \textbf{says}\ \alpha)$

(C4) belongs to the original axiomatization of the logic *ICL* defined in [13], where it replaces the axiom (C). (I) is introduced in the axiomatization of the logic Binder [9], which extends the logic ABLP [3, 21] in order to express the so called *authorization policies*. Notice that (I) is a weaker version of (UNIT).

As axiom (C) is stronger than (C4), it can be proved that $\mathsf{Cond}^{\mathbf{UC}}_{\mathrm{ACL}}$ is stronger than the logic *ICL* [13]:

**Theorem 1.** *For all formulas $\varphi$, $\vdash_{\mathrm{ICL}} \varphi$ implies $\vdash \varphi$.*

In the following, besides $\mathsf{Cond}^{\mathbf{UC}}_{\mathrm{ACL}}$ , we introduce three other logics for access control obtained by considering different combinations of the above axioms (UNIT), (I), (C), and (C4), as summarized in Figure 1.

| Logic | (UNIT) vs (I) | (C) vs (C4) |
|---|---|---|
| $\mathsf{Cond}^{\mathbf{UC}}_{\mathrm{ACL}}$ | (UNIT) | (C) |
| $\mathsf{Cond}^{\mathbf{U4}}_{\mathrm{ACL}}$ | (UNIT) | (C4) |
| $\mathsf{Cond}^{\mathbf{IC}}_{\mathrm{ACL}}$ | (I) | (C) |
| $\mathsf{Cond}^{\mathbf{I4}}_{\mathrm{ACL}}$ | (I) | (C4) |

**Fig. 1.** Summary of constructive conditional logics under consideration.

### 2.2 Axioms for boolean principals

The axioms introduced above do not enforce by themselves any intended property of boolean principals. In this subsection, we discuss the properties that are intended for boolean principals and we introduce axioms which capture such properties. Specifically, we focus on the intended meaning of conjunctions and disjunctions among principals.

Our interpretation of the statement $A \wedge B$ **says** $\phi$ is that $A$ *and* $B$ *jointly (combining their statements) say that* $\phi$. It comes from the interpretation of the statement as a conditional implication: $A$ and $B$ (jointly) conditionally prove $\phi$. Instead, our interpretation of the statement $A \vee B$ **says** $\phi$ is that $A$ *and* $B$ *disjointly (independently) say that* $\phi$, which comes from the reading of the conditional formula as $A$ and $B$ (disjointly) conditionally prove $\phi$. Concerning the statement $A \vee B$ **says** $\phi$, we expect that if both $A$ says $\phi$ and $B$ says $\phi$, then $A$ and $B$ disjointly (independently) say that $\phi$. This property can be captured by the following axiom:

$$A \textbf{ says } \phi \wedge B \textbf{ says } \phi \rightarrow A \vee B \textbf{ says } \phi$$

which corresponds to the well known axiom (CA) of conditional logics [25]. Similarly, we can expect that the converse axiom

$$A \vee B \textbf{ says } \phi \rightarrow A \textbf{ says } \phi \wedge B \textbf{ says } \phi$$

holds. The two axioms together enforce the property that $A$ and $B$ disjointly say that $\phi$ if and only if $A$ says that $\phi$ and $B$ says that $\phi$ .

Concerning $A \wedge B$ **says** $\phi$, we expect that $A$ and $B$ jointly say that $\phi$ when either $A$ or $B$ says that $\phi$. This condition can be enforced by introducing the axiom

$$A \textbf{ says } \phi \rightarrow A \wedge B \textbf{ says } \phi$$

which, although is a controversial axiom of conditional logics, called monotonicity[4], is consistent with the intuitive reading of boolean principals in this intuitionistic setting. For instance, assume that Administrator 1 says that, if user 1 is a superuser, then he has write premissions

$$Admin_1 \textbf{ says } (SuperUser\_user_1 \rightarrow write\_perm\_user_1)$$

and that Administrator 2 says that user 1 is a superuser

$$Admin_2 \textbf{ says } SuperUser\_user_1$$

From these two statements we can conclude that Administrator 1 and Administrator 2, together, say that user 1 has write permissions:

$$Admin_1 \wedge Admin_2 \textbf{ says } write\_perm\_user_1$$

Conversely, we would like to have the property that if $A \wedge B$ **says** $\phi$ then, by combining the statements of $A$ and $B$, $\phi$ can be concluded. This is not equivalent to saying that either $A$ says $\phi$ or $B$ says $\phi$. Indeed, the axiom $(A \wedge B \textbf{ says } \phi) \rightarrow (A \textbf{ says } \phi) \vee (B \textbf{ says } \phi)$ is too strong and not wanted. The wanted property could, for instance, be captured by the second order axiom $(A \wedge B \textbf{ says } \phi) \rightarrow \exists\psi((A \textbf{ says } \psi \rightarrow \phi) \wedge B \textbf{ says } \psi)$. In the following, however, we show that it is possible to capture the wanted property by using standard axioms of conditional logics, namely:

(DT) $A \wedge B \textbf{ says } \phi \rightarrow (A \textbf{ says } (B \rightarrow \phi))$
(ID) $A \textbf{ says } A$

Together such axioms enforce the property that if $A \wedge B$ **says** $\phi$ then, by combining the statements of $A$ and $B$, $\phi$ can be concluded. The intended meaning of (DT) is that, if $A \wedge B$ **says** $\phi$, then $A$ says that $\phi$ holds in all $B$ worlds, i.e., in all the worlds visible to the principal $B$ or in all the worlds in which $B$ is *happy*. The meaning of (ID) is that "$A$ says that principal $A$ is happy", i.e., all the state of affairs (worlds) preferred by $A$ are worlds visible to $A$. We will come back to the notion of visibility in Section 3, when describing the semantic conditions associated with the axioms.

In conclusion, to deal with boolean principals, the axiomatization of the conditional access control logics introduced above includes, in addition to the axioms in Section 2.1, the following axioms:

(CA) $A \textbf{ says } \phi \wedge B \textbf{ says } \phi \rightarrow A \vee B \textbf{ says } \phi$
(CA-conv) $A \vee B \textbf{ says } \phi \rightarrow A \textbf{ says } \phi$
(Mon) $A \textbf{ says } \phi \rightarrow A \wedge B \textbf{ says } \phi$
(DT) $A \wedge B \textbf{ says } \phi \rightarrow (A \textbf{ says } (B \rightarrow \phi))$
(ID) $A \textbf{ says } A$

[4] In general, conditional logics only allow weaker forms of monotonicity, encoded, for instance, by the axiom (CV) of Lewis' logic VC.

The first three axioms are those introduced above. Notice that, the two axioms (DT) and (ID) allow propositions representing principals to occur on the right hand side of the **says** modality.

Observe that, as a difference with *ICL*$^{\mathcal{B}}$ [13], where implication within principals is used to capture the "speaks for" operator, here we do not allow an implication among principals to occur on the left hand side of the says modality. In Section 2.3, we will address the problem of capturing the "speaks for" operator. Moreover, let us observe that, by the normality of the conditional **says** modality, two principals that are logically equivalent as, for instance, principal $A \wedge B$ and principal $A \wedge B \wedge A$ support the same formulas through the **says** modality. This is an advantage of conditional logic over a multi-modal logic in which principals are simply regarded as labels of modalities.

**Theorem 2.** *The above axiomatization is consistent.*

*Proof.* Consistency immediately follows from the fact that, by replacing $A$ **says** $B$ with the intuitionistic implication $A \rightarrow B$, we obtain axioms which are all derivable in intuitionistic logic. □

Let us observe that the above interpretation of conjunction and disjunction between principals is different from the one given in the logic *ICL*$^{\mathcal{B}}$ [13], which actually adopts the opposite interpretation of $\wedge$ and $\vee$: in Garg and Abadi's logic *ICL*$^{\mathcal{B}}$, the meaning of $A \wedge B$ **says** $\phi$ is the same as $A$ **says** $\phi \ \wedge\ B$ **says** $\phi$, while $A \vee B$ **says** $\phi$ means that, by combining the statements of $A$ and $B$, $\phi$ can be concluded. Due to this difference, the properties of the principal $A \wedge B$ in our logic are properties of the principal $A \vee B$ in their logic and, vice-versa, the properties of the principal $A \vee B$ in our logic are properties of the principal $A \wedge B$ in their logic. We do not argue that our interpretation of boolean principals is better that the one in [13], we just observe that it naturally derives from the interpretation of the boolean connectives in the principals, according to the usual semantics of conditionals. Observe that the axioms (trust), (untrust) and (cuc') of the logic *ICL*$^{\mathcal{B}}$ are not derivable from our axiomatization. Also, the addition of the axiom (untrust) $\top$ **says** $\bot$ to our axiomatization would entail that for all principals $A$, $A$ **says** $\bot$, which is an unwanted property.

As an example, assume we want to check whether, given a set of policies $\Gamma$, a principal $A$ is authorized to perform $\phi$ in the logic $\mathsf{Cond}_{\mathrm{ACL}}^{\mathbf{UC}}$ , or, in other words, the request $\phi$ from a principal $A$ is compliant with the set of policies $\Gamma$. Intuitively, given a set of formulas $\Gamma$ representing policies and a formula $\phi$, we say that the request $\phi$ from a principal $A$ is compliant with $\Gamma$ if and only if $\phi$ can be derived from $\Gamma \cup \{A$ **says** $\phi\}$ in the sense of Definition 1, i.e. if and only if $\Gamma, A$ **says** $\phi \vdash \phi$.

*Example 1.* Let $\Gamma$ contain the following formulas (rules):

- $Admin_1$ **says** $(SuperUser\_user_1 \rightarrow write\_perm\_user_1)$
- $Admin_2$ **says** $SuperUser\_user_1$
- $((Admin_1 \wedge Admin_2)$ **says** $delete\_file_1) \rightarrow delete\_file_1$
- $Admin_1 \wedge Admin_2$ **says** $((write\_perm\_user_1 \wedge (user_1$ **says** $delete\_file_1)) \rightarrow delete\_file_1)$

The first two rules have been already introduced above. By the third rule, when Administrator 1 and Administrator 2, together, say that file 1 has to be deleted, then file 1 has to be deleted. By the last rule, when Administrator 1 and Administrator 2, together, say that, when user 1 has write permissions and user 1 says to delete file 1, then file 1 has to be deleted. We can prove that

$$\Gamma, \mathit{user_1}\ \textbf{says}\ \mathit{delete\_file_1} \vdash \mathit{delete\_file_1}$$

In fact, as we have already seen, $(i)$ $(\mathit{Admin_1} \wedge \mathit{Admin_2})$ **says** $\mathit{write\_perm\_user_1}$ follows from the first two rules by (Mon). From $\mathit{user_1}$ **says** $\mathit{delete\_file_1}$, we infer by (UNIT) $(ii)$ $(\mathit{Admin_1} \wedge \mathit{Admin_2})$ **says** $(\mathit{user_1}$ **says** $\mathit{delete\_file_1})$. By propositional reasoning, (RCK) and (K), from $(i)$ and $(ii)$, we derive $(\mathit{Admin_1} \wedge \mathit{Admin_2})$ **says** $(\mathit{write\_perm\_user_1} \wedge (\mathit{user_1}$ **says** $\mathit{delete\_file_1}))$. Finally, from the fourth rule, we conclude $(\mathit{Admin_1} \wedge \mathit{Admin_2})$ **says** $\mathit{delete\_file_1}$, and hence, by rule 3, we conclude $\mathit{delete\_file_1}$.

To conclude this section, let us consider the well known axiom of conditional logics (MP), $A$ **says** $\phi \rightarrow (A \rightarrow \phi)$. Its meaning is the following: “If $A$ says $\phi$, then $\phi$ holds in all the worlds visible to principle $A$”.

We observe that the addition of the axiom (MP) to the logics containing the axiom (UNIT), namely $\mathsf{Cond}^{\mathbf{UC}}_{\mathrm{ACL}}$ and $\mathsf{Cond}^{\mathbf{U4}}_{\mathrm{ACL}}$ , would make the modality **says** to collapse into intuitionistic implication. In fact, it is easy to see that the converse of (MP), namely $(A \rightarrow \phi) \rightarrow A$ **says** $\phi$, can be derived from axioms (UNIT), (ID) and (K).

**Proposition 1.** $(A \rightarrow \phi) \rightarrow (A$ **says** $\phi)$ *is derivable in* $\mathsf{Cond}^{\mathbf{UC}}_{\mathrm{ACL}}$ *and* $\mathsf{Cond}^{\mathbf{U4}}_{\mathrm{ACL}}$ .

*Proof.* From (UNIT), we have $(A \rightarrow \phi) \rightarrow (A$ **says** $(A \rightarrow \phi))$. From (K), $(A$ **says** $(A \rightarrow \phi)) \rightarrow (A$ **says** $A \rightarrow A$ **says** $\phi)$. Hence, by propositional reasoning, $(A \rightarrow \phi) \rightarrow (A$ **says** $A \rightarrow A$ **says** $\phi)$, and then $A$ **says** $A \rightarrow ((A \rightarrow \phi) \rightarrow (A$ **says** $\phi))$. From (ID), $A$ **says** $A$ hence, by modus ponens, $(A \rightarrow \phi) \rightarrow (A$ **says** $\phi)$. □

Although the addition of (MP) makes the logic collapse into intuitionistic logic in the presence of axiom (UNIT), the same does not hold when (UNIT) is replaced by the weaker axiom (I).

### 2.3 Speaks For

The *Speaks For* operator has been introduced in the logic ABLP [3, 21] to reason about transfer of authority from one principal to another. We show that *Speaks For* can be defined in the constructive conditional logics introduced above by using the **says** modality.

Let $\Rightarrow$ be a new connective. $A \Rightarrow B$ is read $A$ *speaks for* $B$, meaning that if $A$ says $\alpha$, then also $B$ says $\alpha$, for any formula $\alpha$. In line with previous literature on access control, the connective $\Rightarrow$ is ruled by the following axioms:

(Speaks For) $(A \Rightarrow B) \rightarrow ((A$ **says** $\alpha) \rightarrow (B$ **says** $\alpha))$
(Reflexivity) $A \Rightarrow A$
(Transitivity) $(A \Rightarrow B) \rightarrow ((B \Rightarrow C) \rightarrow (A \Rightarrow C))$
(Handoff) $(A$ **says** $(B \Rightarrow A)) \rightarrow (B \Rightarrow A)$

where axioms (Speaks for) and (Handoff) relate the connective $\Rightarrow$ with the **says** modality. We can define the connective $\Rightarrow$ by means of the **says** modality as follows:

$$A \Rightarrow B \text{ iff } B \textbf{ says } A$$

In agreement with the interpretation of proposition $A$ as "$A$ is happy", the meaning of $B$ **says** $A$ is that "$B$ says that $A$ is happy", i.e. that all the worlds preferred to $B$ are worlds visible to $A$ (i.e. worlds in which $A$ is happy). It is easy to see that the connective $\Rightarrow$ has the properties encoded by the four axioms above.

**Theorem 3.** *The axioms* (Speaks For), (Reflexivity), (Transitivity) *and* (Handoff) *are derivable in the logics* $\mathsf{Cond}^{\mathbf{UC}}_{\mathrm{ACL}}$ , $\mathsf{Cond}^{\mathbf{U4}}_{\mathrm{ACL}}$ , $\mathsf{Cond}^{\mathbf{IC}}_{\mathrm{ACL}}$ *, and* $\mathsf{Cond}^{\mathbf{I4}}_{\mathrm{ACL}}$ *, given the definition of* $A \Rightarrow B$ *as* $B$ **says** $A$*.*

*Proof.* To prove that axiom (Speaks For) is derivable, we have to prove that

$$(B \textbf{ says } A) \rightarrow ((A \textbf{ says } \alpha) \rightarrow (B \textbf{ says } \alpha))$$

is derivable. Given (Mon) $A$ **says** $\alpha \rightarrow (A \wedge B)$ **says** $\alpha$ and (DT) $(A \wedge B)$ **says** $\alpha \rightarrow B$ **says** $(A \rightarrow \alpha)$, by propositional reasoning, we have that $A$ **says** $\alpha \rightarrow B$ **says** $(A \rightarrow \alpha)$ is derivable. Also, from (K), $B$ **says** $(A \rightarrow \alpha) \rightarrow (B$ **says** $A \rightarrow B$ **says** $\alpha)$ is derivable. By propositional reasoning, we get $A$ **says** $\alpha \rightarrow (B$ **says** $A \rightarrow B$ **says** $\alpha)$, and, hence, $B$ **says** $A \rightarrow (A$ **says** $\alpha \rightarrow B$ **says** $\alpha)$ is derivable.

To prove that (Transitivity) is derivable, the formula $(B$ **says** $A) \rightarrow ((C$ **says** $B) \rightarrow (C$ **says** $A))$ can be shown to be derivable again by using (Mon) and (DT), as in the previous case.

(Reflexivity) is derivable as, by (ID), $A$ **says** $A$, which means that $A \Rightarrow A$.

To prove that (Handoff) is derivable, we need to show that $(A$ **says** $(A$ **says** $B)) \rightarrow (A$ **says** $B)$ is derivable. For the logics containing the axiom (C), it follows immediately from (C) and (K). For the logics containing the axiom (C4), it is an instance of (C4). □

It is important to underline that the proposed encoding of *Speaks for* is possible because **says** is a conditional modality. Moreover, such embedding is *independent* from the choice of the characterizing access control axioms we have considered.

It has to be observed that the fact that the axiom (UNIT) can be applied also to principals may lead to some unintended conclusions. In particular, from (UNIT), when $\alpha$ is the principal $B$, we get $B \rightarrow (A$ **says** $B)$, that is,

$$B \rightarrow (B \Rightarrow A)$$

saying that in all the worlds visible to principal $B$, $B$ speaks for $A$, as well as

$$B \textbf{ says } (B \Rightarrow A)$$

(which is not derivable in *ICL*$^{\Rightarrow}$ [13]). By this property, we can conclude $B$ **says** $(A$ **says** $\varphi)$ from $B$ **says** $(B$ **says** $\varphi)$, for all formulas $\varphi$. This conclusion may seem to be unintended. Observe, however, that, even when the application of (UNIT) is restricted to formulas that are not principals, as in [13], the property $B$ **says** $(B$ **says** $\varphi) \rightarrow B$ **says** $(A$ **says** $\varphi)$ is anyhow derivable from (UNIT), (K) and (C), as well as from (UNIT), (K) and (C4).

Hence, it holds in *ICL* [13], as well as in any logic including (UNIT) and the non controversial axioms (K) and (C4). This may suggest that axiom (UNIT) itself is too strong even when applied only to formulas which are not principals.

As another observation, notice that, when (RCK) is applied to principals, we get:

$$\text{if} \vdash A \rightarrow B, \text{then} \vdash (A \Rightarrow C) \rightarrow (B \Rightarrow C).$$

In a sense, $\vdash A \rightarrow B$ (all the worlds visible to $A$ are also visible to $B$) appears to say something similar to "$B$ speaks for $A$". Actually, in the presence of (UNIT), $(A \rightarrow B) \rightarrow (B \Rightarrow A)$ is derivable (see Proposition 1), so that $\vdash A \rightarrow B$ entails $\vdash (A \Rightarrow C) \rightarrow (B \Rightarrow C)$ by the (Transitivity) of $\Rightarrow$. A similar property also holds in *ICL*$^{\Rightarrow}$ as well as in *ICL*$^{\mathcal{B}}$ [13], namely, if $\vdash B \rightarrow A$, then $\vdash (A \Rightarrow C) \rightarrow (B \Rightarrow C)$ (in *ICL*$^{\mathcal{B}}$ it follows from (untrust) by the transitivity of the speaks for; in *ICL*$^{\Rightarrow}$ $B \Rightarrow A$ is defined as $\Box(B \rightarrow A)$ and the property above follows form transitivity of the speaks for). The difference among the two properties is due to a different interpretation of visibility here as compared to visibility in [13] (see Section 3 below): here $\vdash A \rightarrow B$ means that all the worlds visible to $A$ are also visible to $B$, while in [13] $\vdash B \rightarrow A$ means that all the worlds non visible to $B$ are non visible to $A$. Actually, (by contraposition) they have the same meaning.

In the following we will provide a semantics for the four access control logics introduced so far.

## 3 Conditional Access Control Logics: the Semantics

In this section we introduce a Kripke semantics for the four access control logics introduced above. As the Speaks For connective is a defined connective, we will not take the Speaks For into consideration in this section.

We first define the semantics of $\mathsf{Cond}^{\mathbf{UC}}_{\mathrm{ACL}}$ , then we present the semantics of the other logics by deifning the characterizing conditions on their models. The semantics of the logic $\mathsf{Cond}^{\mathbf{UC}}_{\mathrm{ACL}}$ is defined as follows.

**Definition 2.** *A* $\mathsf{Cond}^{\mathbf{UC}}_{\mathrm{ACL}}$ *model has the form* $\mathcal{M} = (S, \leq, \{R_A\}, h)$ *where:* $S \neq \emptyset$ *is a set of items called worlds;* $\leq$ *is a preorder over S;* $R_A$ *is a binary relation on* $S$ *associated with the formula* $A$*;* $h$ *is an evaluation function* $ATM \longrightarrow Pow(S)$ *that associates to each atomic proposition* $P$ *the set of worlds in which* $P$ *is true.*

*We define the truth conditions of a formula* $\phi \in \mathcal{L}$ *with respect to a world* $t \in S$ *in a model* $\mathcal{M}$*, by the relation* $\mathcal{M}, t \models \phi$*, as follows. We use* $[|\phi|]$ *to denote* $\{y \in S \mid \mathcal{M}, y \models \phi\}$.

1. $\mathcal{M}, t \models P \in ATM$ *iff, for all* $s$ *such that* $t \leq s$, $s \in h(P)$
2. $\mathcal{M}, t \models \varphi \wedge \psi$ *iff* $\mathcal{M}, t \models \varphi$ *and* $\mathcal{M}, t \models \psi$
3. $\mathcal{M}, t \models \varphi \vee \psi$ *iff* $\mathcal{M}, t \models \varphi$ *or* $\mathcal{M}, t \models \psi$
4. $\mathcal{M}, t \models \varphi \rightarrow \psi$ *iff for all* $s$ *such that* $t \leq s$ *(if* $\mathcal{M}, s \models \varphi$ *then* $\mathcal{M}, s \models \psi$*)*
5. $\mathcal{M}, t \not\models \bot$
6. $\mathcal{M}, t \models A$ **says** $\psi$ *iff, for all* $s$ *such that* $tR_As$, $\mathcal{M}, s \vDash \psi$.

*Given a world* $t \in S$ *and a formula* $A \in \mathcal{L}$*, we define* $R_A(t) = \{s \in S \mid tR_As\}$*. The relations* $\leq$ *and* $R_A$ *must satisfy the following conditions:*

$\forall t, s, z \in S$, *if* $s \leq t$ *and* $tR_A z$ *then* $sR_A z$; (S-Int)
$\forall t, s \in S$, *if* $sR_A t$, *then* $s \leq t$; (S-UNIT)
$\forall t, s, z \in S$, *if* $sR_A t$ *and* $t \leq z$, *then* $zR_A z$; (S-C)
$R_{A \vee B}(t) = R_A(t) \cup R_B(t)$; (S-CA)
$\forall t, s, z \in S$, *if* $sR_{A \wedge B} t$, *then* $sR_A t$ *and* $sR_B t$; (S-Mon)
$\forall t, s, z \in S$, *if* $sR_A t$ *and* $t \leq z$, *and* $z \in [|B|]$, *then* $sR_{A \wedge B} z$; (S-DT)
$\forall t, s \in S$, *if* $sR_A t$, *then* $t \in [|A|]$; (S-ID)
*if* $[|A|] = [|B|]$, *then* $R_A = R_B$. (S-RCEA)

*We say that* $\phi$ *is valid in a model* $\mathcal{M}$ *if* $\mathcal{M}, t \models \phi$ *for all* $t \in S$. *We say that* $\phi$ *is* valid tout court *(and write* $\models \phi$*) if* $\phi$ *is valid in every model. We extend the notion of validity to a set of formulas* $\Gamma$ *in the obvious way: for all* $t$, $\mathcal{M}, t \models \Gamma$ *if* $\mathcal{M}, t \models \psi$ *for all* $\psi \in \Gamma$. *Last, we say that* $\phi$ *is a* logical consequence *of* $\Gamma$ *(and write* $\Gamma \models \phi$*) if, for all models* $\mathcal{M}$*, for all worlds* $t \in S$*, if* $\mathcal{M}, t \models \Gamma$*, then* $\mathcal{M}, t \models \phi$.

Condition (S-Int) enforces the property that when a formula $A$ **says** $\phi$ is true in a world $t$, it is also true in all worlds reachable from $t$ by the relation $\leq$ (i.e., in all worlds $s$ such that $t \leq s$). All the other semantic conditions are those associated with the axioms of the logic, apart from condition (S-RCEA), which is the well-known condition for normality in conditional logics, claiming that the accessibility relation $R_A$ is associated with the semantic interpretation of $A$. Namely, if the worlds in which $A$ is visible are the same as those in which $B$ is visible, then the worlds reachable by $R_A$ are the same as those reachable by $R_B$. (S-CA) is the semantic condition for both axioms (CA) and its converse. Notice that, the fact that we represent the binary relation $R_A$ as indexed by a formula does not mean that the semantics for conditional logic is second-order. In fact, $R_A$ represent a selection function (which is used in most formulations of conditional logic semantics), in which $sR_A t$ corresponds to $t \in f([|A|], s)$, where $[|A|]$ is a set of worlds. In this view, the semantic conditions above must be intended as first-order because they quantify over individuals (i.e. worlds) and subsets of the domain (indexes of the binary relation) identified by formulas of the language [5].

Note also that the semantic conditions for some of the axioms, as for instance (DT), slightly depart from the semantic conditions usually given to these axioms in conditional logic. This is due to the fact that our logics are intuitionistic conditional logics and the implication occurring within axioms is intuitionistic implication. Observe that the satisfiability of atomic propositions is defined as usual in intuitionistic logic: the evaluation of a proposition in a world depends on the evaluation of that proposition in all the worlds reachable by $\leq$.

Our semantics assigns a truth value to atomic and boolean principals. The intended meaning is that a principal $A$ is true in a world $w$ when $w$ is *visible* to $A$. The notion of visibility of a world to a principal has been used in the context of access control in [13] as well as in [12]. In particular, the Kripke models for *ICL* [13] include a *view map*, mapping each principal $A$ to the set of worlds which are not visible to $A$. The Kripke semantics in [12] makes use of a view function $\theta$ which maps each world to

[5] It is well known that the extension of first-order logic with quantification over a family of subsets of the domain does not add expressivity because it is equivalent to multi-sorted first-order logic (see [10] Section 4.4).

the set of principals to which the worlds is visible, and it includes the semantic condition (Imp-mon) $w \leq w'$ implies $\theta(w) \subseteq \theta(w')$, which requires that, if a world is visible to a principal $A$, then all the worlds reachable from $w$ are visible to $A$. As a difference with [13] (and similarly to [12]), a property analogous to (Imp-mon) holds in our semantics. Notice that, although the notion of visibility introduced in [13] and [12] is not expressible at the language level, and, in particular, it is not expressible in *ICL* and *ICL*$^{\mathcal{B}}$, however, it can be expressed in the S4 embedding of *ICL* and *ICL*$^{\mathcal{B}}$, where a principal $A$ is not forced to occur on the left hand side of the **says** modality. Our choice of allowing principals to freely occur within formulas, is dictated by the need to provide an axiomatic counterpart to all the semantic conditions in the Kripke models.

Concerning the interpretation of boolean conditionals and, in particular, of the conjunction between principals, it can be proved that, from the semantic conditions (S-Mon), (S-ID) and (S-DT) it follows that:

**Proposition 2.** $R_{A\wedge B}(t) = R_A(t) \cap R_B(t)$.

*Proof.* First, we prove that $R_{A\wedge B}(s) \subseteq R_A(s) \cap R_B(s)$. Let $t \in S$ be a world such that $sR_{A\wedge B}t$. By (S-Mon), we immediately conclude that also $sR_At$ and $sR_Bt$, and we are done.

Finally, we prove that $R_A(s) \cap R_B(s) \subseteq R_{A\wedge B}(s)$. Let $t \in S$ be a world such that $(i)$ $sR_At$ and $(ii)$ $sR_Bt$. By (S-ID), from $(ii)$ it follows that $(iii)$ $t \in [|B|]$. Since $\leq$ is reflexive, we have that $t \leq t$. By (S-DT), from $(i)$ $sR_At$, $t \leq t$, and $(iii)$ $t \in [|B|]$, we conclude that $sR_{A\wedge B}t$ and we are done. □

By the presence of the axiom (C), it turns out that the semantic condition (S-DT) can be equivalently expressed as follows:

**Proposition 3.** *In the axiomatization of* $\mathsf{Cond}_{\mathrm{ACL}}^{\mathbf{UC}}$ *, the following are equivalent:*

1. $\forall t, s, z \in S$*, if* $sR_At$ *and* $t \leq z$*, and* $z \in [|B|]$*, then* $sR_{A\wedge B}z$*;*
2. $\forall t, s \in S$*, if* $sR_At$ *and* $t \in [|B|]$*, then* $sR_{A\wedge B}t$*.*

*Proof.* Let us first prove that, if 1. holds, then also 2. holds. Since $\leq$ is reflexive, we have that $t \leq t$. By replacing $z$ with $t$ in 1., we have that, $\forall t, s \in S$, if $sR_At$ and $t \in [|B|]$, then $sR_{A\wedge B}t$, i.e. 2. holds. Now we prove that, if 2. holds, then also 1. holds. Suppose that $sR_At$ and consider $t \leq z$. By the semantic condition (S-C), we have that also $zR_Az$. By (S-UNIT), we can also observe that $s \leq t$ since $sR_At$. Since $\leq$ is transitive, from $s \leq t$ and $t \leq z$ it follows that $s \leq z$. By the semantic condition (S-Int), since $zR_Az$ and $s \leq z$, we have that also $sR_Az$. If $z \in [|B|]$, since $sR_Az$, by 2. we have that $sR_{A\wedge B}z$, i.e. also 1. holds. □

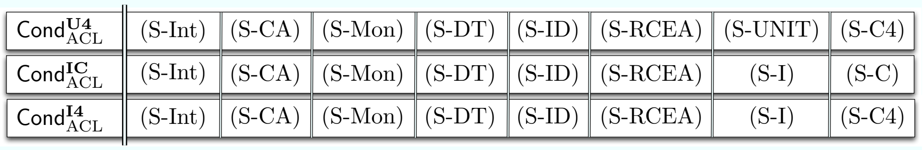
This allows the semantic condition (S-DT) to be equivalently expressed in $\mathsf{Cond}_{\mathrm{ACL}}^{\mathbf{UC}}$ as follows:

$$\forall t, s \in S, \text{ if } sR_At \text{ and } t \in [|B|], \text{ then } sR_{A\wedge B}t \qquad \text{(S-DT)}$$

Let us now introduce the semantic properties that correspond to axioms (C4) and (I) introduced above as alternatives to (C) and (UNIT), characterizing the logics $\mathsf{Cond}_{\mathrm{ACL}}^{\mathbf{U4}}$ , $\mathsf{Cond}_{\mathrm{ACL}}^{\mathbf{IC}}$ and $\mathsf{Cond}_{\mathrm{ACL}}^{\mathbf{I4}}$ , as follows:

$\forall t, s \in S$, if $sR_At$, then $\exists z \in S$ such that $sR_Az$ and $zR_At$; (S-C4)
$\forall t, s, u \in S$, if $tR_Bs$ and $sR_Au$, then $tR_Au$ (S-I)

**Definition 3.** *A model for the logics* $\mathsf{Cond}^{\mathbf{U4}}_{\mathrm{ACL}}$ , $\mathsf{Cond}^{\mathbf{IC}}_{\mathrm{ACL}}$ *and* $\mathsf{Cond}^{\mathbf{I4}}_{\mathrm{ACL}}$ *is as in Definition 2. The relations $\leq$ and $R_A$ satisfy the semantic conditions characterizing each logic as stated in Figure 2.*



| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| $\mathsf{Cond}^{\mathbf{U4}}_{\mathrm{ACL}}$ | (S-Int) | (S-CA) | (S-Mon) | (S-DT) | (S-ID) | (S-RCEA) | (S-UNIT) | (S-C4) |
| $\mathsf{Cond}^{\mathbf{IC}}_{\mathrm{ACL}}$ | (S-Int) | (S-CA) | (S-Mon) | (S-DT) | (S-ID) | (S-RCEA) | (S-I) | (S-C) |
| $\mathsf{Cond}^{\mathbf{I4}}_{\mathrm{ACL}}$ | (S-Int) | (S-CA) | (S-Mon) | (S-DT) | (S-ID) | (S-RCEA) | (S-I) | (S-C4) |

**Fig. 2.** Conditions of relations $\leq$ and $R_A$ for $\mathsf{Cond}^{\mathbf{U4}}_{\mathrm{ACL}}$ , $\mathsf{Cond}^{\mathbf{IC}}_{\mathrm{ACL}}$ and $\mathsf{Cond}^{\mathbf{I4}}_{\mathrm{ACL}}$ .

It is worth noticing that (S-UNIT) and (S-Int), together, imply the condition (S-I). Indeed, consider $tR_Bs$ and $sR_Au$. By (S-UNIT), from $tR_Bs$ we obtain that $t \leq s$. By (S-Int), it immediately follows that $tR_Au$, and we are done.

## 4 Soundness and Completeness of the Axiomatizations with respect to the Semantics

In this section we prove that the axiomatizations of the four conditional access control logics introduced above are sound and complete with respect to their semantics as defined in Section 3. As in the previous sections, we first consider the logic $\mathsf{Cond}^{\mathbf{UC}}_{\mathrm{ACL}}$ . The completeness proof we present is based on the proof of completeness for the Kripke semantics of intuitionistic logic in [31] and extends it to deal with the modality **says** in the language and, more precisely, with the interplay between the relation $\leq$ and the accessibility relations $R_A$ associated with **says** .

**Definition 4 (Consistency).** *Let $\Gamma$ be a set of formulas. $\Gamma$ is consistent iff $\Gamma \not\vdash \bot$. If $\Gamma$ has an infinite number of formulas, we say that $\Gamma$ is consistent iff there are no finite $\Gamma_0 \subset \Gamma$ such that $\Gamma_0 \vdash \bot$.*

**Definition 5 (Saturation).** *Let $\Gamma$ be a set of formulas, we say that $\Gamma$ is saturated iff 1. $\Gamma$ is consistent (Definition 4); 2. if $\Gamma \vdash \varphi$, then $\varphi \in \Gamma$; 3. if $\Gamma \vdash \varphi \vee \psi$, then $\Gamma \vdash \varphi$ or $\Gamma \vdash \psi$.*

**Lemma 1 (Saturated Extensions).** *Let $\Gamma$ be a set of formulas. Suppose $\Gamma \not\vdash \varphi$, then there is a saturated set $\Gamma^*$ such that $\Gamma \subseteq \Gamma^*$ and $\Gamma^* \not\vdash \varphi$.*

*Proof.* This is proven as in [31]. We obtain $\Gamma^*$ as $\bigcup\{\Gamma^k : k \in \mathcal{N}\}$. We let $\Gamma_0 = \Gamma$, and inductively define $\Gamma^k$. Let $\{B_{0,1} \vee B_{0,2}, \ldots B_{n,1} \vee B_{n,2}, \ldots\}$ be an enumeration with infinite repetitions of all the disjunctions of the language. We define $\Gamma^{k+1}$ as follows:

- $\Gamma^{k+1} = \Gamma^k \cup \{B_{k,i}\}$ if $\Gamma^k \vdash B_{k,1} \vee B_{k,2}$, where $i$ is the least of $\{1,2\}$ such that $\Gamma^k \cup \{B_{k,i}\} \not\vdash \varphi$
- $\Gamma^k$ otherwise.

It can be easily shown that $\Gamma^*$ is saturated, that $\Gamma \subseteq \Gamma^*$ , and that $\Gamma^* \not\vdash \varphi$. □

**Definition 6 (Canonical model construction).** *We fix a language $\mathcal{L}^C \subseteq \mathcal{L}$ and we define $\mathbf{M} = (S, \leq, \{R_A\}, h)$ such that: S is the set of all saturated $\Gamma$ on the language $\mathcal{L}^C$; $\Gamma_1 \leq \Gamma_2$ iff $\Gamma_1 \subseteq \Gamma_2$; $\Gamma_1 R_A \Gamma_2$ iff $\{\alpha \mid A$ **says** $\alpha \in \Gamma_1\} \subseteq \Gamma_2$; for all $P \in ATM$, $h(P) = \{\Gamma \in S \mid P \in \Gamma\}$.*

We can prove the following Lemmas:

**Lemma 2.** *Let $\Gamma$ be a set of formulas and let $\Delta = \{\varphi : A$ **says** $\varphi \in \Gamma\}$. If $\Delta \vdash \psi$, then $\Gamma \vdash A$ **says** $\psi$.*

*Proof.* If $\Delta \vdash \psi$, by definition of $\vdash$ there must be $\{\varphi_1, \ldots, \varphi_n\} \subseteq \Delta$ such that $\vdash \varphi_1 \wedge \ldots \wedge \varphi_n \rightarrow \psi$. By (RCK) and (K), $\vdash A$ **says** $\varphi_1 \wedge \ldots \wedge A$ **says** $\varphi_n \rightarrow A$ **says** $\psi$, and from definition of $\vdash$ (and since $A$ **says** $\varphi_i \in \Gamma$ for all $i = 1, \ldots, n$) we conclude that $\Gamma \vdash A$ **says** $\psi$. □

**Lemma 3.** *For all $\Gamma \in S$ and each formula $\varphi \in \mathcal{L}$, we have that $\mathbf{M}, \Gamma \models \varphi$ iff $\varphi \in \Gamma$.*

*Proof.* By induction on the complexity of $\varphi$. In case $\varphi$ is an atomic formula, the lemma holds by definition of $h$. For $\varphi \equiv \phi \wedge \psi$ the proof is easy and left to the reader. For $\varphi \equiv \phi \vee \psi$, then $\Gamma \models \phi \vee \psi \Leftrightarrow (\Gamma \models \phi$ or $\Gamma \models \psi) \Leftrightarrow (\phi \in \Gamma$ or $\psi \in \Gamma) \Leftrightarrow \phi \vee \psi \in \Gamma$ (by the saturation of $\Gamma$). For $\varphi \equiv \phi \rightarrow \psi$, suppose $\Gamma \models \phi \rightarrow \psi$. Then for all saturated $\Gamma^{'} \supseteq \Gamma$ we have that if $\Gamma^{'} \models \phi$, then $\Gamma' \models \psi$. Assume $\Gamma \not\vdash \phi \rightarrow \psi$, then $\Gamma \cup \{\phi\} \not\vdash \psi$; let $\Gamma^{'}$ be a saturated extension of $\Gamma \cup \{\phi\}$ such that $\Gamma^{'} \not\vdash \psi$, then $\Gamma^{'} \models \phi$ but not $\Gamma^{'} \models \psi$ (induction hypothesis). This contradicts $\Gamma \models \phi \rightarrow \psi$. Hence $\Gamma \vdash \phi \rightarrow \psi$. As $\Gamma$ is saturated, by condition 2 in Definition 5, $\phi \rightarrow \psi \in \Gamma$. For the converse, let $\phi \rightarrow \psi \in \Gamma$. For a contradiction suppose $\Gamma \not\models \phi \rightarrow \psi$. Then there would be a $\Gamma'$ with $\Gamma \subseteq \Gamma'$ such that $\Gamma' \models \phi$ but $\Gamma' \not\models \psi$. Since $\Gamma \subseteq \Gamma'$, $\phi \rightarrow \psi \in \Gamma'$. Furthermore by inductive hypothesis $\phi \in \Gamma'$. Hence there are $\gamma_1 \ldots \gamma_n \in \Gamma'$ such that $\vdash \gamma_1 \wedge \ldots \wedge \gamma_n \rightarrow (\phi \rightarrow \psi)$ and $\vdash \gamma_1 \wedge \ldots \wedge \gamma_n \rightarrow \phi$. From the axiomatization (and saturation) it follows that $\psi \in \Gamma'$, which contradicts $\psi \notin \Gamma'$ deriving from $\Gamma' \not\models \psi$ by the inductive hypothesis. Therefore $\Gamma \models \phi \rightarrow \psi$. For $\varphi \equiv A$ **says** $\phi$, suppose $\Gamma \models A$ **says** $\phi$. Hence, for all $\Gamma'$ such that $\Gamma R_A \Gamma'$, $\Gamma' \models \phi$. By inductive hypothesis, $\phi \in \Gamma'$. Let $\Delta = \{\alpha : A$ **says** $\alpha \in \Gamma\}$. By construction, $\Gamma' \supseteq \Delta$. Assume, for a contradiction, that $A$ **says** $\phi \notin \Gamma$. By condition 2 in Definition 5, $\Gamma \not\vdash A$ **says** $\phi$. Then, by Lemma 2, $\Delta \not\vdash \phi$. By Lemma 1, there is a saturated extension $\Delta^*$ of $\Delta$ such that $\Delta^* \not\vdash \phi$, i.e. $\phi \notin \Delta^*$. By definition of $R_A$, $\Gamma R_A \Delta^*$. This contradicts the fact that, for all $\Gamma'$ such that $\Gamma R_A \Gamma'$, $\phi \in \Gamma'$. The converse can be easily shown. □

**Lemma 4.** *Let $\mathbf{M}$ be the canonical model as defined in Definition 6. $\mathbf{M}$ satisfies the conditions* (S-Int), (S-UNIT), (S-C), (S-CA), (S-Mon), (S-DT), (S-ID), *and* (S-RCEA).

*Proof.* We consider each property:

(S-Int) Let $\Gamma \leq \Gamma'$ and $\Gamma' R_A \Gamma''$. Consider any $\phi$ s.t. $A$ **says** $\phi \in \Gamma$. By definition of $\leq$, $A$ **says** $\phi \in \Gamma'$, hence by $\Gamma R_A \Gamma''$, $\phi \in \Gamma''$. By definition of $R_A$ it follows that $\Gamma R_A \Gamma''$.

(S-UNIT) Let $\Gamma R_A \Gamma'$. We want to show that $\Gamma \leq \Gamma'$. Let $\alpha \in \Gamma$. By (UNIT), $\alpha \rightarrow A$ **says** $\alpha \in \Gamma$, hence (by saturation of $\Gamma$) $A$ **says** $\alpha \in \Gamma$. Hence, by construction of the canonical model, $\alpha \in \Gamma'$. Therefore, $\Gamma \leq \Gamma'$.

(S-C) We have to prove that if $\Gamma R_A \Gamma'$, and $\Gamma' \leq \Gamma''$, then $\Gamma'' R_A \Gamma''$. By (C) we know that for all $\phi$, $A$ **says** $(A$ **says** $\phi \rightarrow \phi) \in \Gamma$, hence $A$ **says** $\phi \rightarrow \phi \in \Gamma'$, and also $A$ **says** $\phi \rightarrow \phi \in \Gamma''$ (by definition of $\leq$). From this it follows that for all $A$ **says** $\phi \in \Gamma''$, by saturation of $\Gamma''$, $\phi \in \Gamma''$. By definition of $R_A$ we conclude that $\Gamma'' R_A \Gamma''$.

(S-CA) In order to show that $R_{A \vee B} = R_A \cup R_B$ we have to consider two directions. 1. Let $\Gamma R_A \Gamma'$. For all $C : A \vee B$ **says** $C \in \Gamma$, by (CA-conv) also $A$ **says** $C \in \Gamma$, hence $C \in \Gamma'$. We conclude that $\Gamma R_{A \vee B} \Gamma'$. The same holds if $\Gamma R_B \Gamma'$. Hence, $R_A \cup R_B \subseteq R_{A \vee B}$. 2. Let $\Gamma R_{A \vee B} \Gamma'$. Suppose that not $\Gamma R_A \Gamma'$, i.e. there is $C$ s.t. $A$ **says** $C \in \Gamma$ and $C \notin \Gamma'$. We want to show that in this case $\Gamma R_B \Gamma'$. Consider any $D$ s.t. $B$ **says** $D \in \Gamma$. By (RCK), and by saturation of $\Gamma$, $A$ **says** $C \vee D \in \Gamma$ and $B$ **says** $C \vee D \in \Gamma$. By (CA) $A \vee B$ **says** $C \vee D$. It follows that $C \vee D \in \Gamma'$, and since $C \notin \Gamma'$, $D \in \Gamma'$. We have shown that if not $\Gamma R_A \Gamma'$, then $\Gamma R_B \Gamma'$. We can reason symmetrically in case not $\Gamma R_B \Gamma'$. Hence, $R_{A \vee B} \subseteq R_A \cup R_B$.

(S-Mon) Let $\Gamma R_{A \wedge B} \Gamma'$. Consider $\phi$ s.t. $A$ **says** $\phi \in \Gamma$. By (Mon) it follows that $A \wedge B$ **says** $\phi \in \Gamma$, hence $\phi \in \Gamma'$ and, by definition of $R_A$, $\Gamma R_A \Gamma'$. The same holds for $R_B$.

(S-DT) We have to show that if $\Gamma R_A \Gamma'$, $\Gamma' \leq \Gamma''$, and $\Gamma'' \in [|B|]$, then $\Gamma R_{A \wedge B} \Gamma''$, i.e. $\{\phi$: $A \wedge B$ **says** $\phi \in \Gamma\} \subseteq \Gamma''$. Consider $\phi$ such that $A \wedge B$ **says** $\phi \in \Gamma$. Then, by (DT), $A$ **says** $(B \rightarrow \phi) \in \Gamma$, hence by definition of $R_A$, $B \rightarrow \phi \in \Gamma'$, and by definition of $\leq$, $B \rightarrow \phi \in \Gamma''$. Furthermore, from $\Gamma'' \in [|B|]$, $B \in \Gamma''$ by Lemma 3. By saturation of $\Gamma''$, we conclude that $\phi \in \Gamma''$.

(S-ID) Let $\Gamma R_A \Gamma'$. By (ID) $A$ **says** $A \in \Gamma$ and, by definition of $R_A$, $A \in \Gamma'$ and, by Lemma 3, $\Gamma' \in [[A]]$.

(S-RCEA) If $[[A]] = [[B]]$, then $\vdash A \leftrightarrow B$, otherwise by Lemma 1 there would be $\Gamma \in S$ such that $A \leftrightarrow B \notin \Gamma$. In this case, by Lemma 3 $\Gamma \not\models A \leftrightarrow B$ hence there would be a $\Gamma'$ s.t. $\Gamma \leq \Gamma'$ and $\Gamma' \models A$ but $\Gamma' \not\models B$ (or viceversa). This contradicts the hypothesis that $[[A]] = [[B]]$. Furthermore, from $\vdash A \leftrightarrow B$, by (RCEA) we conclude that $A$ **says** $\phi \leftrightarrow B$ **says** $\phi \in \Gamma$ for each $\Gamma \in S$. Therefore, for all $\Gamma, \Gamma' \in S$, $\Gamma R_A \Gamma'$ iff $\Gamma R_B \Gamma'$, and hence $R_A = R_B$. □

By the above lemmas, we can conclude that the axiomatization of the logic $\mathsf{Cond}^{\mathbf{UC}}_{\mathrm{ACL}}$ given in Section 2 is complete with respect to the semantics in Definition 2:

**Theorem 4 (Soundness and Completeness of $\mathsf{Cond}^{\mathbf{UC}}_{\mathbf{ACL}}$ ).** *Given a formula $\varphi \in \mathcal{L}$, $\models \varphi$ iff $\vdash \varphi$.*

*Proof.* Soundness is straightforward. Concerning the completeness, for a contradiction, suppose $\not\vdash \varphi$. Then by Lemma 1 there is a saturated set $\Gamma^*$ such that $\Gamma^* \not\vdash \varphi$, hence $\varphi \notin \Gamma^*$. By Definition 6 and Lemmas 3 and 4, we conclude that there is a (canonical) model $\mathbf{M} = (S, \leq, \{R_A\}, h)$, made on the language of $\varphi$, with $\Gamma^* \in S$, such that $\mathbf{M}, \Gamma^* \not\models \varphi$. It follows that $\varphi$ is not logically valid, i.e. $\not\models \varphi$. □

We can also show that soundness and completeness apply to the logics $\mathsf{Cond}_{\mathrm{ACL}}^{\mathbf{U4}}$, $\mathsf{Cond}_{\mathrm{ACL}}^{\mathbf{IC}}$ and $\mathsf{Cond}_{\mathrm{ACL}}^{\mathbf{I4}}$, obtained respectively when replacing (C) with (C4) or (UNIT) with (I) or both in $\mathsf{Cond}_{\mathrm{ACL}}^{\mathbf{UC}}$.

**Theorem 5 (Soundness and Completeness of $\mathsf{Cond}_{\mathbf{ACL}}^{\mathbf{IC}}$).** *The axiomatization of the logic* $\mathsf{Cond}_{\mathrm{ACL}}^{\mathbf{IC}}$*, obtained by replacing* (UNIT) *with* (I)*, is sound and complete with respect to the semantics of Definition 2 in which* (S-UNIT) *is replaced with* (S-I) *of Definition 3.*

*Proof.* Soundness is straightforward. For completeness, we reason as done above. We prove that if the logic contains (I) instead of (UNIT) then it satisfies (S-I).

(S-I) Let $\Gamma R_B \Gamma'$ and $\Gamma' R_A \Gamma''$. Consider $\phi$ s.t. $A$ **says** $\phi \in \Gamma$. By (I) $B$ **says** $(A$ **says** $\phi) \in \Gamma$, hence $A$ **says** $\phi \in \Gamma'$ and $\phi \in \Gamma''$. We conclude that $\Gamma R_A \Gamma''$. □

**Theorem 6 (Soundness and Completeness of $\mathsf{Cond}_{\mathbf{ACL}}^{\mathbf{U4}}$).** *The axiomatization of the logic* $\mathsf{Cond}_{\mathrm{ACL}}^{\mathbf{U4}}$*, obtained by replacing* (C) *with* (C4)*, is sound and complete with respect to the semantics of Definition 2 in which* (S-C) *is replaced with* (S-C4) *of Definition 3.*

*Proof.* Soundness is straightforward. For completeness, we reason as done above. We prove that if the logic contains (C4) instead of (C) the logic satisfies (S-C4).

(S-C4) Let $\Gamma R_A \Gamma'$. Consider $\Delta = \{\phi : A$ **says** $\phi \in \Gamma\}$. Clearly, by definition of $R_A$, $\Delta \subseteq \Gamma'$. Consider now the saturation $\Delta^*$ of $\Delta$ obtained as follows. Consider the disjunctive normal form corresponding to $\Delta$: $D_1 \vee \ldots \vee D_n$. Since $\Delta$ is consistent there must be one $D_i$ such that $\Delta \not\vdash \neg D_i$. Furthermore, there must also exist one such $D_i$ in which any formula $A$ **says** $\phi$ positively occurs only if $\phi \in \Gamma'$. For a contradiction suppose that for each $D_i$ consistent with $\Delta$ there was an occurrence of $A$ **says** $\phi$ with $\phi \notin \Gamma'$. Then there would be $A$ **says** $\phi_1 \ldots A$ **says** $\phi_j$ with $\phi_1 \ldots \phi_j \notin \Gamma'$ such that $\Delta \vdash A$ **says** $\phi_1 \vee \ldots \vee A$ **says** $\phi_j$. But in this case also $\Delta \vdash A$ **says** $(\phi_1 \vee \ldots \vee \phi_n)$, and by Lemma 2, $\Gamma \vdash A$ **says** $(A$ **says** $(\phi_1 \vee \ldots \vee \phi_n))$. By (C4) also $\Gamma \vdash A$ **says** $(\phi_1 \vee \ldots \vee \phi_n)$, and hence $(\phi_1 \vee \ldots \vee \phi_n) \in \Delta \subseteq \Gamma'$, which contradicts that $\Gamma'$ is saturated but none of $\phi_1 \ldots \phi_n$ belongs to $\Gamma'$. From this contradiction we conclude that there must be a $D_i$ consistent with $\Delta$ and such that for any positive occurrence of $A$ **says** $\phi$, $\phi \in \Gamma'$. We saturate $\Delta$ with this disjunct, obtaining $\Delta^*$. It can be easily shown that $\Delta^*$ is saturated, and that $\Gamma R_A \Delta^*$ and $\Delta^* R_A \Gamma'$. □

**Theorem 7 (Soundness and Completeness of $\mathsf{Cond}_{\mathbf{ACL}}^{\mathbf{I4}}$).** *The axiomatization of the logic* $\mathsf{Cond}_{\mathrm{ACL}}^{\mathbf{I4}}$*, obtained by replacing* (UNIT) *with* (I) *and* (C) *with* (C4)*, respectively, is sound and complete with respect to the semantics of Definition 2 in which* (S-UNIT) *is replaced with* (S-I) *and* (S-C) *is replaced with* (S-C4).

## 5 A sequent calculus for Conditional Access Control Logics

In this section we present a cut-free sequent calculus for the four conditional logics for access control we propose. Our calculus is called $\mathcal{S}_{\mathsf{Cond}_{\mathrm{ACL}}}$ and it makes use of labels to represent possible worlds, following the line of SeqS, a sequent calculus for standard conditional logics introduced in [26]. In particular, the calculus we propose is formulated following the methods developed in [24] to obtain height-preserving admissibility of weakening and contraction, admissibility of cut, and decidability for modal labelled calculi. In the following, by $\mathcal{S}_{\mathsf{Cond}_{\mathrm{ACL}}}$ we refer to the calculus for any of the four logics under consideration. For the logic $\mathsf{Cond}^{\mathbf{UC}}_{\mathrm{ACL}}$, we also show that we can control the application of some crucial rules, obtaining a terminating calculus $\widehat{\mathcal{S}_{\mathsf{Cond}^{\mathbf{UC}}_{\mathrm{ACL}}}}$. This calculus describes a decision procedure for $\mathsf{Cond}^{\mathbf{UC}}_{\mathrm{ACL}}$, and allows us to conclude that provability is decidable in $O(n^4 logn)$ space.

In addition to the language $\mathcal{L}$ of the logic $\mathsf{Cond}^{\mathbf{UC}}_{\mathrm{ACL}}$, we consider a denumerable alphabet of labels $\mathcal{X}$, whose elements are denoted by $x, y, z, \ldots$. Moreover, in order to obtain a terminating calculus, we define the set $\mathcal{L}_{\mathbf{P}} \subseteq \mathcal{L}$ of principals involved in the computation. Given a set of policies $\Gamma$ and a request $\varphi$ of compliance of a principal $A$ (i.e. we want to verify whether $\Gamma, A$ **says** $\varphi \models \varphi$), we assume that the set $\mathcal{L}_{\mathbf{P}}$ contains at least $A$ and all principals $B$ such that, for some $\phi$, $B$ **says** $\phi$ appears in $\Gamma$.

The calculus $\mathcal{S}_{\mathsf{Cond}_{\mathrm{ACL}}}$ manipulates three types of labelled formulas:

1. *world formulas*, denoted by $x : \alpha$, where $x \in \mathcal{X}$ and $\alpha \in \mathcal{L}$, used to represent that the formula $\alpha$ holds in a world $x$;
2. *transition formulas*, denoted by $x \xrightarrow{A} y$, representing that $xR_Ay$;
3. *order formulas* of the form $y \geq x$ representing the preorder relation $\leq$.

A *sequent* is a pair $\langle \Gamma, \Delta \rangle$, usually denoted with $\Gamma \vdash \Delta$, where $\Gamma$ and $\Delta$ are multisets of labelled formulas. The intuitive meaning of a sequent $\Gamma \vdash \Delta$ is: every model that satisfies all labelled formulas of $\Gamma$ in the respective worlds (specified by the labels) satisfies at least one of the labelled formulas of $\Delta$ (in those worlds). This is made precise by the notion of *validity* of a sequent given in the next definition:

**Definition 7 (Sequent validity).** *Given a model $\mathcal{M} = (S, \leq, \{R_A\}, h)$ for $\mathcal{L}$, and a label alphabet $\mathcal{X}$, we consider a* mapping $I : \mathcal{X} \rightarrow S$. *Let $F$ be a labelled formula, we define $\mathcal{M} \models_I F$ as follows:*

- *$\mathcal{M} \models_I x : \alpha$ iff $\mathcal{M}, I(x) \models \alpha$;*
- *$\mathcal{M} \models_I x \xrightarrow{A} y$ iff $I(x) R_A I(y)$;*
- *$\mathcal{M} \models_I y \geq x$ iff $I(x) \leq I(y)$.*

*We say that $\Gamma \vdash \Delta$ is* valid *in $\mathcal{M}$ if, for every mapping $I : \mathcal{X} \rightarrow S$, if $\mathcal{M} \models_I F$ for every $F \in \Gamma$, then $\mathcal{M} \models_I G$ for some $G \in \Delta$. We say that $\Gamma \vdash \Delta$ is valid in $\mathsf{Cond}^{\mathbf{UC}}_{\mathrm{ACL}}$ if it is valid in every $\mathcal{M}$.*

In Figure 3 we present the basic rules of the calculi $\mathcal{S}_{\mathsf{Cond}_{\mathrm{ACL}}}$, common to all the logics under considerations. In Figure 4 we present the specific rules to adopt in order to

## Basic Rules

$(AX)\ \Gamma, F \vdash \Delta, F \qquad (AX_{\perp})\ \Gamma, x : \perp \vdash \Delta \qquad (AX_{\geq})\ \Gamma \vdash \Delta, x \geq x$

$F$ either $x : P, P \in ATM$ or $y \geq x$

$$\frac{\Gamma, x : P \vdash \Delta, y \geq x \qquad \Gamma, x : P, y : P \vdash \Delta}{\Gamma, x : P \vdash \Delta}(ATM)\ P \in ATM \qquad \frac{\Gamma, y \geq x, y \xrightarrow{A} z, x \xrightarrow{A} z \vdash \Delta}{\Gamma, y \geq x, y \xrightarrow{A} z \vdash \Delta}(INT)$$

$$\frac{\Gamma \vdash \Delta, x : \alpha \qquad \Gamma \vdash \Delta, x : \beta}{\Gamma \vdash \Delta, x : \alpha \wedge \beta}(\wedge R) \qquad \frac{\Gamma, x : \alpha, x : \beta \vdash \Delta}{\Gamma, x : \alpha \wedge \beta \vdash \Delta}(\wedge L)$$

$$\frac{\Gamma \vdash \Delta, x : \alpha, x : \beta}{\Gamma \vdash \Delta, x : \alpha \vee \beta}(\vee R) \qquad \frac{\Gamma, x : \alpha \vdash \Delta \qquad \Gamma, x : \beta \vdash \Delta}{\Gamma, x : \alpha \vee \beta \vdash \Delta}(\vee L)$$

$$\frac{\Gamma, z \geq x, z \geq y, y \geq x \vdash \Delta}{\Gamma, z \geq y, y \geq x \vdash \Delta}(TR) \qquad \frac{\Gamma, y \geq x, y : \alpha \vdash \Delta, y : \beta}{\Gamma \vdash \Delta, x : \alpha \rightarrow \beta}(\rightarrow R)\ y \text{ new}$$

$$\frac{\Gamma, x : \alpha \rightarrow \beta \vdash \Delta, y \geq x \qquad \Gamma, x : \alpha \rightarrow \beta \vdash \Delta, y : \alpha \qquad \Gamma, x : \alpha \rightarrow \beta, y : \beta \vdash \Delta}{\Gamma, x : \alpha \rightarrow \beta \vdash \Delta}(\rightarrow L)$$

$$\frac{\Gamma, x \xrightarrow{A} y \vdash \Delta, y : \alpha}{\Gamma \vdash \Delta, x : A \textbf{ says } \alpha}(\textbf{ says } R)\ y \text{ new} \qquad \frac{\Gamma, x : A \textbf{ says } \alpha \vdash \Delta, x \xrightarrow{A} y \qquad \Gamma, x : A \textbf{ says } \alpha, y : \alpha \vdash \Delta}{\Gamma, x : A \textbf{ says } \alpha \vdash \Delta}(\textbf{ says } L)$$

$$\frac{u : A \vdash u : B \qquad u : B \vdash u : A}{\Gamma, x \xrightarrow{A} y \vdash \Delta, x \xrightarrow{B} y}(EQ)\ u \text{ new} \qquad \frac{\Gamma \vdash \Delta, x \xrightarrow{A \wedge B} y \qquad \Gamma, x \xrightarrow{A} y, x \xrightarrow{B} y \vdash \Delta}{\Gamma \vdash \Delta}(MON)\ A \wedge B \in \mathcal{L}_P$$

$$\frac{\Gamma, z \geq y, x \xrightarrow{A} y \vdash \Delta, z : B \qquad \Gamma, z \geq y, x \xrightarrow{A} y, x \xrightarrow{A \wedge B} z \vdash \Delta}{\Gamma, z \geq y, x \xrightarrow{A} y \vdash \Delta}(DT)\ A \wedge B \in \mathcal{L}_P \qquad \frac{\Gamma, x \xrightarrow{A} y, y : A \vdash \Delta}{\Gamma, x \xrightarrow{A} y \vdash \Delta}(ID)$$

$$\frac{\Gamma \vdash \Delta, x \xrightarrow{A \vee B} y \qquad \Gamma, x \xrightarrow{A} y \vdash \Delta \qquad \Gamma, x \xrightarrow{B} y \vdash \Delta}{\Gamma \vdash \Delta}(CA)\ A \vee B \in \mathcal{L}_P \qquad \frac{\Gamma, x \xrightarrow{A \vee B} y, x \xrightarrow{A} y \vdash \Delta}{\Gamma, x \xrightarrow{A} y \vdash \Delta}(CA - conv)\ A \vee B \in \mathcal{L}_P$$

**Fig. 3.** Basic rules of the sequent calculus $\mathcal{S}_{\mathsf{Cond}_{\mathrm{ACL}}}$ .

$$\frac{\Gamma, z \geq y, x \xrightarrow{A} y, z \xrightarrow{A} z \vdash \Delta}{\Gamma, z \geq y, x \xrightarrow{A} y \vdash \Delta}(C) \qquad \frac{\Gamma, x \xrightarrow{A} y, x \xrightarrow{A} z, z \xrightarrow{A} y \vdash \Delta}{\Gamma, x \xrightarrow{A} y \vdash \Delta}(C4)\ z \text{ new}$$

$$\frac{\Gamma, y \geq x, x \xrightarrow{A} y \vdash \Delta}{\Gamma, x \xrightarrow{A} y \vdash \Delta}(Unit) \qquad \frac{\Gamma, x \xrightarrow{B} y, y \xrightarrow{A} z, x \xrightarrow{A} z \vdash \Delta}{\Gamma, x \xrightarrow{B} y, y \xrightarrow{A} z \vdash \Delta}(I)$$

**Fig. 4.** Additional rules for $\mathsf{Cond}_{\mathrm{ACL}}^{\mathbf{UC}}$ , $\mathsf{Cond}_{\mathrm{ACL}}^{\mathbf{U4}}$ , $\mathsf{Cond}_{\mathrm{ACL}}^{\mathbf{IC}}$ , $\mathsf{Cond}_{\mathrm{ACL}}^{\mathbf{I4}}$ .

| Logic | Calculus | Rules |
|---|---|---|
| $\mathsf{Cond}^{\mathbf{UC}}_{\mathrm{ACL}}$ | $\mathcal{S}_{\mathsf{Cond}^{\mathbf{UC}}_{\mathrm{ACL}}}$ | $\textsc{Basic Rules}\ +(Unit)\ +\ (C)$ |
| $\mathsf{Cond}^{\mathbf{U4}}_{\mathrm{ACL}}$ | $\mathcal{S}_{\mathsf{Cond}^{\mathbf{U4}}_{\mathrm{ACL}}}$ | $\textsc{Basic Rules}\ +(Unit)\ +\ (C4)$ |
| $\mathsf{Cond}^{\mathbf{IC}}_{\mathrm{ACL}}$ | $\mathcal{S}_{\mathsf{Cond}^{\mathbf{IC}}_{\mathrm{ACL}}}$ | $\textsc{Basic Rules}\ +(I)\ +\ (C)$ |
| $\mathsf{Cond}^{\mathbf{I4}}_{\mathrm{ACL}}$ | $\mathcal{S}_{\mathsf{Cond}^{\mathbf{I4}}_{\mathrm{ACL}}}$ | $\textsc{Basic Rules}\ +(I)\ +\ (C4)$ |

**Fig. 5.** Calculi and rules for the constructive conditional access control logics.

deal with one of the presented conditional access control logics, namely $\mathsf{Cond}^{\mathbf{UC}}_{\mathrm{ACL}}$ , $\mathsf{Cond}^{\mathbf{U4}}_{\mathrm{ACL}}$ , $\mathsf{Cond}^{\mathbf{IC}}_{\mathrm{ACL}}$ , or $\mathsf{Cond}^{\mathbf{I4}}_{\mathrm{ACL}}$ , following the schema of Figure 5.

As usual, we say that a sequent $\Gamma \vdash \Delta$ is *derivable* in $\mathcal{S}_{\mathsf{Cond}_{\mathrm{ACL}}}$ if it admits a *derivation*. A derivation is a tree whose nodes are sequents. A branch is a sequence of nodes $\Gamma_1 \vdash \Delta_1, \Gamma_2 \vdash \Delta_2, \ldots, \Gamma_n \vdash \Delta_n, \ldots$ Each node $\Gamma_i \vdash \Delta_i$ is obtained from its immediate successor $\Gamma_{i-1} \vdash \Delta_{i-1}$ by applying *backward* a rule of $\mathcal{S}_{\mathsf{Cond}_{\mathrm{ACL}}}$ , having $\Gamma_{i-1} \vdash \Delta_{i-1}$ as the conclusion and $\Gamma_i \vdash \Delta_i$ as one of its premises. A branch is closed if one of its nodes is an instance of axioms, namely $(AX)$, $(AX_{\geq})$, and $(AX_{\bot})$, otherwise it is open. We say that a tree is closed if all its branches are closed. A sequent $\Gamma \vdash \Delta$ has a derivation in $\mathcal{S}_{\mathsf{Cond}_{\mathrm{ACL}}}$ if there is a closed tree having $\Gamma \vdash \Delta$ as a root.

The axioms represent valid sequents. For instance, $(AX)$ is used to close a branch with a sequent in which a formula $F$ belongs to both its left hand side and its right hand side: $F$ is either a formula $x : P$, where $P$ is an atom, or a formula $y \geq x$. Such a sequent is obviously valid : given any model satisfying all the formulas in the left hand side, then also the formula $F$, then there is at least one formula in the righ-hand side holding in such a model, the formula $F$ itself. Similarly for the other axioms. The rule $(ATM)$ is used to support the condition 1. in Definition 2, namely, given a model $\mathcal{M}$, a world $t$ and an atomic formula $P$ not being a principal, we have that $\mathcal{M}, t \models P$ if and only if, for all $s$ such that $t \leq s$, we have that $s \in h(P)$. Given a sequent containing $x : P$ in the left hand side, the rule (i) checks whether the premise in which $y \geq x$ is added to the right hand side of the sequent is valid: intuitively, this corresponds to finding a world (represented by $y$) which is "greater" than the one represented by $x$; (ii) introduces $y : P$ in the other premise, in order to impose that the atom $P$ also holds in the world represented by $y$ such that $y \geq x$. The rule $(INT)$ supports the condition (S-Int) in Definition 2: if a sequent contains the formulas $y \geq x$ and $y \xrightarrow{A} z$ in its left hand side, then the rule introduces also the transition formula $x \xrightarrow{A} z$, and then checks whether the resulting premise is derivable. The rule $(TR)$ takes care of the transitivity of the relation $\leq$ in an obvious way: if both $z \geq y$ and $y \geq x$ belong to the left hand side of a sequent, then also the relation $z \geq x$ is added to the left hand side of the premise that the calculus tries to derive. The rule $(Unit)$ is used to support the condition (S-UNIT) in Definition 2: if the sequent under consideration contains a transition formula $x \xrightarrow{A} y$ in its left hand side, then the rule introduces also the relation $y \geq x$. Similarly for the other rules related to the other semantic conditions. Some of them are related to the conditions introduced to support boolean principals. As an example, the rule $(MON)$ is used to support the condition (S-Mon) in Definition 2. Intuitively, given a sequent

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\dots, y \geq x \vdash y : P, y \geq x}\,(AX) \qquad \dfrac{}{\dots, x : P, y : P \vdash y : P}\,(AX)}{y \geq x, x \geq u, x : P, x \xrightarrow{A} y \vdash y : P}\,(ATM)}{x \geq u, x : P, x \xrightarrow{A} y \vdash y : P}\,(Unit)}{x \geq u, x : P \vdash x : A \textbf{ says } P}\,(\textbf{ says } R)}{\vdash u : P \rightarrow (A \textbf{ says } P)}\,(\rightarrow R)$$

**Fig. 6.** A derivation in $\mathcal{S}_{\mathsf{Cond}_{\mathrm{ACL}}}$ for an instance of the axiom (UNIT).

$\Gamma \vdash \Delta$, the rule works as follows: the left premise checks whether $\Gamma \vdash \Delta, x \xrightarrow{A \wedge B} y$ is a valid sequent, trying to check whether there is a world (represented by the label $y$) reachable from the world represented by $x$ given the boolean principal $A \wedge B$; the right premise adds tra transitions $x \xrightarrow{A} y$ and $x \xrightarrow{B} y$ according to the condition (S-Mon). The side condition is introduced in order to ensure that $A \wedge B$ belongs to the set of available principals. Similarly for the other rules supporting the other conditions of boolean principals. The rule $(EQ)$ is used in order to support the rule (RCEA), roughly speaking the rule has to ensure that, if $A$ and $B$ are equivalent, i.e. they are true in the same worlds, then, given a world represented by $x$, the selection function selects the same worlds for $x$ (represented by $y$) for both $A$ and $B$. To this aim, if a sequent $\Gamma, x \xrightarrow{A} y \vdash \Delta, x \xrightarrow{B} y$ has to be proved, then the $(EQ)$ rule introduces a branch in the backward derivation, trying to find a proof for both sequents $u : A \vdash u : B$ and $u : B \vdash u : A$. The restrictions on the rules $(\rightarrow R)$, ( **says** $R)$, and $(EQ)$ are necessary to preserve the soundness of the calculus.

As an example, in Figure 6 we show a derivation in $\mathcal{S}_{\mathsf{Cond}_{\mathrm{ACL}}}$ of an instance of the axiom (UNIT). Given $P \in ATM$, in order to show that the formula $P \rightarrow (A \textbf{ says } P)$ is valid, we build a derivation in $\mathcal{S}_{\mathsf{Cond}_{\mathrm{ACL}}}$ for the sequent $\vdash u : P \rightarrow (A \textbf{ says } P)$.

The calculus $\mathcal{S}_{\mathsf{Cond}_{\mathrm{ACL}}}$ is sound and complete with respect to the semantics. In order to prove it, we need some basic structural properties.

### 5.1 Basic Structural properties of $\mathcal{S}_{\mathsf{Cond}_{\mathrm{ACL}}}$

First of all, we define the complexity of a labelled formula:

**Definition 8 (Complexity of a labelled formula cp(F)).** *We define the complexity of a labelled formula $F$ as follows:*

- $cp(x : \gamma) = 2 * \mid \gamma \mid$
- $cp(x : \bot) = 2$
- $cp(y \geq x) = 2$
- $cp(x \xrightarrow{A} y) = 2 * \mid A \mid + 1$

*where $\mid F \mid$ is the number of symbols occurring in the string representing $F$.*

Now we can introduce some basic structural properties holding in $\mathcal{S}^{\mathsf{Cond}_{\mathrm{ACL}}}$. First, we show that *weakening* and *label substitution* are height preserving admissible in $\mathcal{S}^{\mathsf{Cond}_{\mathrm{ACL}}}$. As usual, the height of a derivation corresponds to the height of the tree representing the derivation itself.

**Lemma 5 (Height-preserving admissibility of weakening).** *If $\Gamma \vdash \Delta$ has a derivation of height $h$, then $\Gamma \vdash \Delta, F$ and $\Gamma, F \vdash \Delta$ have a derivation of height $h' \leq h$.*

*Proof.* By induction on the height of the derivation of $\Gamma \vdash \Delta$. The base case is straightforward: if $\Gamma \vdash \Delta$ is an instance of an axiom, so are $\Gamma \vdash \Delta, F$ and $\Gamma, F \vdash \Delta$. For the inductive step, we have to consider all possibile rules applied to $\Gamma \vdash \Delta$ in a backward proof search. We distinguish two subcases:

- the derivation of $\Gamma \vdash \Delta$ is ended by an application of $(EQ)$ as follows:

$$\frac{u : A \vdash u : B \qquad\qquad u : B \vdash u : A}{\Gamma', x \xrightarrow{A} y \vdash \Delta', x \xrightarrow{B} y}\ (EQ)$$

  All formulas different from the transition formulas involved in the rule application are side formulas in $(EQ)$, therefore we can conclude as follows:

$$\frac{u : A \vdash u : B \qquad\qquad u : B \vdash u : A}{\Gamma', x \xrightarrow{A} y, F \vdash \Delta', x \xrightarrow{B} y}\ (EQ)$$

  and similarly to prove that also $\Gamma', x \xrightarrow{A} y \vdash \Delta', x \xrightarrow{B} y, F$ is derivable;
- the derivation is ended by the application of a rule which is different from $(EQ)$. As an example, we present the case of $(DT)$, the other ones are similar and left to the reader:

$$\frac{(1)\ \Gamma', z \geq y, x \xrightarrow{A} y \vdash \Delta, z : B \qquad (2)\ \Gamma', z \geq y, x \xrightarrow{A} y, x \xrightarrow{A \wedge B} y \vdash \Delta}{\Gamma', z \geq y, x \xrightarrow{A} y \vdash \Delta}\ (DT)$$

  We can apply the inductive hypothesis on the two premises, obtaining derivations for $(1')$ $\Gamma', z \geq y, x \xrightarrow{A} y, F \vdash \Delta, z : B$, $(1'')$ $\Gamma', z \geq y, x \xrightarrow{A} y \vdash \Delta, z : B, F$, $(2')$ $\Gamma', z \geq y, x \xrightarrow{A} y, x \xrightarrow{A \wedge B} y, F \vdash \Delta$, and $(2'')$ $\Gamma', z \geq y, x \xrightarrow{A} y, x \xrightarrow{A \wedge B} y \vdash \Delta, F$. We obtain a derivation of $\Gamma', z \geq y, x \xrightarrow{A} y, F \vdash \Delta$ by an application of $(DT)$ to $(1')$ and $(2')$, as well as a derivation of $\Gamma', z \geq y, x \xrightarrow{A} y \vdash \Delta, F$ by applying $(DT)$ to $(1'')$ and $(2'')$. □

**Lemma 6 (Height-preserving label substitution).** *If a sequent $\Gamma \vdash \Delta$ has a derivation of height $h$, then $\Gamma[x/y] \vdash \Delta[x/y]$ has a derivation of height $h' \leq h$, where $\Gamma[x/y] \vdash \Delta[x/y]$ is the sequent obtained from $\Gamma \vdash \Delta$ by replacing all occurrences of the label $x$ by the label $y$.*

*Proof.* By induction on the height of $\Gamma \vdash \Delta$. The base case is straightforward: if $\Gamma \vdash \Delta$ is an axiom, it is still an axiom if we replace each $x$ with $y$. For the inductive step, we only present the most interesting case of $(\textbf{ says } R)$, the other cases are easy and left to the reader. Consider the following derivation:

$$\dfrac{(i)\ \Gamma, x \xrightarrow{A} y \vdash \Delta', y : \gamma}{\Gamma \vdash \Delta', x : A \textbf{ says } \gamma}\ (\textbf{ says } R)$$

In order to obtain a derivation (of at most the same height) of $\Gamma[x/y] \vdash \Delta'[x/y], y : A \textbf{ says } \gamma$ we proceed as follows. First, we apply the inductive hypothesis to $(i)$ by replacing all occurrences of $y$ with $z$, with $z$ not occurring in $\Gamma$ and $\Delta'$. Notice that, by the condition on the application of $(\textbf{ says } R)$, $y$ is new in $(i)$, that is to say $y$ does not occur in $\Gamma$ and $\Delta'$. It follows that we have a derivation of $(ii)\ \Gamma, x \xrightarrow{A} z \vdash \Delta', z : \gamma$, whose height is no greater than the height of $(i)$. We can further apply the inductive hypothesis on $(ii)$ by replacing all occurrences of $x$ with $y$, obtaining a derivation of no greater height than $(ii)$ (then, than $(i)$) of $\Gamma[x/y], y \xrightarrow{A} z \vdash \Delta'[x/y], z : \gamma$, from which we conclude by an application of $(\textbf{ says } R)$. □

We can also show that all the rules of $\mathcal{S}^{\mathsf{Cond}_{\mathrm{ACL}}}$, with the exception of $(EQ)$, are height-preserving invertible.

**Lemma 7 (Height-preserving invertibility of rules).** *Let $\Gamma \vdash \Delta$ be an instance of the conclusion of a rule R of $\mathcal{S}^{\mathsf{Cond}_{\mathrm{ACL}}}$, with R different from $(EQ)$. If $\Gamma \vdash \Delta$ is derivable, then the premise(s) of R is (are) derivable with a derivation of (at most) the same height.*

*Proof.* We have to consider each rule of the calculus. We distinguish between:

- rules $(ATM)$, $(INT)$, $(\rightarrow L)$, $(\textbf{ says } L)$, $(MON)$, $(DT)$, $(ID)$, $(CA)$, $(CA - conv)$, $(C)$, $(C4)$, $(Unit)$, and $(I)$: in these rules, the premises contain all formulas of the respective conclusions. Therefore, we conclude that we have a proof (of no greater height) of the premises since weakening is height-preserving admissible (Lemma 5);
- all other rules, not copying their principal formulas in the premises. For each rule, we proceed by induction on the height of the derivation of $\Gamma \vdash \Delta$. We only present the most interesting case of $(\rightarrow R)$. The other cases are easier and left to the reader. For the base case, suppose that $\Gamma \vdash \Delta', x : \alpha \rightarrow \beta$ is an axiom: since axioms do not involve complex formulas, we immediately conclude that also $\Gamma, y \geq x, y : \alpha \vdash \Delta', y : \beta$ is an axiom, and we are done. For the inductive step, we distinguish two subcases:
  - the proof of $\Gamma \vdash \Delta', x : \alpha \rightarrow \beta$ is ended by an application of $(\rightarrow R)$ to $x : \alpha \rightarrow \beta$, i.e. the proof is ended as follows:

    $$\dfrac{(i)\ \Gamma, y \geq x, y : \alpha \vdash \Delta', z : \beta}{\Gamma \vdash \Delta', x : \alpha \rightarrow \beta}\ (\rightarrow R)$$

    In this case, we immediately conclude, since we have a derivation of the premise $(i)$ of $(\rightarrow R)$. Notice also that, if the height of the starting derivation is $h$, then the height of the proof of $(i)$ is $h - 1$;

- the proof of $\Gamma \vdash \Delta', x : \alpha \rightarrow \beta$ is ended by an application of a rule (R') different from $(\rightarrow R)$ or by $(\rightarrow R)$ to a formula $u : \gamma \rightarrow \delta \in \Delta'$: in this case, we apply the inductive hypothesis on the premises, then we conclude by an application of (R'). As an example, consider a derivation ended by an application of ( **says** $L$) as follows:

$$\frac{(ii)\ \Gamma', x : A\ \textbf{says}\ \gamma \vdash \Delta', x : \alpha \rightarrow \beta, x \xrightarrow{A} y \qquad (iii)\ \Gamma', x : A\ \textbf{says}\ \gamma, y : \gamma \vdash \Delta', x : \alpha \rightarrow \beta}{\Gamma', x : A\ \textbf{says}\ \gamma \vdash \Delta', x : \alpha \rightarrow \beta}\ (\ \textbf{says}\ L)$$

We can apply the inductive hypothesys on $(ii)$ and $(iii)$, i.e. we have derivations (of at most the same height) of $(ii')\ \Gamma', x : A\ \textbf{says}\ \gamma, z \geq x, z : \alpha \vdash \Delta', x \xrightarrow{A} y, z : \beta$ and $(iii')\ \Gamma', x : A\ \textbf{says}\ \gamma, y : \gamma, z \geq x, z : \alpha \vdash \Delta', z : \beta$, where $(ii')$ and $(iii')$ are, respectively, the premises of rule $(\rightarrow R)$ applied to $(ii)$ and $(iii)$. We conclude by an application of ( **says** $L$):

$$\frac{\begin{array}{c}(ii')\ \Gamma', x : A\ \textbf{says}\ \gamma, z \geq x, z : \alpha \vdash \Delta', x \xrightarrow{A} y, z : \beta \\ (iii')\ \Gamma', x : A\ \textbf{says}\ \gamma, y : \gamma, z \geq x, z : \alpha \vdash \Delta', z : \beta\end{array}}{(iv)\ \Gamma', x : A\ \textbf{says}\ \gamma, z \geq x, z : \alpha \vdash \Delta', z : \beta}\ (\ \textbf{says}\ L)$$

It is worth noticing that $z$ does not occur in $\Gamma'$ and $\Delta'$. Therefore, by Lemma 6 and $(iv)$, we have a derivation (of at most the same height) of $\Gamma', x : A\ \textbf{says}\ \gamma, y \geq x, y : \alpha \vdash \Delta', y : \beta$, which is the premise of the rule $(\rightarrow R)$ applied to $\Gamma', x : A\ \textbf{says}\ \gamma \vdash \Delta', x : \alpha \rightarrow \beta$, and we are done. □

It is worth noticing that the height-preserving invertibility also preserves the number of applications of the rules in a proof, that is to say: if $\Gamma_1 \vdash \Delta_1$ is derivable by Lemma 7 since it is the premise of a backward application of an invertible rule R to $\Gamma_2 \vdash \Delta_2$, then it has a derivation containing *the same rule applications* of the proof of $\Gamma_2 \vdash \Delta_2$. For instance, if $(1)\ \Gamma, x \xrightarrow{A} y \vdash \Delta$ is derivable with a proof $\Pi$, then $(2)\ \Gamma, x \xrightarrow{A} y, y : A \vdash \Delta$ is derivable since $(ID)$ is invertible; moreover, there exists a proof of $(2)$ containing the same rules of $\Pi$, obtained by adding $y : A$ in each sequent of $\Pi$ from which $(1)$ descends. This fact will be systematically used throughout this section, in the sense that we will assume that every proof transformation due to the invertibility preserves the number of rules applications in the initial proof.

We can show that the rules of *contraction* are admissibile in $\mathcal{S}_{\mathsf{Cond}_{\mathrm{ACL}}}$ .

**Lemma 8 (Height-preserving and rule-preserving admissibility of contraction).** *The rules of contraction are height-preserving admissible in* $\mathcal{S}_{\mathsf{Cond}_{\mathrm{ACL}}}$ *, i.e. if a sequent* $\Gamma \vdash \Delta, F, F$ *is derivable in SeqS, then there is a derivation of no greater height of* $\Gamma \vdash \Delta, F$*, and if a sequent* $\Gamma, F, F \vdash \Delta$ *is derivable in* $\mathcal{S}_{\mathsf{Cond}_{\mathrm{ACL}}}$ *, then there is a derivation of no greater height of* $\Gamma, F \vdash \Delta$*. Moreover, the rules of contraction are rule-preserving admissibile in* $\mathcal{S}_{\mathsf{Cond}_{\mathrm{ACL}}}$ *, i.e. the proof of the contracted sequent does not add any rule application to the initial proof.*

*Proof.* By simultaneous induction on the height of the drivations for left and right contraction. For the base case, let $\Gamma \vdash \Delta, F, F$ be an axiom. We have the following subcases:

- $F$ is either $y \geq x$ or $x : P$ with $P \in ATM$ and $F \in \Gamma$: in this case, we immediately conclude that also $\Gamma \vdash \Delta, F$ is an axiom;
- $F$ is $x \geq x$: again, also $\Gamma \vdash \Delta, F$ is an instance of $(AX_{\geq})$ and we are done;
- $x : \bot \in \Gamma$: once again, also $\Gamma \vdash \Delta, F$ is an instance of $(AX_{\bot})$.

The other base case, namely the case where $\Gamma, F, F \vdash \Delta$ is an axiom, is symmetric.

For the inductive step, we consider the last rule applied to $\Gamma \vdash \Delta, F, F$ (resp. $\Gamma, F, F \vdash \Delta$). We distinguish three cases:

- the proof is ended by an application of $(EQ)$: in this case, we can conclude since $(EQ)$ only involves two transition formulas, one on the left hand side and one on the right hand side of the sequent. Even if $F$ is a transition formula $x \xrightarrow{A} y$ involved in the application of $(EQ)$, as follows:

$$\dfrac{u : A' \vdash u : A \qquad\qquad u : A \vdash u : A'}{\Gamma', x \xrightarrow{A'} y \vdash \Delta, x \xrightarrow{A} y, x \xrightarrow{A} y}\,(EQ)$$

  the rule can be directly applied to the contracted sequent, and we are done:

$$\dfrac{u : A' \vdash u : A \qquad\qquad u : A \vdash u : A'}{\Gamma', x \xrightarrow{A'} y \vdash \Delta, x \xrightarrow{A} y}\,(EQ)$$

- the applied rule is different from $(EQ)$ and the contracted formula $F$ is not principal in the application of the rule: in this case, both occurrences of $F$ are in the premise(s) of the rule, which have a smaller derivation height. By the inductive hypothesis, they can be contracted and the conclusion is obtained by applying the rule to the contracted premise(s). As an example, consider a proof ended by an application of $(DT)$ as follows:

$$\dfrac{\Gamma', z \geq y, x \xrightarrow{A} y \vdash \Delta, F, F, z : B \qquad \Gamma', z \geq y, x \xrightarrow{A} y, x \xrightarrow{A \wedge B} z \vdash \Delta, F, F}{\Gamma', z \geq y, x \xrightarrow{A} y \vdash \Delta, F, F}\,(DT)$$

  We apply the inductive hypothesis on the two premises, then we conclude by an application of $(DT)$:

$$\dfrac{\Gamma', z \geq y, x \xrightarrow{A} y \vdash \Delta, F, z : B \qquad \Gamma', z \geq y, x \xrightarrow{A} y, x \xrightarrow{A \wedge B} z \vdash \Delta, F}{\Gamma', z \geq y, x \xrightarrow{A} y \vdash \Delta, F}\,(DT)$$

- the applied rule is different from $(EQ)$ and the contracted formula $F$ is principal in the application of the rule: we consider all the rules:
  - $(ATM)$: the proof is ended as follows:

$$\dfrac{\Gamma', x : P, x : P \vdash \Delta, y \geq x \qquad \Gamma', x : P, x : P, y : P \vdash \Delta}{\Gamma', x : P, x : P \vdash \Delta}\,(ATM)$$

    We apply the inductive hypothesis on the premises, obtaining a proof of $\Gamma', x : P \vdash \Delta, y \geq x$ and of $\Gamma', x : P, y : P \vdash \Delta$, from which we conclude by an application of $(ATM)$;

- $(INT)$, $(MON)$, $(DT)$, $(ID)$, $(CA)$, $(CA-conv)$, $(C)$, $(C4)$, $(Unit)$, and $(I)$: in these cases, the proof is similar to the one proposed above for $(ATM)$ and then left to the reader;
- $(\wedge L)$: the proof is ended as follows:

$$\frac{\Gamma, x:\alpha, x:\beta, x:\alpha\wedge\beta \vdash \Delta}{\Gamma, x:\alpha\wedge\beta, x:\alpha\wedge\beta \vdash \Delta}\,(\wedge L)$$

  Since $(\wedge L)$ is height-preserving invertible (Lemma 7), we have a proof of at most the same height of the premise of $\Gamma, x:\alpha, x:\alpha, x:\beta, x:\beta \vdash \Delta$. We can apply the inductive hypothesis to obtain a proof (of no greater height) of $\Gamma, x:\alpha, x:\beta, x:\beta \vdash \Delta$, to which we can again apply the inductive hypothesis to obtain a proof of $\Gamma, x:\alpha, x:\beta \vdash \Delta$, from which we conclude by an application of $(\wedge L)$;
- $(\wedge R)$: the proof is ended as follows:

$$\frac{(i)\ \Gamma \vdash \Delta, x:\alpha, x:\alpha\wedge\beta \qquad (ii)\ \Gamma \vdash \Delta, x:\beta, x:\alpha\wedge\beta}{\Gamma \vdash \Delta, x:\alpha\wedge\beta, x:\alpha\wedge\beta}\,(\wedge R)$$

  By Lemma 7 and $(i)$, we have a derivation of $(i')$ $\Gamma \vdash \Delta, x:\alpha, x:\alpha$ and of $(i'')$ $\Gamma \vdash \Delta, x:\alpha, x:\beta$ of at most the same height of $(i)$. Similarly, we have proofs of $(ii')$ $\Gamma \vdash \Delta, x:\beta, x:\alpha$ and $(ii'')$ $\Gamma \vdash \Delta, x:\beta, x:\beta$. We apply the inductive hypothesis to $(i')$ and $(ii'')$, obtaining proofs of $\Gamma \vdash \Delta, x:\alpha$ and $\Gamma \vdash \Delta, x:\beta$, respectively, from which we conclude by an application of $(\wedge R)$;
- $(\vee R)$ and $(\vee L)$: these cases are similar to the ones for $(\wedge R)$ and $(\wedge L)$ and therefore left to the reader;
- $(\rightarrow R)$: the proof is ended as follows:

$$\frac{\Gamma, y\geq x, y:\alpha \vdash \Delta, x:\alpha\rightarrow\beta, y:\beta}{\Gamma \vdash \Delta, x:\alpha\rightarrow\beta, x:\alpha\rightarrow\beta}\,(\rightarrow R)$$

  Since $(\rightarrow R)$ is height-preserving invertible (Lemma 7), we have a derivation of at most the same height of the premise of $\Gamma, y\geq x, z\geq x, y:\alpha, z:\alpha \vdash \Delta, y:\beta, z:\beta$. $y$ and $z$ are new labels, not occurring in $\Gamma$ and $\Delta$. By the height-preserving label substitution (Lemma 6), we replace the occurrences of $z$ with $y$ to obtain a derivation of $\Gamma, y\geq x, y\geq x, y:\alpha, y:\alpha \vdash \Delta, y:\beta, y:\beta$. We apply three times the inductive hypothesis, obtaining a derivation of $\Gamma, y\geq x, y:\alpha \vdash \Delta, y:\beta$, from which we conclude by an application of $(\rightarrow R)$;
- $(\rightarrow L)$: the proof is ended as follows:

$$\frac{\begin{array}{c}(i)\ \Gamma, x:\alpha\rightarrow\beta, x:\alpha\rightarrow\beta \vdash \Delta, y\geq x\\ (ii)\ \Gamma, x:\alpha\rightarrow\beta, x:\alpha\rightarrow\beta \vdash \Delta, y:\alpha\\ (iii)\ \Gamma, x:\alpha\rightarrow\beta, x:\alpha\rightarrow\beta, y:\beta \vdash \Delta\end{array}}{\Gamma, x:\alpha\rightarrow\beta, x:\alpha\rightarrow\beta \vdash \Delta}\,(\rightarrow L)$$

We can apply the inductive hypothesis on the three premises, obtaining derivations (of at most the same heights) of $(i')$ $\Gamma, x : \alpha \rightarrow \beta \vdash \Delta, y \geq x$, $(ii')$ $\Gamma, x : \alpha \rightarrow \beta \vdash \Delta, y : \alpha$ , and $(iii')$ $\Gamma, x : \alpha \rightarrow \beta, y : \beta \vdash \Delta$, from which we conclude by an application of $(\rightarrow L)$;

- ( **says** $R$) and ( **says** $L$): these cases are similar to the ones for $(\rightarrow R)$ and $(\rightarrow L)$, respectively, and left to the reader. □

We conclude this section by listing some lemmas and properties holding in $\mathcal{S}_{\mathsf{Cond}_{\mathrm{ACL}}}$ that will be used to prove its soundness and completeness:

**Lemma 9.** *A sequent* $\vdash x : A \rightarrow B$ *is derivable in* $\mathcal{S}_{\mathsf{Cond}_{\mathrm{ACL}}}$ *if and only if the sequent* $x : A \vdash x : B$ *is derivable in* $\mathcal{S}_{\mathsf{Cond}_{\mathrm{ACL}}}$ *.*

*Proof.* If $x : A \vdash x : B$ is derivable, then, by Lemma 5, also $x \geq u, x : A \vdash x : B$ is derivable. By an application of $(\rightarrow R)$, we obtain a derivation of $\vdash u : A \rightarrow B$. By Lemma 6 we conclude with a derivation of $\vdash x : A \rightarrow B$.

If $\vdash x : A \rightarrow B$ is derivable, then we have also a derivation for $u \geq x, u : A \vdash u : B$ since $(\rightarrow R)$ is invertible (Lemma 7). It can be observed that no rule of $\mathcal{S}_{\mathsf{Cond}_{\mathrm{ACL}}}$ manipulate the label $x$, therefore the formula $u \geq x$ is useless. This means that there is a derivation in $\mathcal{S}_{\mathsf{Cond}_{\mathrm{ACL}}}$ of $u : A \vdash u : B$ and, by Lemma 6, there is a derivation of $x : A \vdash x : B$. □

We can generalize axioms to a generic formula $F$, that is to say:

**Proposition 4.** *Given any formula* $F$*, the sequent* $\Gamma, F \vdash \Delta, F$ *is derivable in* $\mathcal{S}_{\mathit{Cond}_{\mathrm{ACL}}}$ .

*Proof.* By induction on the complexity of $F$. For the base case, we have that $F$ is either $x : P$ with $P \in ATM$ or $y \geq x$, then the sequent is an instance of $(AX)$ and we are done. For the inductive step, we distinguish two subcases:

- $F$ has the form $x \xrightarrow{A} y$: by inductive hypothesis, $u : A \vdash u : A$ is derivable, then we conclude that $\Gamma, x \xrightarrow{A} y \vdash \Delta, x \xrightarrow{A} y$ is derivable by an application of $(EQ)$;
- $F$ is a complex formula $x : A \otimes B$, where $\otimes$ stands for $\{\rightarrow, \wedge, \vee,$ **says** $\}$. We only present the most interesting cases of **says** and $\rightarrow$, the other cases are similar and left to the reader. Concerning **says** , there are derivations in $\mathcal{S}_{\mathsf{Cond}_{\mathrm{ACL}}}$ for $(1)$ $u : A \vdash u : A$ and $(2)$ $\Gamma, x : A$ **says** $B, x \xrightarrow{A} y, y : B \vdash \Delta, y : B$ by inductive hypothesis. We can conclude as follows:

$$\dfrac{\dfrac{(1)\ u : A \vdash u : A \qquad (1)\ u : A \vdash u : A}{\Gamma, x : A \ \textbf{says}\ B, x \xrightarrow{A} y \vdash \Delta, y : B, x \xrightarrow{A} y}\,(EQ) \qquad (2)\ \Gamma, x : A \ \textbf{says}\ B, x \xrightarrow{A} y, y : B \vdash \Delta, y : B}{\dfrac{\Gamma, x : A \ \textbf{says}\ B, x \xrightarrow{A} y \vdash \Delta, y : B}{\Gamma, x : A \ \textbf{says}\ B \vdash \Delta, x : A \ \textbf{says}\ B}\,(\ \textbf{says}\ R)}\,(\ \textbf{says}\ L)$$

Concerning $\rightarrow$, again we apply the inductive hypothesis to prove that there are derivations of $(3)$ $\Gamma, y \geq x, x : A \rightarrow B, y : A, y : B \vdash \Delta, y : B$ and $(4)$ $\Gamma, y \geq x, x : A \rightarrow B, y : A \vdash \Delta, y : B, y : A$. We conclude as follows:

$$\dfrac{\dfrac{\begin{array}{c}\Gamma, y \geq x, x : A \rightarrow B, y : A \vdash \Delta, y : B, y \geq x \\ (3)\ \Gamma, y \geq x, x : A \rightarrow B, y : A, y : B \vdash \Delta, y : B \\ (4)\ \Gamma, y \geq x, x : A \rightarrow B, y : A \vdash \Delta, y : B, y : A\end{array}}{\Gamma, y \geq x, x : A \rightarrow B, y : A \vdash \Delta, y : B}\,(\rightarrow L)}{\Gamma, x : A \rightarrow B \vdash \Delta, x : A \rightarrow B}\,(\rightarrow R)$$

□

**Lemma 10.** *Given any formula $\gamma \in \mathcal{L}$, the sequent $\Gamma, y \geq x, x : \gamma \vdash \Delta, y : \gamma$ is derivable in $\mathcal{S}_{\mathsf{Cond}_{\mathsf{ACL}}}$ .*

*Proof.* We consider all possible formulas $\gamma \in \mathcal{L}$, starting with atomic ones $\gamma = P \in ATM$. The sequent $y : P \vdash y : P$ is an instance of $(AX)$. Since weakening is admissible (Lemma 5), we have that also $(1)\ \Gamma, y \geq x, x : P, y : P \vdash \Delta, y : P$ is derivable. The same for $(1')\ \Gamma, y \geq x, x : P \vdash \Delta, y : P, y \geq x$, since $y \geq x \vdash y \geq x$ is an instance of $(AX)$. We conclude by an application of the rule $(ATM)$:

$$\dfrac{(1')\ \Gamma, y \geq x, x : P \vdash \Delta, y : P, y \geq x \qquad\qquad (1)\ \Gamma, y \geq x, x : P, y : P \vdash \Delta, y : P}{\Gamma, y \geq x, x : P \vdash \Delta, y : P}\,(ATM)$$

For the complex formulas, we only present the most interesting cases of $\gamma = A \rightarrow B$ and $\gamma = A$ **says** $B$, the other cases are easy and left to the reader. By Proposition 4, we have derivations for $(2)\ v : A \vdash v : A$, $(3)\ v : B \vdash v : B$, $(4)\ z : B \vdash z : B$, and $(5)\ v \geq x \vdash v \geq x$, and, by Lemma 5, of $(2')\ \Gamma, v \geq x, v \geq y, y \geq x, x : A \rightarrow B, v : A \vdash v : B, v : A$, $(3')\ \Gamma, v \geq x, v \geq y, y \geq x, x : A \rightarrow B, v : A, v : B \vdash v : B$, $(4')\ \Gamma, y \geq x, y \xrightarrow{A} z, x \xrightarrow{A} z, x : A$ **says** $B, z : B \vdash \Delta, z : B$, and $(5')\ \Gamma, v \geq x, v \geq y, y \geq x, x : A \rightarrow B, v : A \vdash v : B, v \geq x$. We can conclude as follows:

$$\dfrac{\dfrac{\dfrac{\begin{array}{c}(5')\ \Gamma, v \geq x, v \geq y, y \geq x, x : A \rightarrow B, v : A \vdash v : B, v \geq x \\ (2')\ \Gamma, v \geq x, v \geq y, y \geq x, x : A \rightarrow B, v : A \vdash v : B, v : A \\ (3')\ \Gamma, v \geq x, v \geq y, y \geq x, x : A \rightarrow B, v : A, v : B \vdash v : B\end{array}}{\Gamma, v \geq x, v \geq y, y \geq x, x : A \rightarrow B, v : A \vdash v : B}\,(\rightarrow L)}{\Gamma, v \geq y, y \geq x, x : A \rightarrow B, v : A \vdash v : B}\,(TR)}{\Gamma, y \geq x, x : A \rightarrow B \vdash \Delta, y : A \rightarrow B}\,(\rightarrow R)$$

$$\dfrac{\dfrac{\dfrac{\dfrac{(2)\ v : A \vdash v : A \qquad (2)\ v : A \vdash v : A}{\Gamma, y \geq x, y \xrightarrow{A} z, x \xrightarrow{A} z, x : A\ \textbf{says}\ B \vdash \Delta, z : B, x \xrightarrow{A} z}\,(EQ) \qquad (4')\ \Gamma, y \geq x, y \xrightarrow{A} z, x \xrightarrow{A} z, x : A\ \textbf{says}\ B, z : B \vdash \Delta, z : B}{\Gamma, y \geq x, y \xrightarrow{A} z, x \xrightarrow{A} z, x : A\ \textbf{says}\ B \vdash \Delta, z : B}\,(\textbf{says}\ L)}{\Gamma, y \geq x, y \xrightarrow{A} z, x : A\ \textbf{says}\ B \vdash \Delta, z : B}\,(INT)}{\Gamma, y \geq x, x : A\ \textbf{says}\ B \vdash \Delta, y : A\ \textbf{says}\ B}\,(\textbf{says}\ R)$$

□

**Lemma 11.** *If $\Gamma, x \geq x \vdash \Delta$ is derivable in $\mathcal{S}_{\mathsf{Cond}_{\mathrm{ACL}}}$, then also $\Gamma \vdash \Delta$ is derivable with a derivation of at most the same height.*

*Proof.* By induction on the height of the derivation of $\Gamma, x \geq x \vdash \Delta$. The base case is easy, since axioms do not involve formulas $x \geq x$ in the left hand side of a sequent, with the only exception of the case in which $x \geq x \in \Delta$: however, in this case, $\Gamma \vdash \Delta$ is an instance of $(AX_{\geq})$ and we are done. For the inductive step, we have to consider all the rules of $\mathcal{S}_{\mathsf{Cond}_{\mathrm{ACL}}}$ that can be applied to end the derivation of $\Gamma, x \geq x \vdash \Delta$. To save space, we only present the most interesting case of a proof ended with an application of $(TR)$ as follows:

$$\frac{\Gamma', y \geq x, y \geq x, x \geq x \vdash \Delta}{\Gamma', y \geq x, x \geq x \vdash \Delta}\,(TR)$$

By inductive hypothesis, there is a derivation of at most the same height of $\Gamma', y \geq x, y \geq x \vdash \Delta$, then, by Lemma 8, of $\Gamma', y \geq x \vdash \Delta$, and we are done. The other cases are similar and left to the reader. □

**Lemma 12.** *If $\Gamma \vdash \Delta, x : \bot$ is derivable in $\mathcal{S}_{\mathsf{Cond}_{\mathrm{ACL}}}$, then also $\Gamma \vdash \Delta$ is derivable.*

*Proof.* By induction on the height of the derivation of $\Gamma \vdash \Delta, x : \bot$. The base case is straighforward, since $x : \bot$ in the right hand side of a sequent is involved in an axiom only in case $x : \bot \in \Gamma$, however in this case we immediatley conclude that $\Gamma \vdash \Delta$ is an instance of $(AX_{\bot})$. For the inductive step, we just observe that all the rules except $(EQ)$ copy $x : \bot$ in their premise(s), then we can conclude the proof by applying the inductive hypothesis to such premise(s) and then reapplying the same rules. In case the derivation of $\Gamma \vdash \Delta, x : \bot$ is ended by an application of $(EQ)$ the proof is also straightforward, since $(EQ)$ is applied to transition formulas belonging to $\Gamma$ and $\Delta$, therefore we have a proof of $\Gamma \vdash \Delta$ by an application of $(EQ)$. □

### 5.2 Soundness and Completeness of $\mathcal{S}_{\mathsf{Cond}_{\mathrm{ACL}}}$

Let us first prove that the calculus $\mathcal{S}_{\mathsf{Cond}_{\mathrm{ACL}}}$ is sound with respect to the semantics:

**Theorem 8 (Soundness of $\mathcal{S}_{\mathsf{Cond}_{\mathrm{ACL}}}$).** *If a sequent $\Gamma \vdash \Delta$ is derivable, then $\Gamma \vdash \Delta$ is valid in the sense of Definition 7.*

*Proof.* By induction on the height of the derivation of $\Gamma \vdash \Delta$. The base cases are as follows:

- $\Gamma \vdash \Delta$ is an instance of $(AX)$, i.e. there is an $F$ such that $F \in \Gamma \cap \Delta$. In this case, given any model $\mathcal{M}$, if it satifies all the formulas in $\Gamma$, then it also satisfies $F$. As a consequence, such model also satisfies at least a formula in $\Delta$ (the formula $F$ itself), and the sequent is valid;
- $\Gamma \vdash \Delta$ is an instance of $(AX_{\bot})$, i.e. $x : \bot \in \Gamma$: we immediately conclude that the sequent is valid, since there is no model satifying $x : \bot$;
- $\Gamma \vdash \Delta$ is an instance of $(AX_{\geq})$, i.e. $x \geq x \in \Delta$: in this case, given any model $\mathcal{M}$ and any function $I$, since $\leq$ is reflexive, we have that $I(x) \leq I(x)$, then the formula $x \geq x$ is satisfied in $\mathcal{M}$ via $I$ and the sequent is valid.

For the inductive step, we have the following cases (the list is exhaustive):

- the derivation of $\Gamma', x : P \vdash \Delta$ ends with an application of $(ATM)$, with $P \in ATM$. By inductive hypothesis, the premises $\Gamma', x : P \vdash \Delta, y \geq x$ and $\Gamma', x : P, y : P \vdash \Delta$ are valid sequents. By absurd, suppose the conclusion is not, that is to say there is a model $\mathcal{M}$ and a function $I$ such that $\mathcal{M} \models_I F$ for every $F \in \Gamma'$, $\mathcal{M} \models_I x : P$ (i.e. $I(x) \in h(P)$), whereas $\mathcal{M} \not\models_I G$ for any $G \in \Delta$. Since $\Gamma', x : P \vdash \Delta, y \geq x$ is valid, we have that $\mathcal{M} \models_I y \geq x$, i.e. $I(x) \leq I(y)$ and, since $I(x) \in h(P)$ and $P \in ATM$, we have also that $I(y) \in h(P)$. Therefore, $\mathcal{M}$ satisfies via $I$ all formulas in the left hand side of the premise $\Gamma', x : P, y : P \vdash \Delta$, however $\mathcal{M} \not\models_I G$ for any $G \in \Delta$, against its validity;
- the derivation of $\Gamma', x : \alpha \wedge \beta \vdash \Delta$ ends with an application of $(\wedge L)$: by inductive hypothesis, the sequent $\Gamma', x : \alpha, x : \beta \vdash \Delta$ is valid. By absurd, the conclusion is not, i.e. there is a model $\mathcal{M}$ and a function $I$ such that $\mathcal{M} \models_I F$ for every $F \in \Gamma'$, $\mathcal{M} \models_I x : \alpha \wedge \beta$ (i.e., $I(x) \in [|\alpha|] \cap [|\beta|]$), whereas $\mathcal{M} \not\models_I G$ for any $G \in \Delta$. It immediately follows that $\mathcal{M} \models_I x : \alpha$ as well as $\mathcal{M} \models_I x : \beta$, so $\mathcal{M} \models_I F$ for every $F$ in the left hand side of the premise, whereas $\mathcal{M} \not\models_I G$ for any $G \in \Delta$, against the validity of the premise itself;
- the derivation of $\Gamma \vdash \Delta', x : \alpha \wedge \beta$ ends with an application of $(\wedge R)$: by inductive hypothesis, the sequents $\Gamma \vdash \Delta', x : \alpha$ and $\Gamma \vdash \Delta', x : \beta$ are valid. By absurd, suppose that the conclusion $\Gamma \vdash \Delta', x : \alpha \wedge \beta$ is not valid, i.e. there is a model $\mathcal{M}$ and a function $I$ such that $\mathcal{M} \models_I F$ for every $F \in \Gamma$, whereas $\mathcal{M} \not\models_I G$ for any $G \in \Delta$ and $\mathcal{M} \not\models_I x : \alpha \wedge \beta$, i.e. either $I(x) \notin [|\alpha|]$ or $I(x) \notin [|\beta|]$. If $I(x) \notin [|\alpha|]$, we have that $\mathcal{M}$ satisfies via $I$ all the formulas in the left hand side of the premise $\Gamma \vdash \Delta', x : \alpha$, whereas it falsifies all the formulas in its right hand side, against the validity of such premise. Reasoning in the same way, in case $I(x) \notin [|\beta|]$ we contradict the hypothesis that $\Gamma \vdash \Delta', x : \beta$ is valid;
- the derivation of $\Gamma', x : \alpha \vee \beta \vdash \Delta$ ends with an application of $(\vee L)$: by inductive hypothesis, the sequents $\Gamma', x : \alpha \vdash \Delta$ and $\Gamma', x : \beta \vdash \Delta$ are valid. By absurd, suppose that the conclusion is not, i.e. there is a model $\mathcal{M}$ and a function $I$ such that $\mathcal{M} \models_I F$ for every $F \in \Gamma'$ and $\mathcal{M} \models_I x : \alpha \vee \beta$, i.e. $I(x) \in [|\alpha|] \cup [|\beta|]$, whereas $\mathcal{M} \not\models_I G$ for any $G \in \Delta$. Since $I(x) \in [|\alpha|] \cup [|\beta|]$, we have that either $I(x) \in [|\alpha|]$ or $I(x) \in [|\beta|]$. In case $I(x) \in [|\alpha|]$, we have that $\mathcal{M} \models_I x : \alpha$, however, this contradicts the fact that the premise $\Gamma', x : \alpha \vdash \Delta$ of $(\vee L)$ is valid, since $\mathcal{M} \models_I F$ for every $F \in \Gamma'$ but $\mathcal{M} \not\models_I G$ for any $G \in \Delta$. In case $I(x) \in [|\beta|]$, we reason in the same way and we contradict the fact that the premise $\Gamma', x : \beta \vdash \Delta$ of $(\vee L)$ is valid;
- the derivation of $\Gamma \vdash \Delta', x : \alpha \vee \beta$ ends with an application of $(\vee R)$: by inductive hypothesis, the sequent $\Gamma \vdash \Delta', x : \alpha, x : \beta$ is valid. By absurd, suppose that the conclusion is not, i.e. there is a model $\mathcal{M}$ and a function $I$ such that $\mathcal{M} \models_I F$ for every $F \in \Gamma$, whereas $\mathcal{M} \not\models_I G$ for any $G \in \Delta'$ and $\mathcal{M} \not\models_I x : \alpha \vee \beta$, i.e. $I(x) \notin [|\alpha \vee \beta|]$, that is to say $I(x) \notin [|\alpha|]$ and $I(x) \notin [|\beta|]$. This contradicts the validity of $\Gamma \vdash \Delta', x : \alpha, x : \beta$, since we have a model $\mathcal{M}$ and a function $I$ such that $\mathcal{M} \models_I F$ for every $F \in \Gamma'$, whereas $\mathcal{M} \not\models_I G$ for any $G \in \Delta'$ and $\mathcal{M} \not\models_I x : \alpha$ and $\mathcal{M} \not\models_I x : \beta$;
- the derivation of $\Gamma', x : \alpha \rightarrow \beta \vdash \Delta$ ends with an application of $(\rightarrow L)$: by inductive hypothesis, the premises (1) $\Gamma', x : \alpha \rightarrow \beta \vdash \Delta, y \geq x$, (2) $\Gamma', x :$

$\alpha \rightarrow \beta \vdash \Delta, y : \alpha$, and $(3)$ $\Gamma', x : \alpha \rightarrow \beta, y : \beta \vdash \Delta$ are valid. By absurd, the conclusion is not, i.e. there is a model $\mathcal{M}$ and a function $I$ such that $\mathcal{M} \models_I F$ for every $F \in \Gamma'$, $\mathcal{M} \models_I x : \alpha \rightarrow \beta$ (i.e., $I(x) \in [|\alpha \rightarrow \beta|]$), whereas $\mathcal{M} \not\models_I G$ for any $G \in \Delta'$. By the validity of $(1)$, we can conclude that also $\mathcal{M} \models_I y \geq x$, i.e. $I(x) \leq I(y)$. Similarly, by the validity of $(2)$, we can conclude that $\mathcal{M} \models_I y : \alpha$, i.e. $I(y) \in [|\alpha|]$. Since $I(x) \leq I(y)$, $I(y) \in [|\alpha|]$, and $I(x) \in [|\alpha \rightarrow \beta|]$, we have that $I(y) \in [|\beta|]$, i.e. $\mathcal{M} \models_I y : \beta$. Therefore, $\mathcal{M}$ satisfies, via $I$, all the formulas in the left hand side of the premise $(3)$, whereas it falsifies all the formulas in the right hand side, against the hypothesis that $(3)$ is valid;

- the derivation of $\Gamma \vdash \Delta', x : \alpha \rightarrow \beta$ ends with an application of $(\rightarrow R)$: by inductive hypothesis, the premise $\Gamma, y \geq x, y : \alpha \vdash \Delta', y : \beta$ is valid. By absurd, suppose that the conclusion is not, i.e. there is a model $\mathcal{M}$ and a function $I$ such that $\mathcal{M} \models_I F$ for every $F \in \Gamma$, whereas $\mathcal{M} \not\models_I G$ for any $G \in \Delta$ and $\mathcal{M} \not\models_I x : \alpha \rightarrow \beta$, i.e. $I(x) \notin [|\alpha \rightarrow \beta|]$. This means that there exists a world $w$ such that $I(x) \leq w$ and $w \in [|\alpha|]$, whereas $w \notin [|\beta|]$. Let us define a function $I'$ such that $I'(y) = w$, whereas $I'(k) = I(k)$ for all labels $k$ different from $y$. Since $y$ is a label not occurring in the conclusion, it immediately follows that $\mathcal{M} \models_{I'} F$ for every $F \in \Gamma$, whereas $\mathcal{M} \not\models_{I'} G$ for any $G \in \Delta'$. Furthermore, since $I(x) \leq w$, we have that $\mathcal{M} \models_{I'} y \geq x$ and, since $w \in [|\alpha|]$, we have that $\mathcal{M} \models_{I'} y : \alpha$. From the fact that $w \notin [|\beta|]$, we also conclude that $\mathcal{M} \not\models_{I'} y : \beta$, against the validity of $\Gamma, y \geq x, y : \alpha \vdash \Delta', y : \beta$;
- the derivation of $\Gamma', x : A$ **says** $\gamma \vdash \Delta$ ends with an application of ( **says** $L$): by inductive hypothesis, the premises $(4)$ $\Gamma', x : A$ **says** $\gamma \vdash \Delta, x \xrightarrow{A} y$ and $(5)$ $\Gamma', x : A$ **says** $\gamma, y : \gamma \vdash \Delta$ are valid. By absurd, the conclusion is not, i.e. there is a model $\mathcal{M}$ and a function $I$ such that $\mathcal{M} \models_I F$ for every $F \in \Gamma'$, $\mathcal{M} \models_I x : A$ **says** $\gamma$ (i.e., for all $w \in R_A(I(x))$ we have that $w \in [|\gamma|]$), whereas $\mathcal{M} \not\models_I G$ for any $G \in \Delta$. Since $(4)$ is valid, we have that $\mathcal{M} \models_I x \xrightarrow{A} y$, that is to say $I(y) \in R_A(I(x))$. Therefore, since $\mathcal{M} \models_I x : A$ **says** $\gamma$, we have that also $I(y) \in [|\gamma|]$. We can conclude that $\mathcal{M} \models_I F$ for every $F \in \Gamma'$ and $\mathcal{M} \models_I y : \gamma$, but $\mathcal{M} \not\models_I G$ for any $G \in \Delta$ against the validity of $(5)$;
- the derivation of $\Gamma \vdash \Delta', x : A$ **says** $\gamma$ ends with an application of ( **says** $R$): by inductive hypothesis, the premise $\Gamma, x \xrightarrow{A} y \vdash \Delta', y : \gamma$ is valid. By absurd, suppose that the conclusion is not, i.e. there is a model $\mathcal{M}$ and a function $I$ such that $\mathcal{M} \models_I F$ for every $F \in \Gamma$, whereas $\mathcal{M} \not\models_I G$ for any $G \in \Delta$ and $\mathcal{M} \not\models_I x : A$ **says** $\gamma$, i.e. $I(x) \notin [|A$ **says** $\gamma|]$. This means that there exists a world $w$ such that $I(x) R_A w$ and $w \notin [|\gamma|]$. We define a function $I'$ such that $I'(y) = w$, whereas $I'(k) = I(k)$ for all labels $k$ different from $y$. Since $y$ is a label not occurring in the conclusion, it immediately follows that $\mathcal{M} \models_{I'} F$ for every $F \in \Gamma$, whereas $\mathcal{M} \not\models_{I'} G$ for any $G \in \Delta'$. Moreover, $I(x) R_A w$ means that $\mathcal{M} \models_{I'} x \xrightarrow{A} y$, as well as $w \notin [|\gamma|]$ means that $\mathcal{M} \not\models_{I'} y : \gamma$, against the validity of the premise $\Gamma, x \xrightarrow{A} y \vdash \Delta', y : \gamma$;
- the derivation of $\Gamma', x \xrightarrow{A} y \vdash \Delta', x \xrightarrow{B} y$ ends with an application of $(EQ)$: by inductive hypothesis, the premises $u : A \vdash u : B$ and $u : B \vdash u : A$ are valid sequents. This means that, given any model $\mathcal{M}$ and any function $I$, we have

that $I(u) \in [|A|]$ if and only if $I(u) \in [|B|]$, that is to say $[|A|] = [|B|]$. By the condition (S-RCEA) in Definition 2, we have that also $R_A = R_B$. By absurd, the conclusion is not valid, that is to say there is a model $\mathcal{M}$ and a function $I$ such that $\mathcal{M} \models_I F$ for every $F \in \Gamma'$, $\mathcal{M} \models_I x \xrightarrow{A} y$ (i.e. $I(x)R_A I(y)$), whereas $\mathcal{M} \not\models_I G$ for any $G \in \Delta'$ and $\mathcal{M} \not\models_I x \xrightarrow{B} y$ (i.e. $I(y) \notin R_B(I(x))$). The facts that $I(y) \in R_A(I(x))$ but $I(y) \notin R_B(I(x))$ contradict the fact that $R_A = R_B$;

- the derivation of $\Gamma', z \geq y, y \geq x \vdash \Delta$ ends with an application of $(TR)$: by inductive hypothesis, the premise $\Gamma', z \geq y, y \geq x, z \geq x \vdash \Delta$ is valid. By absurd, the conclusion is not, i.e. there is a model $\mathcal{M}$ and a function $I$ such that $\mathcal{M} \models_I F$ for every $F \in \Gamma'$, $\mathcal{M} \models_I z \geq y$ (i.e. $I(y) \leq I(z)$), $\mathcal{M} \models_I y \geq x$ (i.e. $I(x) \leq I(y)$), whereas $\mathcal{M} \not\models_I G$ for any $G \in \Delta$. Since the relation $\leq$ is transitive, it immediately follows that $I(x) \leq I(z)$, therefore $\mathcal{M} \models_I z \geq x$, against the validity of the premise;
- the derivation of $\Gamma', y \geq x, y \xrightarrow{A} z \vdash \Delta$ is ended by an application of $(INT)$: by inductive hypothesis, the premise $\Gamma', y \geq x, y \xrightarrow{A} z, x \xrightarrow{A} z \vdash \Delta$ is valid. By absurd, the conclusion is not, that is to say there is a model $\mathcal{M}$ and a function $I$ such that $\mathcal{M} \models_I F$ for every $F \in \Gamma'$, $\mathcal{M} \models_I y \geq x$ (i.e. $I(x) \leq I(y)$), $\mathcal{M} \models_I y \xrightarrow{A} z$ (i.e. $I(y)R_A I(z)$), whereas $\mathcal{M} \not\models_I G$ for any $G \in \Delta$. By (S-Int) in Definition 2, from $I(x) \leq I(y)$ and $I(y)R_A I(z)$ it follows that $I(x)R_A I(z)$, therefore $\mathcal{M}$ satisfies via $I$ all the formulas in the left hand side of the premise, and none in the right hand side, against its validity;
- the derivation of $\Gamma', x \xrightarrow{A} y \vdash \Delta$ ends by an application of $(ID)$: by inductive hypothesis, the premise $\Gamma', x \xrightarrow{A} y, y : A \vdash \Delta$ is a valid sequent. By absurd, the conclusion is not, i.e. there is a model $\mathcal{M}$ and a function $I$ such that $\mathcal{M} \models_I F$ for every $F \in \Gamma'$, $\mathcal{M} \models_I x \xrightarrow{A} y$ (i.e., $I(x)R_A I(y)$), whereas $\mathcal{M} \not\models_I G$ for any $G \in \Delta$. By (S-ID) in Definition 2, we have that, since $I(x)R_A I(y)$, it holds that $I(y) \in [|A|]$, against the validity of the premise;
- the derivation of $\Gamma \vdash \Delta$ ends by an application of $(CA)$: by inductive hypothesis, the premises $(i)$ $\Gamma \vdash \Delta, x \xrightarrow{A \vee B} y$, $(ii)$ $\Gamma, x \xrightarrow{A} y \vdash \Delta$ and $(iii)$ $\Gamma, x \xrightarrow{B} y \vdash \Delta$ are valid sequents. By absurd, the conclusion is not, i.e. there is a model $\mathcal{M}$ and a function $I$ such that $\mathcal{M} \models_I F$ for every $F \in \Gamma$, whereas $\mathcal{M} \not\models_I G$ for any $G \in \Delta$. Since $(i)$ $\Gamma \vdash \Delta, x \xrightarrow{A \vee B} y$ is valid, we have that $\mathcal{M} \models_I x \xrightarrow{A \vee B} y$, i.e. $I(x)R_{A \vee B} I(y)$. By (S-CA) in Definition 2, we have that $R_{A \vee B}(I(x)) = R_A(I(x)) \cup R_B(I(x))$, then $I(y) \in R_A(I(x)) \cup R_B(I(x))$, that is to say either $I(y) \in R_A(I(x))$ or $I(y) \in R_B(I(x))$. Suppose $I(y) \in R_A(I(x))$: in this case, we have also that $\mathcal{M} \models_I x \xrightarrow{A} y$, against the validity of the premise $(ii)$ $\Gamma, x \xrightarrow{A} y \vdash \Delta$. In case $I(y) \in R_B(I(x))$, we conclude analogously against the validity of $(iii)$ $\Gamma, x \xrightarrow{B} y \vdash \Delta$;
- the derivation of $\Gamma', x \xrightarrow{A} y \vdash \Delta$ ends by an application of $(CA - conv)$: by inductive hypothesis, the premise $\Gamma', x \xrightarrow{A \vee B} y, x \xrightarrow{A} y \vdash \Delta$ is valid. By absurd, the conclusion is not, i.e. there is a model $\mathcal{M}$ and a function $I$ such that $\mathcal{M} \models_I F$ for every $F \in \Gamma'$, $\mathcal{M} \models_I x \xrightarrow{A} y$ (i.e., $I(x)R_A I(y)$), whereas $\mathcal{M} \not\models_I G$ for

any $G \in \Delta$. By (S-CA) in Definition 2, we have that $R_{A \vee B}(I(x)) = R_A(I(x)) \cup R_B(I(x))$, then $I(y) \in R_A(I(x))$ implies $I(y) \in R_A(I(x)) \cup R_B(I(x))$, thus $I(y) \in R_{A \vee B}(I(x))$. We conclude that $\mathcal{M} \models_I x \xrightarrow{A \vee B} y$, against the validity of the premise;

- the derivation of $\Gamma', z \geq y, x \xrightarrow{A} y \vdash \Delta$ ends by an application of $(DT)$: by inductive hypothesis, the premises $\Gamma', z \geq y, x \xrightarrow{A} y \vdash \Delta, z : B$ and $\Gamma', z \geq y, x \xrightarrow{A} y, x \xrightarrow{A \wedge B} z \vdash \Delta$ are valid sequents. By absurd, the conclusion is not, i.e. there is a model $\mathcal{M}$ and a function $I$ such that $\mathcal{M} \models_I F$ for every $F \in \Gamma'$, $\mathcal{M} \models_I z \geq y$ (i.e. $I(y) \leq I(z)$), $\mathcal{M} \models_I x \xrightarrow{A} y$ (i.e., $I(x) R_A I(y)$), whereas $\mathcal{M} \not\models_I G$ for any $G \in \Delta$. Since $\Gamma', z \geq y, x \xrightarrow{A} y \vdash \Delta, z : B$ is valid, it follows that also $\mathcal{M} \models_I z : B$, that is to say $I(z) \in [|B|]$. By (S-DT) in Definition 2, from $I(x) R_A I(y)$, $I(y) \leq I(z)$, and $I(z) \in [|B|]$, it follows that also $I(x) R_{A \wedge B} I(z)$, i.e. $\mathcal{M} \models_I x \xrightarrow{A \wedge B} z$, against the validity of the premise $\Gamma', z \geq y, x \xrightarrow{A} y, x \xrightarrow{A \wedge B} z \vdash \Delta$;
- the derivation of $\Gamma \vdash \Delta$ ends by an application of $(MON)$: by inductive hypothesis, the premises $\Gamma \vdash \Delta, x \xrightarrow{A \wedge B} y$ and $\Gamma, x \xrightarrow{A} y, x \xrightarrow{B} y \vdash \Delta$ are valid. By absurd, the conclusion is not, i.e. there is a model $\mathcal{M}$ and a function $I$ such that $\mathcal{M} \models_I F$ for every $F \in \Gamma$, whereas $\mathcal{M} \not\models_I G$ for any $G \in \Delta$. Since the premise $\Gamma \vdash \Delta, x \xrightarrow{A \wedge B} y$ is valid, we have that also $\mathcal{M} \models_I x \xrightarrow{A \wedge B} y$, that is to say $I(x) R_{A \wedge B} I(y)$. By (S-Mon) in Definition 2, we have that $I(x) R_A I(y)$ and $I(x) R_B I(y)$, therefore $\mathcal{M} \models_I x \xrightarrow{A} y$ and $\mathcal{M} \models_I x \xrightarrow{B} y$, against the validity of the premise $\Gamma, x \xrightarrow{A} y, x \xrightarrow{B} y \vdash \Delta$.
- the derivation of $\Gamma', x \xrightarrow{A} y \vdash \Delta$ ends by an application of $(Unit)$: by inductive hypothesis, the premise $\Gamma', x \xrightarrow{A} y, y \geq x \vdash \Delta$ is a valid sequent. By absurd, the conclusion is not, i.e. there is a model $\mathcal{M}$ and a function $I$ such that $\mathcal{M} \models_I F$ for every $F \in \Gamma'$, $\mathcal{M} \models_I x \xrightarrow{A} y$ (i.e., $I(x) R_A I(y)$), whereas $\mathcal{M} \not\models_I G$ for any $G \in \Delta$. By (S-UNIT) in Definition 2, we have that, since $I(x) R_A I(y)$, also $I(x) \leq I(y)$, then $\mathcal{M} \models_I y \geq x$, against the validity of the premise;
- the derivation of $\Gamma', x \xrightarrow{B} y, y \xrightarrow{A} z \vdash \Delta$ ends by an application of $(I)$: by inductive hypothesis, the premise $\Gamma', x \xrightarrow{B} y, y \xrightarrow{A} z, x \xrightarrow{A} z \vdash \Delta$ is a valid sequent. By absurd, the conclusion is not, i.e. there is a model $\mathcal{M}$ and a function $I$ such that $\mathcal{M} \models_I F$ for every $F \in \Gamma'$, $\mathcal{M} \models_I x \xrightarrow{B} y$ (i.e., $I(x) R_B I(y)$), $\mathcal{M} \models_I y \xrightarrow{A} z$ (i.e., $I(y) R_A I(z)$), whereas $\mathcal{M} \not\models_I G$ for any $G \in \Delta$. By (S-I) in Definition 3, we have that, since $I(x) R_B I(y)$ and $I(y) R_A I(z)$, also $I(x) R_A I(z)$, then $\mathcal{M} \models_I x \xrightarrow{A} z$, against the validity of the premise;
- the derivation of $\Gamma', z \geq y, x \xrightarrow{A} y \vdash \Delta$ ends by an application of $(C)$: by inductive hypothesis, the premise $\Gamma', z \geq y, x \xrightarrow{A} y, z \xrightarrow{A} z \vdash \Delta$ is a valid sequent. By absurd, the conclusion is not, i.e. there is a model $\mathcal{M}$ and a function $I$ such that $\mathcal{M} \models_I F$ for every $F \in \Gamma'$, $\mathcal{M} \models_I z \geq y$ (i.e., $I(y) \leq I(z)$), and $\mathcal{M} \models_I x \xrightarrow{A} y$ (i.e., $I(x) R_A I(y)$), whereas $\mathcal{M} \not\models_I G$ for any $G \in \Delta$. By (S-C) in

Definition 2, we have that, since $I(x)R_AI(y)$ and $I(y) \leq I(z)$, also $I(z)R_AI(z)$, then $\mathcal{M} \models_I z \xrightarrow{A} z$, against the validity of the premise;

– the derivation of $\Gamma', x \xrightarrow{A} y \vdash \Delta$ ends by an application of $(C4)$: by inductive hypothesis, the premise $\Gamma', x \xrightarrow{A} y, x \xrightarrow{A} z, z \xrightarrow{A} y \vdash \Delta$ is a valid sequent. By absurd, the conclusion is not, i.e. there is a model $\mathcal{M}$ and a function $I$ such that $\mathcal{M} \models_I F$ for every $F \in \Gamma'$, $\mathcal{M} \models_I x \xrightarrow{A} y$ (i.e., $I(x)R_AI(y)$), whereas $\mathcal{M} \not\models_I G$ for any $G \in \Delta$. By (S-C4) in Definition 3, since $I(x)R_AI(y)$, there exists a world $w$ such that $I(x)R_Aw$ and $wR_AI(y)$. Let us now consider a function $I'$ defined as follows: $I'(z) = w$ and $I'(k) = I(k)$ for all labels $k \neq z$. Since $z$ is a label not occurring in the conclusion of the rule, it immediately follows that $\mathcal{M} \models_{I'} F$ for every $F \in \Gamma'$, $\mathcal{M} \models_{I'} x \xrightarrow{A} y$ (since $I'(x) = I(x), I'(y) = I(y)$ and $I(x)R_AI(y)$), $\mathcal{M} \models_{I'} x \xrightarrow{A} z$ (since $I'(z) = w$ and, as observed above, $I(x)R_Aw$), $\mathcal{M} \models_{I'} z \xrightarrow{A} y$ (since $wR_AI(y)$), whereas $\mathcal{M} \not\models_I G$ for any $G \in \Delta$, against the validity of the premise. □

Completeness is an easy consequence of the admissibility of *cut*[6]. By cut we mean the following rule:

$$\frac{\Gamma \vdash \Delta, F \qquad\qquad \Gamma, F \vdash \Delta}{\Gamma \vdash \Delta}\ (cut)$$

where $F$ is any labelled formula. The standard proof of admissibility of cut proceeds by a double induction over the complexity of $F$ and the sum of the heights of the derivations of the two premises of $(cut)$, in the sense that we replace one cut by one or several cuts on formulas of smaller complexity, or on sequents derived by shorter derivations.

**Theorem 9.** *If $\Gamma \vdash \Delta, F$ and $\Gamma, F \vdash \Delta$ are derivable in $\mathcal{S}_{\mathsf{Cond}_{\mathrm{ACL}}}$, so is $\Gamma \vdash \Delta$, i.e. the rule $(cut)$ is admissible in $\mathcal{S}_{\mathsf{Cond}_{\mathrm{ACL}}}$.*

*Proof.* By double induction on the complexity of the cut formula and on the sum of the heights of the premises of the cut inference. To make the schema of the proof clear, we define: $c_F$ as the complexity of $F$, i.e. $c_F = cp(F)$; $h_1$ as the height of the derivation

[6] It is worth noticing that one can give a semantic proof of completeness, however as a difference with modal logics, the proof is considerably more complex and require nonetheless the cut rule (see [27] for a semantic completeness proof of a tableau calculus for the conditional logic CK). We explain intuitively the difficulty. The usual way to prove completeness semantically is by contraposition, that is to say to extract a counter model from a failed branch of a (suitable) proof tree. To this purpose one needs to "saturate" a branch by applying the rules as much as possible. However the model being constructed must satisfy the normality condition, i.e. if $[|A|] = [|A'|]$ then it must be $R_A = R_{A'}$, or equivalently, the selection function must be well-defined on arbitrary subsets of worlds. To ensure this property, a simple branch saturation is not enough. One has to consider in the saturation process other formulas not occurring in the branch and use inevitably the cut rule to make the whole construction work, the latter being a kind of Henkin construction. For this reason we prefer the much simpler syntactic proof.

of $\Gamma \vdash \Delta, F$; $h_2$ as the height of the derivation of $\Gamma, F \vdash \Delta$. For the base case of the induction on the complexity of the cut formula, we consider the cases in which $c_F = 2$ (its minimal value), namely the cases $F = x : P$ with $P \in ATM$, $F = x : \bot$, and $F = y \geq x$. Then, we fix $c_F$ and we prove the base case(s) for the induction on the sum of the height of the premises, namely we prove the theorem for the cases in which $h_1 = 0$ or $h_2 = 0$ (or both), i.e. (at least) one of the two premises is an axiom. For the inductive steps, we replace the initial cut by one or more applications of cut either (i) on formulas $G$ such that $cp(G) < c_F$, i.e. we apply the inductive hypothesis on the complexity of the cut formula to prove that, if $\Gamma' \vdash \Delta', G$ and $\Gamma', G \vdash \Delta'$ are derivable, so is $\Gamma' \vdash \Delta'$, or (ii) on the same formula $F$ but cutting sequents $\Gamma' \vdash \Delta', F$ and $\Gamma', F \vdash \Delta'$ whose derivations have heights $h_1'$ and $h_2'$ such that $h_1' + h_2' < h_1 + h_2$.

We analize each case in detail.

• Base case of the induction on the complexity $c_F$ of the cut formula: $c_F = 2$. As mentioned above, we consider three subcases: 1. the cut formula $F$ is an order formula $y \geq x$; 2. the cut formula $F$ is a world formula $x : P$ where $P$ is an atom ($P \in ATM$); 3. the cut formula $F$ is $x : \bot$.

1. We proceed by induction on the sum of the heights of the derivations of $\Gamma \vdash \Delta, y \geq x$ and $\Gamma, y \geq x \vdash \Delta$ to show that also $\Gamma \vdash \Delta$ is derivable.
   For the base of the induction, suppose that (at least) one of the premises of $(cut)$ is an instance of an axiom. For instance, assume that $\Gamma \vdash \Delta, y \geq x$ is an axiom (the other half is symmetric). We distinguish the following subcases: (i) $u : \bot \in \Gamma$, and we immediately conclude that also $\Gamma \vdash \Delta$ is an instance of $(AX_\bot)$; (ii) $u \geq u \in \Delta$, then we immediately get that also $\Gamma \vdash \Delta$ is an instance of $(AX_\geq)$; (iii) $F \in \Gamma \cap \Delta$, and obviously $\Gamma \vdash \Delta$ is an instance of $(AX)$ too; (iv) $y \geq x \in \Gamma$, i.e. $\Gamma = \Gamma', y \geq x$: in this case, the right premise of $(cut)$ is $\Gamma', y \geq x, y \geq x \vdash \Delta$, and we can conclude that also $\Gamma', y \geq x \vdash \Delta$ is derivable since contraction is admissible (Lemma 8).
   For the inductive step, let us consider the last rule, say R, applied in the derivation of $\Gamma \vdash \Delta, y \geq x$. We distinguish two subcases:
   – the rule R is $(EQ)$, i.e. the derivation is ended as follows:

$$\dfrac{u : A \vdash u : A' \qquad\qquad u : A' \vdash u : A}{\Gamma', v \xrightarrow{A} z \vdash \Delta', v \xrightarrow{A'} z, y \geq x} \ (EQ)$$

   In this case, since order formulas do not play any role in an application of $(EQ)$ (only transition formulas are involved), we show that also $\Gamma \vdash \Delta = \Gamma', v \xrightarrow{A} z \vdash \Delta', v \xrightarrow{A'} z$ is derivable by means of the following derivation:

$$\dfrac{u : A \vdash u : A' \qquad\qquad u : A' \vdash u : A}{\Gamma', v \xrightarrow{A} z \vdash \Delta', v \xrightarrow{A'} z} \ (EQ)$$

   – the rule R is different from $(EQ)$: we just observe that no rule of $\mathcal{S}_{\mathsf{Cond}_{\mathsf{ACL}}}$ has an order formula on the right hand side of a sequent as a principal formula. Furthermore, in all the rules, $y \geq x$ is copied into the premise(s). Therefore, we can apply the inductive hypothesis on the sum of the heights of the premises of $(cut)$ to the sequent $\Gamma, y \geq x \vdash \Delta$ and the premise(s) of $\Gamma \vdash \Delta, y \geq x$, then we conclude by an application of R. As an example, consider the case R is $(ID)$, the other cases are similar and left to the reader. The derivation is as follows:

$$\dfrac{(1)\ \Gamma', x \xrightarrow{A} y, y : A \vdash \Delta, y \geq x}{\Gamma', x \xrightarrow{A} y \vdash \Delta, y \geq x}\ (ID)$$

Since weakening is height-preserving admissible (Lemma 5), since $\Gamma', x \xrightarrow{A} y, y \geq x \vdash \Delta$ is derivable, there is also a derivation, of at most the same height, of $(2)\ \Gamma', x \xrightarrow{A} y, y : A, y \geq x \vdash \Delta$. We can then apply the inductive hypothesis on the sum of the heights to cut $(1)$ and $(2)$, and we obtain a derivation also for $\Gamma', x \xrightarrow{A} y, y : A \vdash \Delta$, from which we conclude by an application of $(ID)$.

2. As in the previous case, we proceed by induction on the sum of the heights of the derivations of $\Gamma \vdash \Delta, x : P$ and $\Gamma, x : P \vdash \Delta$.
For the base case, we have that (at least) one of the two sequents is an axiom, suppose $\Gamma, x : P \vdash \Delta$ (the other half is symmetric). As in the previous case, the proof is straightforward in cases $u : \bot \in \Gamma$, $F \in \Gamma \cap \Delta$ and $u \geq u \in \Delta$. In case $x : P \in \Delta$, i.e. $\Delta = \Delta', x : P$, we observe that the left premise of $(cut)$ has the form $\Gamma \vdash \Delta', x : P, x : P$ and, by contraction (Lemma 8), we conclude that $\Gamma \vdash \Delta', x : P$ is derivable.
We proceed similarly to case 1 also for the inductive step. First of all, we consider the rule R ending the derivation of $\Gamma \vdash \Delta, x : P$. We distinguish two cases:
   - the rule R is $(EQ)$, i.e. the derivation is ended as follows:

$$\dfrac{u : A \vdash u : A' \qquad\qquad u : A' \vdash u : A}{\Gamma', v \xrightarrow{A} z \vdash \Delta', v \xrightarrow{A'} z, x : P}\ (EQ)$$

   As we have done for the corresponding case in 1, we immediately get that $\Gamma \vdash \Delta = \Gamma', v \xrightarrow{A} z \vdash \Delta', v \xrightarrow{A'} z$ is derivable by an application of $(EQ)$ to $u : A \vdash u : A'$ and $u : A' \vdash u : A$, since $x : P$ does not play any role in the application of $(EQ)$, which involves only transition formulas;
   - the rule R is different from $(EQ)$: as in case 1, we just observe that no rule of $\mathcal{S}\mathsf{Cond}_{\mathsf{ACL}}$ has a formula $x : P$, where $P$ is an atom, on the right hand side of a sequent as a principal formula. Furthermore, in all the rules, $x : P$ is copied into the premise(s). We conclude exactly as we made in case 1, namely we apply the inductive hypothesis on the sum of the heights of the premises to cut $\Gamma, x : P \vdash \Delta$ and the premise(s) of $\Gamma \vdash \Delta, x : P$, then we conclude by an application of R. As an example, consider the case R is $(Unit)$, the other cases are similar and left to the reader. The derivation is as follows:

$$\dfrac{(1)\ \Gamma', y \geq x, x \xrightarrow{A} y \vdash \Delta, x : P}{\Gamma', x \xrightarrow{A} y \vdash \Delta, x : P}\ (Unit)$$

Since weakening is height-preserving admissible (Lemma 5), since $\Gamma', x \xrightarrow{A} y, x : P \vdash \Delta$ is derivable, we have a derivation of at most the same height of $(2)$ $\Gamma', y \geq x, x \xrightarrow{A} y, x : P \vdash \Delta$. We apply the inductive hypothesis to cut $(1)$ and $(2)$, then we obtain a derivation of $\Gamma', y \geq x, x \xrightarrow{A} y \vdash \Delta$, from which we conclude by an application of $(Unit)$.

3. In this case, since $\Gamma \vdash \Delta, x : \bot$ is derivable, we immediately conclude that $\Gamma \vdash \Delta$ is derivable from Lemma 12.

• Base case of the induction on the sum of the heights of the premises of the cut inference: (at least) one of the two premises of $(cut)$ is an axiom. We have several subcases: 1. $F \in \Gamma \cap \Delta$ or $x : \bot \in \Gamma$: in this case, it immediately follows that also $\Gamma \vdash \Delta$ is derivable and we are done. 2. $\Gamma \vdash \Delta, F$ is an axiom since $F = x \geq x$: consider the other sequent $\Gamma, x \geq x \vdash \Delta$. Since it is derivable, by Lemma 11, also $\Gamma \vdash \Delta$ is derivable, and we are done. 3. $\Gamma \vdash \Delta, F$ is an axiom since $F \in \Gamma$, that is to say $\Gamma = \Gamma', F$: in this case, the other premise of $(cut)$ is $\Gamma', F, F \vdash \Delta$ and, by Lemma 8, we can conclude that also $\Gamma', F \vdash \Delta$ is derivable, thus $\Gamma \vdash \Delta$ is derivable, and we are done. 4. $\Gamma, F \vdash \Delta$ is an axiom since $F = x : \bot$: in this case, the other premise corresponds to $\Gamma \vdash \Delta, x : \bot$ and, by Lemma 12, we have that also $\Gamma \vdash \Delta$ is derivable. 5. $\Gamma, F \vdash \Delta$ is an axiom since $F \in \Delta$, i.e. $\Delta = \Delta', F$: similarly to case 3, we have that the other premise corresponds to $\Gamma \vdash \Delta', F, F$, and we conclude that $\Gamma \vdash \Delta', F$=$\Gamma \vdash \Delta$ is derivable since contraction is admissible (Lemma 8).

• Inductive step: we distinguish the following two cases:

(case 1) the last step of *one* of the two premises is obtained by a rule in which $F$ is *not* the principal formula. We further distinguish two subcases: (i) one of the sequents, say $\Gamma, F \vdash \Delta$ is obtained by the $(EQ)$ rule, where $F$ is not principal. The premises of $(EQ)$ do not contain $F$, since this rule only involves two transition formulas belonging to $\Gamma$ and $\Delta$. Therefore, we have a proof of $\Gamma \vdash \Delta$ by a direct application of $(EQ)$ to it; (ii) the sequent where $F$ is not principal is derived by any rule R, except the $(EQ)$ rule. This case is standard, we can permute R over the cut, i.e. we cut the premise(s) of R and then we apply R to the result of cut. We present two examples, namely the case in which R is $(DT)$ applied to the left premise of $(cut)$ and the case in which R is $(Unit)$ applied to the right premise of $(cut)$. The other cases are very similar and left to the reader. For $(DT)$, consider a derivation ending as follows:

$$\dfrac{\dfrac{\begin{array}{l}(i)\ \Gamma', z \geq y, x \xrightarrow{A} y \vdash \Delta, F, z : B \\ (ii)\ \Gamma', z \geq y, x \xrightarrow{A} y, x \xrightarrow{A \wedge B} z \vdash \Delta, F\end{array}}{\Gamma', z \geq y, x \xrightarrow{A} y \vdash \Delta, F}\,(DT) \qquad (iii)\ \Gamma', z \geq y, x \xrightarrow{A} y, F \vdash \Delta}{\Gamma', z \geq y, x \xrightarrow{A} y \vdash \Delta}\,(cut)$$

By $(iii)$ and Lemma 5, we have derivations of no greater heights of $(iii')$ $\Gamma', z \geq y, x \xrightarrow{A} y, F \vdash \Delta, z : B$ and $(iii'')$ $\Gamma', z \geq y, x \xrightarrow{A} y, x \xrightarrow{A \wedge B} z, F \vdash \Delta$. We can apply the inductive hypothesis on the sum of the heights of the premises, namely we cut $(i)$ with $(iii')$ obtaining a derivation of $(iv)$ $\Gamma', z \geq y, x \xrightarrow{A} y \vdash \Delta, z : B$, and we cut

$(ii)$ with $(iii'')$ obtaining a derivation of $(v)\ \Gamma', z \geq y, x \xrightarrow{A} y, x \xrightarrow{A \wedge B} z \vdash \Delta$. From $(iv)$ and $(v)$ we conclude by an application of $(DT)$ as follows:

$$\dfrac{(iv)\ \Gamma', z \geq y, x \xrightarrow{A} y \vdash \Delta, z : B \qquad (v)\ \Gamma', z \geq y, x \xrightarrow{A} y, x \xrightarrow{A \wedge B} z \vdash \Delta}{\Gamma', z \geq y, x \xrightarrow{A} y \vdash \Delta}\ (DT)$$

Notice that we have applied the inductive hypothesis on the height since the cut formula is $F$ itself. Concerning $(Unit)$, consider a derivation ended as follows:

$$\dfrac{(i)\ \Gamma', x \xrightarrow{A} y \vdash \Delta, F \qquad \dfrac{(ii)\ \Gamma', y \geq x, x \xrightarrow{A} y, F \vdash \Delta}{\Gamma', x \xrightarrow{A} y, F \vdash \Delta}\ (Unit)}{\Gamma', x \xrightarrow{A} y \vdash \Delta}\ (cut)$$

Since weakening is heigh-preserving admissible (Lemma 5), we have a derivation of $(i')\ \Gamma', y \geq x, x \xrightarrow{A} y \vdash \Delta, F$. Also in this case, we apply the inductive hypothesis on the height to cut $(i')$ and $(ii)$, then we conclude by an application of $(Unit)$:

$$\dfrac{\dfrac{(i')\ \Gamma', y \geq x, x \xrightarrow{A} y \vdash \Delta, F \qquad (ii)\ \Gamma', y \geq x, x \xrightarrow{A} y, F \vdash \Delta}{\Gamma', y \geq x, x \xrightarrow{A} y \vdash \Delta}\ (cut)}{\Gamma', x \xrightarrow{A} y \vdash \Delta}\ (Unit)$$

(case 2) $F$ is the principal formula in the last step of *both* derivations of the premises of the cut inference. There are thirteen subcases: $F$ is introduced a) by $(\wedge R)$ - $(\wedge L)$, b) by $(\vee R)$ - $(\vee L)$, c) by $(\rightarrow R)$ - $(\rightarrow L)$, d) by $($ **says** $R)$ - $($ **says** $L)$, e) by $(EQ)$ on the left and on the right, f) by $(EQ)$ on the left and by $(Unit)$ on the right, g) by $(EQ)$ on the left and by $(ID)$ on the right, h) by $(EQ)$ on the left and by $(C)$ on the right, i) by $(EQ)$ on the left and by $(DT)$ on the right, j) by $(EQ)$ on the left and by $(CA - conv)$ on the right, k) by $(EQ)$ on the left and by $(C4)$ on the right, l) by $(EQ)$ on the left and by $(I)$ on the right, m) by $(EQ)$ on the left and by $(INT)$ on the right. The list is exhaustive. Notice that the rules $(CA)$ and $(MON)$ are not involved in any case, since there is no principal formula $F$ in their conclusions. The same for $(TR)$ and $(ATM)$, since there is no rule having a formula $y \geq x$ (respectively, $x : P$ with $P \in ATM$) on the right hand side of its conclusion as a principal formula. We present each case in detail:

- a) We have the following derivation:

$$\dfrac{\dfrac{(1)\ \Gamma \vdash \Delta, x : \alpha \qquad (2)\ \Gamma \vdash \Delta, x : \beta}{\Gamma \vdash \Delta, x : \alpha \wedge \beta}\ (\wedge R) \qquad \dfrac{(3)\ \Gamma, x : \alpha, x : \beta \vdash \Delta}{\Gamma, x : \alpha \wedge \beta \vdash \Delta}\ (\wedge L)}{\Gamma \vdash \Delta}\ (cut)$$

  Since weakening is admissible (Lemma 5), we have a derivation of no greater height than $(1)$ also for $(1')\ \Gamma, x : \beta \vdash \Delta, x : \alpha$. We conclude by applying two times the inductive hypothesis, cutting formulas whose complexity is lower than the one of $x : \alpha \wedge \beta$, as follows:

$$\dfrac{(2)\ \Gamma \vdash \Delta, x:\beta \qquad \dfrac{(1')\ \Gamma, x:\beta \vdash \Delta, x:\alpha \qquad (3)\ \Gamma, x:\alpha, x:\beta \vdash \Delta}{\Gamma, x:\beta \vdash \Delta}\,(cut)}{\Gamma \vdash \Delta}\,(cut)$$

- b) We have the following derivation:

$$\dfrac{\dfrac{(1)\ \Gamma \vdash \Delta, x:\alpha, x:\beta}{\Gamma \vdash \Delta, x:\alpha \vee \beta}\,(\vee R) \qquad \dfrac{(2)\ \Gamma, x:\alpha \vdash \Delta \qquad (3)\ \Gamma, x:\beta \vdash \Delta}{\Gamma, x:\alpha \vee \beta \vdash \Delta}\,(\vee L)}{\Gamma \vdash \Delta}\,(cut)$$

By weakening (Lemma 5), we have a derivation of $(2')$ $\Gamma, x:\alpha \vdash \Delta, x:\beta$ of no greater height than $(2)$. As in case a), we conclude by applying two times the inductive hypothesis on the complexity of the cut formula, replacing the initial cut as follows:

$$\dfrac{\dfrac{(1)\ \Gamma \vdash \Delta, x:\alpha, x:\beta \qquad (2')\ \Gamma, x:\alpha \vdash \Delta, x:\beta}{\Gamma \vdash \Delta, x:\beta}\,(cut) \qquad (3)\ \Gamma, x:\beta \vdash \Delta}{\Gamma \vdash \Delta}\,(cut)$$

- c) We have the following derivation:

$$\dfrac{\dfrac{(1)\ \Gamma, z \geq x, z:\alpha \vdash \Delta, z:\beta}{(5)\ \Gamma \vdash \Delta, x:\alpha \rightarrow \beta}\,(\rightarrow R) \qquad \dfrac{\begin{array}{c}(2)\ \Gamma, x:\alpha \rightarrow \beta \vdash \Delta, y \geq x\\ (3)\ \Gamma, x:\alpha \rightarrow \beta \vdash \Delta, y:\alpha\\ (4)\ \Gamma, x:\alpha \rightarrow \beta, y:\beta \vdash \Delta\end{array}}{\Gamma, x:\alpha \rightarrow \beta \vdash \Delta}\,(\rightarrow L)}{\Gamma \vdash \Delta}\,(cut)$$

First, observe that the label $z$ in the premise of $(\rightarrow R)$ is new, i.e. it does not occur in the conclusion of such rule. By Lemma 6, we have a derivation of no greater height than $(1)$ also of $(1')$ $\Gamma, y \geq x, y:\alpha \vdash \Delta, y:\beta$. Since weakening is height-preserving admissibile, we have derivations for $(5')$ $\Gamma \vdash \Delta, x:\alpha \rightarrow \beta, y \geq x$, $(5'')$ $\Gamma \vdash \Delta, x:\alpha \rightarrow \beta, y:\alpha$, and $(5''')$ $\Gamma, y:\beta \vdash \Delta, x:\alpha \rightarrow \beta$, whose heights are no greater than the height of $(5)$. By applying the inductive hypothesis on the height of the derivations, we can cut $(2)$ and $(5')$, obtaining a derivation of $(6)$ $\Gamma \vdash \Delta, y \geq x$, $(3)$ and $(5'')$, obtaining a derivation of $(7)$ $\Gamma \vdash \Delta, y:\alpha$, $(3)$ and $(5''')$, obtaining a derivation of $(8)$ $\Gamma, y:\beta \vdash \Delta$. By weakening (Lemma 5), we have also derivations of $(7')$ $\Gamma, y \geq x \vdash \Delta, y:\alpha$ and $(8')$ $\Gamma, y \geq x, y:\alpha, y:\beta \vdash \Delta$. We replace the initial cut with three cuts on formulas whose complexity is lower than the one of $x:\alpha \rightarrow \beta$, as follows:

$$\dfrac{(6)\ \Gamma \vdash \Delta, y \geq x \qquad \dfrac{(7')\ \Gamma, y \geq x \vdash \Delta, y:\alpha \qquad \dfrac{\begin{array}{c}(1')\ \Gamma, y \geq x, y:\alpha \vdash \Delta, y:\beta\\ (8')\ \Gamma, y \geq x, y:\alpha, y:\beta \vdash \Delta\end{array}}{\Gamma, y \geq x, y:\alpha \vdash \Delta}\,(cut)}{\Gamma, y \geq x \vdash \Delta}\,(cut)}{\Gamma \vdash \Delta}\,(cut)$$

- d) We have the following derivation:

$$\dfrac{\dfrac{(1)\ \Gamma, x \xrightarrow{A} z \vdash \Delta, z : \gamma}{(4)\ \Gamma \vdash \Delta, x : A \textbf{ says } \gamma}\,(\textbf{ says } R) \qquad \dfrac{(2)\ \Gamma, x : A \textbf{ says } \gamma \vdash \Delta, x \xrightarrow{A} y \quad (3)\ \Gamma, x : A \textbf{ says } \gamma, y : \gamma \vdash \Delta}{\Gamma, x : A \textbf{ says } \gamma \vdash \Delta}\,(\textbf{ says } L)}{\Gamma \vdash \Delta}\,(cut)$$

First, observe that, since the label $z$ does not occur in the conclusion of ( **says** $R$), by Lemma 6 we have a derivation of $(1')$ $\Gamma, x \xrightarrow{A} y \vdash \Delta, y : \gamma$. By weakening (Lemma 5), we have derivations of $(4')$ $\Gamma \vdash \Delta, x : A$ **says** $\gamma, x \xrightarrow{A} y$ and $(4'')$ $\Gamma, y : \gamma \vdash \Delta, x : A$ **says** $\gamma$, whose heights are no greater than the one for $(4)$. We apply the inductive hypothesis on the height of the derivations to cut $(2)$ and $(4')$, obtaining $(5)$ $\Gamma \vdash \Delta, x \xrightarrow{A} y$, and to cut $(3)$ with $(4'')$, obtaining $(6)$ $\Gamma, y : \gamma \vdash \Delta$. By Lemma 5 we have also a derivation for $(6')$ $\Gamma, x \xrightarrow{A} y, y : \gamma \vdash \Delta$. We conclude as follows by applying two times the inductive hypothesis on the complexity of the cut formula:

$$\dfrac{(5)\ \Gamma \vdash \Delta, x \xrightarrow{A} y \qquad \dfrac{(1')\ \Gamma, x \xrightarrow{A} y \vdash \Delta, y : \gamma \qquad (6')\ \Gamma, x \xrightarrow{A} y, y : \gamma \vdash \Delta}{\Gamma, x \xrightarrow{A} y \vdash \Delta}\,(cut)}{\Gamma \vdash \Delta}\,(cut)$$

- e) We have the following derivation:

$$\dfrac{\dfrac{(1)\ u : B \vdash u : A \qquad (2)\ u : A \vdash u : B}{\Gamma', x \xrightarrow{B} y \vdash \Delta', x \xrightarrow{C} y, x \xrightarrow{A} y}\,(EQ) \qquad \dfrac{(3)\ u : A \vdash u : C \qquad (4)\ u : C \vdash u : A}{\Gamma', x \xrightarrow{B} y, x \xrightarrow{A} y \vdash \Delta', x \xrightarrow{C} y}\,(EQ)}{\Gamma', x \xrightarrow{B} y \vdash \Delta', x \xrightarrow{C} y}\,(cut)$$

By Lemma 5, from $(1)$ we obtain a proof of $(1')$ $u : B \vdash u : A, u : C$, from $(2)$ we obtain a proof of $(2')$ $u : A, u : C \vdash u : B$, from $(3)$ we obtain a proof of $(3')$ $u : A, u : B \vdash u : C$, and from $(4)$ we obtain a proof of $(4')$ $u : C \vdash u : A, u : B$. We replace the initial cut with the following derivation, where $(cut)$ is eliminable by applying the inductive hypothesis on the complexity of the cut formula:

$$\dfrac{\dfrac{\begin{array}{c}(1')\ u : B \vdash u : A, u : C \\ (3')\ u : A, u : B \vdash u : C\end{array}}{u : B \vdash u : C}\,(cut) \qquad \dfrac{\begin{array}{c}(2')\ u : A, u : C \vdash u : B \\ (4')\ u : C \vdash u : A, u : B\end{array}}{u : C \vdash u : B}\,(cut)}{\Gamma', x \xrightarrow{B} y \vdash \Delta', x \xrightarrow{C} y}\,(EQ)$$

- f) The derivation is ended as follows:

$$\dfrac{\dfrac{u : A \vdash u : A' \qquad u : A' \vdash u : A}{(2)\ \Gamma', x \xrightarrow{A'} y \vdash \Delta, x \xrightarrow{A} y}\,(EQ) \qquad \dfrac{(1)\ \Gamma', x \xrightarrow{A'} y, x \xrightarrow{A} y, y \geq x \vdash \Delta}{\Gamma', x \xrightarrow{A'} y, x \xrightarrow{A} y \vdash \Delta}\,(Unit)}{\Gamma', x \xrightarrow{A'} y \vdash \Delta}\,(cut)$$

By Lemma 5, we have a derivation of height no greater than $(2)$ of $(2')$ $\Gamma', x \xrightarrow{A'} y, y \geq x \vdash \Delta, x \xrightarrow{A} y$. We can replace the initial cut by applying the inductive hypothesis on the height of the derivations to cut $(2')$ and $(1)$ as follows:

$$\dfrac{\dfrac{(2')\ \Gamma', x \xrightarrow{A'} y, y \geq x \vdash \Delta, x \xrightarrow{A} y \qquad (1)\ \Gamma', x \xrightarrow{A'} y, x \xrightarrow{A} y, y \geq x \vdash \Delta}{\Gamma', x \xrightarrow{A'} y, y \geq x \vdash \Delta}\,(cut)}{\Gamma', x \xrightarrow{A'} y \vdash \Delta}\,(Unit)$$

- g) The derivation we are considering is as follows:

$$\dfrac{\dfrac{u : A \vdash u : A' \qquad (1)\ u : A' \vdash u : A}{(3)\ \Gamma', x \xrightarrow{A'} y \vdash \Delta, x \xrightarrow{A} y}\,(EQ) \qquad \dfrac{(2)\ \Gamma', x \xrightarrow{A'} y, x \xrightarrow{A} y, y : A \vdash \Delta}{\Gamma', x \xrightarrow{A'} y, x \xrightarrow{A} y \vdash \Delta}\,(ID)}{\Gamma', x \xrightarrow{A'} y \vdash \Delta}\,(cut)$$

First of all, by the height-preserving admissibility of label substitution (Lemma 6), we have a derivation of no greater height of $(1)$ for $(1')$ $y : A' \vdash y : A$. Moreover, by weakening (Lemma 5), we have derivations for $(3')$ $\Gamma', x \xrightarrow{A'} y, y : A, y : A' \vdash \Delta, x \xrightarrow{A} y$ of no greater height with respect to $(3)$, for $(2')$ $\Gamma', x \xrightarrow{A'} y, x \xrightarrow{A} y, y : A, y : A' \vdash \Delta$ of no greater height with respect to $(2)$, and of $(1'')$ $\Gamma', x \xrightarrow{A'} y, y : A' \vdash \Delta, y : A$ of no greater height with respect to $(1')$. We can conclude by replacing the initial cut by the two following cuts:

$$\dfrac{\dfrac{(1'')\ \Gamma', x \xrightarrow{A'} y, y : A' \vdash \Delta, y : A \qquad \dfrac{\begin{array}{c}(3')\ \Gamma', x \xrightarrow{A'} y, y : A, y : A' \vdash \Delta, x \xrightarrow{A} y\\ (2')\ \Gamma', x \xrightarrow{A'} y, x \xrightarrow{A} y, y : A, y : A' \vdash \Delta\end{array}}{\Gamma', x \xrightarrow{A'} y, y : A, y : A' \vdash \Delta}\,(cut)}{\Gamma', x \xrightarrow{A'} y, y : A' \vdash \Delta}\,(cut)}{\Gamma', x \xrightarrow{A'} y \vdash \Delta}\,(ID)$$

The upper cut (between $(3')$ and $(2)$) can be eliminated by applying the inductive hypothesis on the height of the premises, whereas the lower one can be removed by applying the inductive hypothesis on the complexity of the cut formula.

- h) We have the following derivation:

$$\dfrac{\dfrac{(I)\ u : A' \vdash u : A \qquad (II)\ u : A \vdash u : A'}{\Gamma', z \geq y, x \xrightarrow{A'} y \vdash \Delta, x \xrightarrow{A} y}\,(EQ) \qquad \dfrac{(1)\ \Gamma', z \geq y, x \xrightarrow{A'} y, x \xrightarrow{A} y, z \xrightarrow{A} z \vdash \Delta}{(2)\ \Gamma', z \geq y, x \xrightarrow{A'} y, x \xrightarrow{A} y \vdash \Delta}\,(C)}{\Gamma', z \geq y, x \xrightarrow{A'} y \vdash \Delta}\,(cut)$$

This case is more complicated: intuitively, we cannot conclude as in the previous case g) by cutting $(1)$ and the conclusion of $(EQ)$ (and using necessary weakenings), because of the presence of $z \xrightarrow{A} z$. More precisely, the application of the inductive hypothesis on the sum of the heights of the derivations would lead to a derivation of $\Gamma', z \geq y, x \xrightarrow{A'} y, z \xrightarrow{A} z \vdash \Delta$, from which we are not able to conclude.

In order to tackle this problem, we first show that the sequent $(2')$ $\Gamma', z \geq y, x \xrightarrow{A'} y, x \xrightarrow{A'} y \vdash \Delta$ is derivable, that is to say we replace $A$ with the equivalent formula $A'$ in one or more transition formulas[7] in $(2)$, since $(I)$ and $(II)$ are derivable. Given this, we immediately conclude that $\Gamma', z \geq y, x \xrightarrow{A'} y \vdash \Delta$ is derivable since contraction is admissible (Lemma 8). We proceed by induction on the height of the derivation of $(2)$. The base case corresponds to the situation in which $(2)$ is an instance of the axioms: since axioms do not involve transition formulas, we can easily observe that either there is a formula $G$ such that $G \in \Gamma' \cap \Delta$ or $z \geq y \in \Delta$ or, for some $w$, $w : \bot \in \Gamma'$ or $w \geq w \in \Delta$. In all these cases, it immediately follows that also $(2')$ $\Gamma', z \geq y, x \xrightarrow{A'} y, x \xrightarrow{A'} y \vdash \Delta$ is an axiom and we are done. For the inductive step, we consider each rule ending the derivation of $(2)$. We distinguish two subcases:

- the derivation of $(2)$ is ended by an application of $(EQ)$ as follows:

$$\dfrac{(III)\, u : A \vdash u : B \qquad\qquad (IV)\, u : B \vdash u : A}{(2)\ \Gamma', z \geq y, x \xrightarrow{A'} y, x \xrightarrow{A} y \vdash \Delta', x \xrightarrow{B} y}\,(EQ)$$

  Since weakening is admissible (Lemma 5), from $(I)$ we obtain a derivation of $(I')$ $u : A' \vdash u : A, u : B$, from $(II)$ we obtain a proof of $(II')$ $u : B, u : A \vdash u : A'$, from $(III)$ we obtain a proof of $(III')$ $u : A, u : A' \vdash u : B$ and from $(IV)$ we obtain a proof of $(IV')$ $u : B \vdash u : A, u : A'$. We conclude that $(2')$ is derivable as follows:

$$\dfrac{\dfrac{\begin{array}{c}(I')\, u : A' \vdash u : A, u : B \\ (III')\, u : A, u : A' \vdash u : B\end{array}}{u : A' \vdash u : B}\,(cut) \qquad \dfrac{\begin{array}{c}(IV')\, u : B \vdash u : A, u : A' \\ (II')\, u : B, u : A \vdash u : A'\end{array}}{u : B \vdash u : A'}\,(cut)}{(2')\ \Gamma', z \geq y, x \xrightarrow{A'} y, x \xrightarrow{A'} y \vdash \Delta', x \xrightarrow{B} y}\,(EQ)$$

  Notice that the two cuts can be eliminated by applying the inductive hypothesis on the complexity of the cut formula: indeed, the cut formula is $u : A$, whose complexity is lower than the one of $x \xrightarrow{A} y$;

- the derivation of $(2)$ is ended by an application of $(ID)$ as follows:

$$\dfrac{(3)\ \Gamma', z \geq y, x \xrightarrow{A'} y, x \xrightarrow{A} y, y : A \vdash \Delta}{(2)\ \Gamma', z \geq y, x \xrightarrow{A'} y, x \xrightarrow{A} y \vdash \Delta}\,(ID)$$

[7] In the general case, transition formulas can have the following forms: $u \xrightarrow{A} v$, $u \xrightarrow{A \vee B} v$, $u \xrightarrow{A \wedge B} v$.

First of all, we apply the inductive hypothesis to replace $A$ with $A'$ in $(3)$, obtaining a proof of $(3')$ $\Gamma', z \geq y, x \xrightarrow{A'} y, x \xrightarrow{A'} y, y : A \vdash \Delta$, then, by Lemma 5, we have a proof also for $(3'')$ $\Gamma', z \geq y, y : A', x \xrightarrow{A'} y, x \xrightarrow{A'} y, y : A \vdash \Delta$. By Lemma 6 and weakening (Lemma 5), from $(I)$ $u : A' \vdash u : A$ we obtain a proof of $(I')$ $\Gamma', z \geq y, y : A', x \xrightarrow{A'} y, x \xrightarrow{A'} y \vdash \Delta, y : A$. We apply the inductive hypothesis of cut to $(3'')$ and $(I')$, again on the complexity of the cut formula which is $y : A$, whose complexity is lower than the one of $x \xrightarrow{A} y$. We obtain a derivation of $\Gamma', z \geq y, y : A', x \xrightarrow{A'} y, x \xrightarrow{A'} y \vdash \Delta$, from which we conclude by an application of $(ID)$;

- the derivation of $(2)$ is ended by an application of $(DT)$ as follows:

$$\dfrac{(3)\ \Gamma', z \geq y, x \xrightarrow{A'} y, x \xrightarrow{A} y \vdash \Delta, z : B \qquad (4)\ \Gamma', z \geq y, x \xrightarrow{A'} y, x \xrightarrow{A} y, x \xrightarrow{A \wedge B} z \vdash \Delta}{(2)\ \Gamma', z \geq y, x \xrightarrow{A'} y, x \xrightarrow{A} y \vdash \Delta}\ (DT)$$

First of all, we show that $u : A \wedge B \vdash u : A' \wedge B$ and $u : A' \wedge B \vdash u : A \wedge B$ are derivable. Indeed, by Lemma 5, from $(I)$ and $(II)$ we have derivations for $(I')$ $u : A', u : B \vdash u : A$ and $(II')$ $u : A, u : B \vdash u : A'$. Moreover, $(5)$ $u : A, u : B \vdash u : B$ and $(6)$ $u : A', u : B \vdash u : B$ are derivable (they are instances of the axiom $(AX)$), from which we can build the following derivations:

$$\dfrac{\dfrac{(II')\ u : A, u : B \vdash u : A' \qquad (5)\ u : A, u : B \vdash u : B}{u : A, u : B \vdash u : A' \wedge B}\ (\wedge R)}{u : A \wedge B \vdash u : A' \wedge B}\ (\wedge L)$$

$$\dfrac{\dfrac{(I')\ u : A', u : B \vdash u : A \qquad (6)\ u : A', u : B \vdash u : B}{u : A', u : B \vdash u : A \wedge B}\ (\wedge R)}{u : A' \wedge B \vdash u : A \wedge B}\ (\wedge L)$$

Therefore, we can apply the inductive hypothesis to $(3)$, obtaining a proof of $(3')$ $\Gamma', z \geq y, x \xrightarrow{A'} y, x \xrightarrow{A'} y \vdash \Delta, z : B$, as well as to $(4)$ to obtain a proof of $(4')$ $\Gamma', z \geq y, x \xrightarrow{A'} y, x \xrightarrow{A'} y, x \xrightarrow{A' \wedge B} z \vdash \Delta$. We immediately conclude by an application of $(DT)$ to $(3')$ and $(4')$;

- the derivation of $(2)$ is ended by an application of $(CA-conv)$ as follows:

$$\dfrac{(3)\ \Gamma', z \geq y, x \xrightarrow{A'} y, x \xrightarrow{A} y, x \xrightarrow{A \vee B} z \vdash \Delta}{(2)\ \Gamma', z \geq y, x \xrightarrow{A'} y, x \xrightarrow{A} y \vdash \Delta}\ (CA-conv)$$

Similarly to the case of $(DT)$, we observe that also $u : A \vee B \vdash u : A' \vee B$ and $u : A' \vee B \vdash u : A \vee B$ are derivable, then we apply the inductive hypothesis on $(3)$ to obtain a proof of $\Gamma', z \geq y, x \xrightarrow{A'} y, x \xrightarrow{A'} y, x \xrightarrow{A' \vee B} z \vdash \Delta$, from which we conclude by an application of $(CA-conv)$;

- the last rule in the derivation of $(2)$ is different from $(EQ)$, $(ID)$, $(DT)$ and $(CA - conv)$: in all these cases, the transition formula $x \xrightarrow{A} y$ is copied into the premise(s). We can immediately conclude by first applying the inductive hypothesis, i.e. by replacing $A$ with $A'$, in such premise(s), and then by applying the same rule. As an example, let us consider a proof ended by an application of $(C4)$ as follows:

$$\dfrac{(3)\ \Gamma', z \geq y, x \xrightarrow{A'} y, x \xrightarrow{A} y, x \xrightarrow{A} w, w \xrightarrow{A} y \vdash \Delta}{(2)\ \Gamma', z \geq y, x \xrightarrow{A'} y, x \xrightarrow{A} y \vdash \Delta}\ (C4)$$

  We can apply the inductive hypothesis on $(3)$ to obtain a derivation of $(3')\ \Gamma', z \geq y, x \xrightarrow{A'} y, x \xrightarrow{A'} y, x \xrightarrow{A'} w, w \xrightarrow{A'} z \vdash \Delta$, from which we conclude by an application of $(C4)$.

– i) The derivation is as follows:

$$\dfrac{\dfrac{(1)\ u : A' \vdash u : A \qquad (2)\ u : A \vdash u : A'}{\Gamma', z \geq y, x \xrightarrow{A'} y \vdash \Delta, x \xrightarrow{A} y}\ (EQ) \qquad \dfrac{\begin{array}{c}\Gamma', z \geq y, x \xrightarrow{A'} y, x \xrightarrow{A} y \vdash \Delta, z : B \\ \Gamma', z \geq y, x \xrightarrow{A'} y, x \xrightarrow{A} y, x \xrightarrow{A \wedge B} z \vdash \Delta\end{array}}{(3)\ \Gamma', z \geq y, x \xrightarrow{A'} y, x \xrightarrow{A} y \vdash \Delta}\ (DT)}{\Gamma', z \geq y, x \xrightarrow{A'} y \vdash \Delta}\ (cut)$$

Since $(1)\ u : A' \vdash u : A$ and $(2)\ u : A \vdash u : A'$ are derivable, we can prove that also $(3')\ \Gamma', z \geq y, x \xrightarrow{A'} y, x \xrightarrow{A'} y \vdash \Delta$ is derivable. The proof is by induction on the height of the derivation of $(3)$, is exactly the same as the one proposed for case h) and it is therefore omitted. Since contraction is admissible (Lemma 8), we can immediately conclude from $(3')$.

– j) We have the following derivation:

$$\dfrac{\dfrac{u : A' \vdash u : A \qquad u : A \vdash u : A'}{\Gamma', x \xrightarrow{A'} y \vdash \Delta, x \xrightarrow{A} y}\ (EQ) \qquad \dfrac{\Gamma', x \xrightarrow{A'} y, x \xrightarrow{A} y, x \xrightarrow{A \vee B} y \vdash \Delta}{(1)\ \Gamma', x \xrightarrow{A'} y, x \xrightarrow{A} y \vdash \Delta}\ (CA - conv)}{\Gamma', x \xrightarrow{A'} y \vdash \Delta}\ (cut)$$

We proceed as in the previous cases h) and i) to prove that we have a derivation of $(1')\ \Gamma', x \xrightarrow{A'} y, x \xrightarrow{A'} y \vdash \Delta$. Since contraction is admissible (Lemma 8), we conclude that also $\Gamma', x \xrightarrow{A'} y \vdash \Delta$ is derivable.

– k) We are considering the following derivation:

$$\dfrac{\dfrac{u : A' \vdash u : A \qquad u : A \vdash u : A'}{\Gamma', x \xrightarrow{A'} y \vdash \Delta, x \xrightarrow{A} y}\ (EQ) \qquad \dfrac{\Gamma', x \xrightarrow{A'} y, x \xrightarrow{A} y, x \xrightarrow{A} z, z \xrightarrow{A} y \vdash \Delta}{(1)\ \Gamma', x \xrightarrow{A'} y, x \xrightarrow{A} y \vdash \Delta}\ (C4)}{\Gamma', x \xrightarrow{A'} y \vdash \Delta}\ (cut)$$

Also in this case we proceed similarly to what done for cases h), i) and j): by induction on the height of the derivation of $(1)$, we prove that there is a derivation of $\Gamma', x \xrightarrow{A'} y, x \xrightarrow{A'} y \vdash \Delta$, then we conclude by contraction (Lemma 8) that $\Gamma', x \xrightarrow{A'} y \vdash \Delta$ is derivable.

– l) We have the following derivation:

$$\dfrac{\dfrac{u : A' \vdash u : A \qquad u : A \vdash u : A'}{\Gamma', x \xrightarrow{A'} y, y \xrightarrow{B} z \vdash \Delta, x \xrightarrow{A} y}\,(EQ) \qquad \dfrac{\Gamma', x \xrightarrow{A'} y, x \xrightarrow{A} y, y \xrightarrow{B} z, x \xrightarrow{B} z \vdash \Delta}{(1)\ \Gamma', x \xrightarrow{A'} y, x \xrightarrow{A} y, y \xrightarrow{B} z \vdash \Delta}\,(I)}{\Gamma', x \xrightarrow{A'} y, y \xrightarrow{B} z \vdash \Delta}\,(cut)$$

As in the previous cases, we first show that $(1')$ $\Gamma', x \xrightarrow{A'} y, x \xrightarrow{A'} y, y \xrightarrow{B} z \vdash \Delta$ is derivable; again, the proof is by induction on the height of the derivation of $(1)$ and it makes use of the inductive hypothesis of cut on the complexity of the cut formula. We then conclude by contraction (Lemma 8) that $\Gamma', x \xrightarrow{A'} y, y \xrightarrow{B} z \vdash \Delta$ is derivable.

– m) We have the following derivation:

$$\dfrac{\dfrac{u : A \vdash u : A' \qquad u : A' \vdash u : A}{\Gamma', x \geq z, x \xrightarrow{A'} y \vdash \Delta, x \xrightarrow{A} y}\,(EQ) \qquad \dfrac{\Gamma', x \geq z, x \xrightarrow{A'} y, x \xrightarrow{A} y, z \xrightarrow{A} y \vdash \Delta}{(1)\ \Gamma', x \geq z, x \xrightarrow{A'} y, x \xrightarrow{A} y \vdash \Delta}\,(INT)}{\Gamma', x \geq z, x \xrightarrow{A'} y \vdash \Delta}\,(cut)$$

As in the previous cases, we first show that $(1')$ $\Gamma', x \geq z, x \xrightarrow{A'} y, x \xrightarrow{A'} y \vdash \Delta$ is derivable, then we conclude that $\Gamma', x \geq z, x \xrightarrow{A'} y \vdash \Delta$ is also derivable since contraction is admissible (Lemma 8). □

It is worth noticing that in the proof of Theorem 9 above, in cases h), i), j), k), l), and m), it is needed a property that, given that $u : A \vdash u : A'$ and $u : A' \vdash u : A$ are derivable, allows us to replace $A$ with $A'$ in one or more transition formulas $x \xrightarrow{A} y$ (resp. $x \xrightarrow{A \vee B} y$ or $x \xrightarrow{A \wedge B} y$) in a derivable sequent $\Gamma \vdash \Delta$. The proof of such property in turn requires $(cut)$ (see case h) as an example). As an alternative to the proof presented above, in order to prove the admissibility of cut for $\mathcal{S}_{\mathsf{Cond}_{\mathsf{ACL}}}$, we can proceed as done in [28] to deal with conditional logics containing the axiom (CEM) of *conditional excluded middle*. Let $\Gamma[x_i \xrightarrow{F} y_i] \vdash \Delta[u_j \xrightarrow{F} v_j]$ be a sequent containing *any* number of transitions labelled with the formula $F$, where $F$ is either $A$ or $A \wedge B$ or $A \vee B$; moreover, if $u : A \vdash u : A'$ and $u : A' \vdash u : A$ are derivable, we denote with $\Gamma^\star \vdash \Delta^\star$ the sequent obtained by replacing *any* number of transitions labelled with either $A$ or $A \wedge B$ or $A \vee B$ with the same transitions where $A$ is replaced by $A'$ in $\Gamma[x_i \xrightarrow{F} y_i] \vdash \Delta[u_j \xrightarrow{F} v_j]$. We can prove that cut is admissible by "splitting" the notion of cut in two propositions:

- (A) If $\varGamma \vdash \varDelta, F$ and $\varGamma, F \vdash \varDelta$ are derivable, so is $\varGamma \vdash \varDelta$, i.e. the rule $(cut)$ is admissible in $\mathcal{S}_{\mathsf{Cond}_{\mathrm{ACL}}}$ ;
- (B) if (I) $\varGamma[x_i \xrightarrow{F} y_i] \vdash \varDelta[u_j \xrightarrow{F} v_j]$ , (II) $u : A \vdash u : A'$ and (III) $u : A' \vdash u : A$ are derivable, then $\varGamma^\star \vdash \varDelta^\star$ is derivable.

The proof is by mutual induction between (A) and (B). The induction on (A) is, as in the proof of Theorem 9 above, a double induction on the complexity of the cut formula and on the sum of the heights of the premises of $(cut)$, whereas the induction on (B) is on the height of the derivation of (I). To prove (A) in the above mentioned cases from h) to m), we need to apply the inductive hypothesis on (B) to one of the premises of $(cut)$, and this is allowed since the height of such premise (say $h_2$) is lower than $h_1 + h_2$. To prove (B), in case the derivation of (I) $\varGamma[x_i \xrightarrow{F} y_i] \vdash \varDelta[u_j \xrightarrow{F} v_j]$ is ended by an application of either $(EQ)$ or $(ID)$, we need to apply the inductive hypothesis on (A) on the complexity of the cut formulas, and this is allowed since the cut formulas are subformulas of the initial $x \xrightarrow{F} y$.

Now we can prove the completeness of the calculus $\mathcal{S}_{\mathsf{Cond}_{\mathrm{ACL}}}$ :

**Theorem 10 (Completeness of $\mathcal{S}_{\mathsf{Cond}_{\mathrm{ACL}}}$ ).** *If a sequent $\varGamma \vdash \varDelta$ is valid in the sense of Definition 7, then $\varGamma \vdash \varDelta$ is derivable.*

*Proof.* We have to prove that the axioms are derivable and that the set of derivable formulas is closed under (MP), (RCEA), and (RCK).

First, we show a derivation in $\mathcal{S}_{\mathsf{Cond}_{\mathrm{ACL}}}$ of the axioms:

- (FALSE)

$$\dfrac{x \geq u, x : \bot \vdash x : \gamma}{\vdash u : \bot \to \gamma}\,(\to R)$$

- (THEN-1): by Lemma 10, we have that, given any formula $\alpha$, there is a derivation in $\mathcal{S}_{\mathsf{Cond}_{\mathrm{ACL}}}$ for $(i)$ $y \geq x, x \geq u, y : \beta, x : \alpha \vdash y : \alpha$. We can conclude as follows:

$$\dfrac{\dfrac{(i)\; y \geq x, x \geq u, y : \beta, x : \alpha \vdash y : \alpha}{x \geq u, x : \alpha \vdash x : \beta \to \alpha}\,(\to R)}{\vdash u : \alpha \to (\beta \to \alpha)}\,(\to R)$$

- (THEN-2)

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\begin{array}{c}\ldots, z \geq y \vdash z \geq y, \ldots\\ \ldots, z : \alpha \vdash \ldots, z : \alpha\end{array} \qquad \dfrac{\begin{array}{c}\ldots, z \geq x \vdash z \geq x, \ldots\\ \ldots, z : \alpha \vdash \ldots, z : \alpha\end{array} \qquad \dfrac{\begin{array}{c}\ldots \vdash z \geq z, \ldots\\ z : \beta, \ldots \vdash z : \beta, \ldots\\ z : \gamma, \ldots \vdash z : \gamma, \ldots\end{array}}{\ldots, z : \beta \to \gamma, z : \beta, z : \alpha \vdash \ldots, z : \gamma}\,(\to L)}{z \geq x, \ldots, z : \alpha, z : \beta, x : \alpha \to (\beta \to \gamma) \vdash \ldots, z : \gamma}\,(\to L)}{z \geq x, z \geq y, y \geq x, x \geq u, x : \alpha \to (\beta \to \gamma), y : \alpha \to \beta, z : \alpha \vdash z : \gamma}\,(\to L)}{z \geq y, y \geq x, x \geq u, x : \alpha \to (\beta \to \gamma), y : \alpha \to \beta, z : \alpha \vdash z : \gamma}\,(TR)}{y \geq x, x \geq u, x : \alpha \to (\beta \to \gamma), y : \alpha \to \beta \vdash y : \alpha \to \gamma}\,(\to R)}{x \geq u, x : \alpha \to (\beta \to \gamma) \vdash x : (\alpha \to \beta) \to (\alpha \to \gamma)}\,(\to R)}{\vdash u : (\alpha \to (\beta \to \gamma)) \to ((\alpha \to \beta) \to (\alpha \to \gamma))}\,(\to R)$$

- (AND-1), (AND-2) (the two cases are symmetric)

$$\dfrac{\dfrac{x \geq u, x : \alpha, x : \beta \vdash x : \alpha}{x \geq u, x : \alpha \wedge \beta \vdash x : \alpha}\,(\wedge L)}{\vdash u : \alpha \wedge \beta \rightarrow \alpha}\,(\rightarrow R)$$

- (AND-3): by Lemma 10, we have a derivation for $(ii)\ y \geq x, x \geq u, x : \alpha, y : \beta \vdash y : \alpha$, from which we conclude as follows:

$$\dfrac{\dfrac{\dfrac{(ii)\ y \geq x, x \geq u, x : \alpha, y : \beta \vdash y : \alpha \qquad y \geq x, x \geq u, x : \alpha, y : \beta \vdash y : \beta}{y \geq x, x \geq u, x : \alpha, y : \beta \vdash y : \alpha \wedge \beta}\,(\wedge R)}{x \geq u, x : \alpha \vdash x : \beta \rightarrow (\alpha \wedge \beta)}\,(\rightarrow R)}{\vdash u : \alpha \rightarrow (\beta \rightarrow (\alpha \wedge \beta))}\,(\rightarrow R)$$

- (OR-1), (OR-2) (the two cases are symmetric)

$$\dfrac{\dfrac{x \geq u, x : \alpha \vdash x : \alpha, x : \beta}{x \geq u, x : \alpha \vdash x : \alpha \vee \beta}\,(\vee R)}{\vdash u : \alpha \rightarrow \alpha \vee \beta}\,(\rightarrow R)$$

- (OR-3)

$$\dfrac{\dfrac{\dfrac{\dfrac{\begin{array}{c} z \geq y, \ldots z \geq y, z : \beta \\ \ldots, z : \beta \vdash z : \beta \end{array} \quad \dfrac{\dfrac{\dfrac{\begin{array}{c} \ldots z \geq x \vdash \ldots, z \geq x \\ \ldots, z : \alpha \vdash \ldots, z : \alpha \\ \ldots, z : \beta \vdash \ldots, z : \beta \end{array}}{z \geq x, x : \alpha \rightarrow \beta, \ldots, z : \alpha \vdash z : \gamma, z : \beta}\,(\rightarrow L)}{z \geq y, y \geq x, x : \alpha \rightarrow \beta, \ldots, z : \alpha \vdash z : \gamma, z : \beta}\,(TR) \qquad \ldots, z : \gamma \vdash z : \gamma, z : \beta}{z \geq y, y \geq x, x : \alpha \rightarrow \beta, \ldots, z : \alpha \vee \gamma \vdash z : \gamma, z : \beta}\,(\vee L)}{z \geq y, y \geq x, x \geq u, x : \alpha \rightarrow \beta, y : \gamma \rightarrow \beta, z : \alpha \vee \gamma \vdash z : \beta}\,(\rightarrow L)}{y \geq x, x \geq u, x : \alpha \rightarrow \beta, y : \gamma \rightarrow \beta \vdash y : \alpha \vee \gamma \rightarrow \beta}\,(\rightarrow R)}{x \geq u, x : \alpha \rightarrow \beta \vdash x : (\gamma \rightarrow \beta) \rightarrow (\alpha \vee \gamma \rightarrow \beta)}\,(\rightarrow R)}{\vdash u : (\alpha \rightarrow \beta) \rightarrow ((\gamma \rightarrow \beta) \rightarrow (\alpha \vee \gamma \rightarrow \beta))}\,(\rightarrow R)$$

- (K)

$$\dfrac{\dfrac{v : A \vdash v : A}{\ldots, y \xrightarrow{A} z \vdash z : \beta, y \xrightarrow{A} z}\,(EQ) \qquad \dfrac{\dfrac{\dfrac{v : A \vdash v : A}{\ldots, x \xrightarrow{A} z \vdash x \xrightarrow{A} z, z : \beta}\,(EQ) \quad \dfrac{\begin{array}{c}\ldots \vdash z : \beta, z \geq z \\ \ldots, z : \alpha \vdash z : \beta, z : \alpha \\ \ldots, z : \beta \vdash z : \beta\end{array}}{\ldots, z : \alpha \rightarrow \beta, z : \alpha \vdash z : \beta}\,(\rightarrow L)}{x \xrightarrow{A} z, y \geq x, y \xrightarrow{A} z, x : A \textbf{ says } (\alpha \rightarrow \beta), z : \alpha, \ldots \vdash z : \beta}\,(\textbf{ says } L)}{y \geq x, y \xrightarrow{A} z, x : A \textbf{ says } (\alpha \rightarrow \beta), z : \alpha, \ldots \vdash z : \beta}\,(INT)}{\dfrac{\dfrac{\dfrac{y \geq x, x \geq u, y \xrightarrow{A} z, x : A \textbf{ says } (\alpha \rightarrow \beta), y : A \textbf{ says } \alpha \vdash z : \beta}{y \geq x, x \geq u, x : A \textbf{ says } (\alpha \rightarrow \beta), y : A \textbf{ says } \alpha \vdash y : A \textbf{ says } \beta}\,(\textbf{ says } R)}{x \geq u, x : A \textbf{ says } (\alpha \rightarrow \beta) \vdash x : A \textbf{ says } \alpha \rightarrow A \textbf{ says } \beta}\,(\rightarrow R)}{\vdash u : A \textbf{ says } (\alpha \rightarrow \beta) \rightarrow (A \textbf{ says } \alpha \rightarrow A \textbf{ says } \beta)}\,(\rightarrow R)}\,(\textbf{ says } L)$$

– (CA): let us first observe that, since $A \vee B$ occurs in the left hand side of **says** in the initial formula, we have that $A \vee B \in \mathcal{L}_{\mathbf{P}}$. We have the following derivation:

$$\dfrac{\dfrac{\dfrac{\dfrac{\begin{array}{c}v : A \vdash v : A, v : B \\ v : B \vdash v : A, v : B\end{array}}{v : A \vee B \vdash v : A, v : B}\,(\vee L)}{v : A \vee B \vdash v : A \vee B}\,(\vee R)}{\ldots, x \xrightarrow{A \vee B} y \vdash y : \gamma, x \xrightarrow{A \vee B} y}\,(EQ) \quad \dfrac{\dfrac{v : A \vdash v : A}{\ldots x \xrightarrow{A} y}\,(EQ) \quad \ldots, y : \gamma \vdash y : \gamma}{\ldots, x \xrightarrow{A} y, x : A \textbf{ says } \gamma \vdash y : \gamma}\,(\textbf{ says } L) \quad \dfrac{\dfrac{v : B \vdash v : B}{\ldots x \xrightarrow{B} y}\,(EQ) \quad \ldots, y : \gamma \vdash y : \gamma}{\ldots, x \xrightarrow{B} y, x : B \textbf{ says } \gamma \vdash y : \gamma}\,(\textbf{ says } L}{\dfrac{\dfrac{\dfrac{x \geq u, x \xrightarrow{A \vee B} y, x : A \textbf{ says } \gamma, x : B \textbf{ says } \gamma \vdash y : \gamma}{x \geq u, x : A \textbf{ says } \gamma, x : B \textbf{ says } \gamma \vdash x : A \vee B \textbf{ says } \gamma}\,(\textbf{ says } R)}{x \geq u, x : A \textbf{ says } \gamma \wedge B \textbf{ says } \gamma \vdash x : A \vee B \textbf{ says } \gamma}\,(\wedge L)}{\vdash u : A \textbf{ says } \gamma \wedge B \textbf{ says } \gamma \rightarrow A \vee B \textbf{ says } \gamma}\,(\rightarrow R)}\,(CA)$$

– (CA-conv): similarly to the case of (CA), we observe that $A \vee B \in \mathcal{L}_{\mathbf{P}}$. We have the following derivation:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{v : A \vee B \vdash v : A \vee B}{\ldots, x \xrightarrow{A \vee B} y \vdash y : \gamma, x \xrightarrow{A \vee B} y}\,(EQ) \quad \ldots, y : \gamma \vdash y : \gamma}{x \geq u, x \xrightarrow{A} y, x \xrightarrow{A \vee B} y, x : A \vee B \textbf{ says } \gamma \vdash y : \gamma}\,(\textbf{ says } L)}{x \geq u, x \xrightarrow{A} y, x : A \vee B \textbf{ says } \gamma \vdash y : \gamma}\,(CA - conv)}{x \geq u, x : A \vee B \textbf{ says } \gamma \vdash x : A \textbf{ says } \gamma}\,(\textbf{ says } R)}{\vdash u : A \vee B \textbf{ says } \gamma \rightarrow A \textbf{ says } \gamma}\,(\rightarrow R)$$

- (Mon): similarly to the cases of (CA) and (CA-conv), we observe that $A \wedge B \in \mathcal{L}_{\mathbf{P}}$. We have the following derivation:

$$\dfrac{\dfrac{\dfrac{\dfrac{\begin{array}{c} v : A, v : B \vdash v : A \\ v : A, v : B \vdash v : B \end{array}}{v : A, v : B \vdash v : A \wedge B}\,(\wedge R)}{v : A \wedge B \vdash v : A \wedge B}\,(\wedge L)}{\ldots, x \overset{A \wedge B}{\longrightarrow} y \vdash y : \gamma, x \overset{A \wedge B}{\longrightarrow} y}\,(EQ) \qquad \dfrac{\dfrac{v : A \vdash v : A}{\ldots, x \overset{A}{\longrightarrow} y \vdash y : \gamma, x \overset{A}{\longrightarrow} y}\,(EQ) \qquad \ldots, y : \gamma \vdash y : \gamma}{\ldots, x \overset{A}{\longrightarrow} y, x \overset{B}{\longrightarrow} y, x : A \textbf{ says } \gamma \vdash y : \gamma}\,(\textbf{ says } L)}{\dfrac{\dfrac{x \geq u, x \overset{A \wedge B}{\longrightarrow} y, x : A \textbf{ says } \gamma \vdash y : \gamma}{x \geq u, x : A \textbf{ says } \gamma \vdash x : A \wedge B \textbf{ says } \gamma}\,(\textbf{ says } R)}{\vdash u : A \textbf{ says } \gamma \rightarrow A \wedge B \textbf{ says } \gamma}\,(\rightarrow R)}\,(MON)$$

- (DT): similarly to the case of (Mon), we observe that $A \wedge B \in \mathcal{L}_{\mathbf{P}}$. We have the following derivation:

$$\dfrac{\dfrac{\dfrac{\ldots, z : B \vdash z : \gamma, z : B \qquad \dfrac{\dfrac{v : A \wedge B \vdash v : A \wedge B}{\ldots, x \overset{A \wedge B}{\longrightarrow} z \vdash, z : \gamma, x \overset{A \wedge B}{\longrightarrow} z}\,(EQ) \qquad \ldots, z : \gamma \vdash z : \gamma}{\ldots, x \overset{A \wedge B}{\longrightarrow} z, x : A \wedge B \textbf{ says } \gamma \vdash z : \gamma}\,(\textbf{ says } L)}{z \geq y, x \geq u, x \overset{A}{\longrightarrow} y, x : A \wedge B \textbf{ says } \gamma, z : B \vdash z : \gamma}\,(DT)}{\dfrac{x \geq u, x \overset{A}{\longrightarrow} y, x : A \wedge B \textbf{ says } \gamma \vdash y : B \rightarrow \gamma}{x \geq u, x : A \wedge B \textbf{ says } \gamma \vdash x : A \textbf{ says } (B \rightarrow \gamma)}\,(\textbf{ says } R)}\,(\rightarrow R)}{\vdash u : A \wedge B \textbf{ says } \gamma \rightarrow (A \textbf{ says } (B \rightarrow \gamma))}\,(\rightarrow R)$$

- (ID)

$$\dfrac{\dfrac{x \overset{A}{\longrightarrow} y, y : A \vdash y : A}{x \overset{A}{\longrightarrow} y \vdash y : A}\,(ID)}{\vdash x : A \textbf{ says } A}\,(\textbf{ says } R)$$

- (UNIT): by Lemma 10 we have a derivation in $\mathcal{S}_{\mathsf{Cond}_{\mathsf{ACL}}}$ of $(iii)\ y \geq x, x \geq u, x : \gamma, x \overset{A}{\longrightarrow} y \vdash y : \gamma$, from which we conclude as follows:

$$\dfrac{\dfrac{\dfrac{(iii)\ y \geq x, x \geq u, x : \gamma, x \overset{A}{\longrightarrow} y \vdash y : \gamma}{x \geq u, x : \gamma, x \overset{A}{\longrightarrow} y \vdash y : \gamma}\,(Unit)}{x \geq u, x : \gamma \vdash x : A \textbf{ says } \gamma}\,(\textbf{ says } R)}{\vdash u : \gamma \rightarrow (A \textbf{ says } \gamma)}\,(\rightarrow R)$$

- (I)

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{v : A \vdash v : A \qquad v : A \vdash v : A}{\ldots, x \xrightarrow{A} z \vdash z : \gamma, x \xrightarrow{A} z}\,(EQ) \qquad \ldots, z : \gamma \vdash z : \gamma}{x \geq u, x \xrightarrow{B} y, y \xrightarrow{A} z, x \xrightarrow{A} z, x : A\ \textbf{says}\ \gamma \vdash z : \gamma}\,(\ \textbf{says}\ L)}{x \geq u, x \xrightarrow{B} y, y \xrightarrow{A} z, x : A\ \textbf{says}\ \gamma \vdash z : \gamma}\,(I)}{x \geq u, x \xrightarrow{B} y, x : A\ \textbf{says}\ \gamma \vdash y : A\ \textbf{says}\ \gamma}\,(\ \textbf{says}\ R)}{x \geq u, x : A\ \textbf{says}\ \gamma \vdash x : B\ \textbf{says}\ (A\ \textbf{says}\ \gamma)}\,(\ \textbf{says}\ R)}{\vdash u : (A\ \textbf{says}\ \gamma) \rightarrow (B\ \textbf{says}\ A\ \textbf{says}\ \gamma)}\,(\rightarrow R)$$

– (C)

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{v : A \vdash v : A \qquad v : A \vdash v : A}{\ldots, z \xrightarrow{A} z \vdash z : \gamma, z \xrightarrow{A} z}\,(EQ) \qquad \ldots, z : \gamma \vdash z : \gamma}{z \geq y, x \xrightarrow{A} y, z \xrightarrow{A} z, z : A\ \textbf{says}\ \gamma \vdash z : \gamma}\,(\ \textbf{says}\ L)}{z \geq y, x \xrightarrow{A} y, z : A\ \textbf{says}\ \gamma \vdash z : \gamma}\,(C)}{x \xrightarrow{A} y \vdash y : (A\ \textbf{says}\ \gamma) \rightarrow \gamma}\,(\rightarrow R)}{\vdash x : A\ \textbf{says}\ (A\ \textbf{says}\ \gamma \rightarrow \gamma)}\,(\ \textbf{says}\ R)$$

– (C4)

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{v : A \vdash v : A \qquad v : A \vdash v : A}{\ldots, x \xrightarrow{A} z \vdash y : \gamma, x \xrightarrow{A} z}\,(EQ) \qquad \dfrac{\dfrac{v : A \vdash v : A \qquad v : A \vdash v : A}{\ldots, z \xrightarrow{A} y \vdash y : \gamma, z \xrightarrow{A} y}\,(EQ) \qquad \ldots, y : \gamma \vdash y : \gamma}{\ldots, z \xrightarrow{A} y, z : A\ \textbf{says}\ \gamma \vdash y : \gamma}\,(\ \textbf{says}\ L)}{x \geq u, x \xrightarrow{A} y, x \xrightarrow{A} z, z \xrightarrow{A} y, x : A\ \textbf{says}\ (A\ \textbf{says}\ \gamma) \vdash y : \gamma}\,(\ \textbf{says}\ L)}{x \geq u, x \xrightarrow{A} y, x : A\ \textbf{says}\ (A\ \textbf{says}\ \gamma) \vdash y : \gamma}\,(C4)}{x \geq u, x : A\ \textbf{says}\ (A\ \textbf{says}\ \gamma) \vdash x : A\ \textbf{says}\ \gamma}\,(\ \textbf{says}\ R)}{\vdash u : (A\ \textbf{says}\ (A\ \textbf{says}\ \gamma)) \rightarrow (A\ \textbf{says}\ \gamma)}\,(\rightarrow R)$$

Let us now show that the set of derivable formulas is closed under (MP), (RCEA), and (RCK). For (MP), suppose we have a derivation for $(iv)\ \vdash x : \alpha$ and $(v)\ \vdash x : \alpha \rightarrow \beta$. Since weakening is admissible, we have that also $(iv')\ \vdash x : \alpha, x : \beta$ and $(v')\ x : \alpha \vdash x : \alpha \rightarrow \beta, x : \beta$ have a derivation in $\mathcal{S}_{\mathsf{Cond}_{\mathsf{ACL}}}$. Since $(cut)$ is admissible, we can conclude that $\vdash x : \beta$ is derivable as follows:

$$\dfrac{(iv')\ \vdash x : \alpha, x : \beta \qquad \dfrac{(v')x : \alpha \vdash x : \alpha \rightarrow \beta, x : \beta \qquad \dfrac{\begin{array}{c} x : \alpha \rightarrow \beta, x : \alpha \vdash x : \beta, x \geq x \\ x : \alpha \rightarrow \beta, x : \alpha \vdash x : \beta, x : \alpha \\ x : \alpha \rightarrow \beta, x : \alpha, x : \beta \vdash x : \beta \end{array}}{x : \alpha \rightarrow \beta, x : \alpha \vdash x : \beta}\,(\rightarrow L)}{x : \alpha \vdash x : \beta}\,(cut)}{\vdash x : \beta}\,(cut)$$

For (RCEA), we proceed as follows. As usual, $\vdash A \leftrightarrow B$ is a shorthand for $\vdash A \rightarrow B$ and $\vdash B \rightarrow A$. Suppose we have a derivation for $\vdash v : A \rightarrow B$ and for $\vdash v : B \rightarrow A$. By Lemma 9, we have also derivations for $v : A \vdash v : B$ and $v : B \vdash v : A$. The following derivation shows that also $\vdash u : (A \textbf{ says } \gamma) \rightarrow (B \textbf{ says } \gamma)$ is derivable in $\mathcal{S}_{\mathsf{Cond}_{\text{ACL}}}$ (the other half is symmetric):

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{v : A \vdash v : B \qquad\qquad v : B \vdash v : A}{x \geq u, x : A \textbf{ says } \gamma, x \xrightarrow{B} y \vdash y : \gamma, x \xrightarrow{A} y}\,(EQ) \qquad \ldots, y : \gamma \vdash y : \gamma}{x \geq u, x : A \textbf{ says } \gamma, x \xrightarrow{B} y \vdash y : \gamma}\,(\textbf{ says } L)}{x \geq u, x : A \textbf{ says } \gamma \vdash x : B \textbf{ says } \gamma}\,(\textbf{ says } R)}{\vdash u : (A \textbf{ says } \gamma) \rightarrow (B \textbf{ says } \gamma)}\,(\rightarrow R)}{}$$

For (RCK), suppose there is a derivation for $\vdash y : \alpha \rightarrow \beta$. By Lemma 9, there is also a derivation for $(vi)\; y : \alpha \vdash y : \beta$ and, by weakening, of $(vi')\; x \geq u, x : A \textbf{ says } \alpha, x \xrightarrow{A} y, y : \alpha \vdash y : \beta$, from which we conclude:

$$\dfrac{\dfrac{\dfrac{\ldots x \xrightarrow{A} y \vdash x \xrightarrow{A} y, \ldots \qquad (vi')\; x \geq u, x : A \textbf{ says } \alpha, x \xrightarrow{A} y, y : \alpha \vdash y : \beta}{x \geq u, x : A \textbf{ says } \alpha, x \xrightarrow{A} y \vdash y : \beta}\,(\textbf{ says } L)}{x \geq u, x : A \textbf{ says } \alpha \vdash x : A \textbf{ says } \beta}\,(\textbf{ says } R)}{\vdash u : (A \textbf{ says } \alpha) \rightarrow (A \textbf{ says } \beta)}\,(\rightarrow R)$$

□

Completeness of $\mathcal{S}_{\mathsf{Cond}_{\text{ACL}}}$ with respect to the models of the respective logic in Definitions 2 and 3 immediately follows from the completeness of the axiomatization with respect to the semantics, shown in Theorems 4, 5, 6, and 7. We have that a formula $\varphi \in \mathcal{L}$ is valid if and only if the sequent $\vdash u : \varphi$ has a derivation in $\mathcal{S}_{\mathsf{Cond}_{\text{ACL}}}$ .

### 5.3 Decidability and complexity of $\mathsf{Cond}_{\mathbf{ACL}}^{\mathbf{UC}}$

In this section we focus on the logic $\mathsf{Cond}_{\text{ACL}}^{\mathbf{UC}}$ , for which we are able to describe a decision procedure $\widehat{\mathcal{S}_{\mathsf{Cond}_{\text{ACL}}^{\mathbf{UC}}}}$ (starting from $\mathcal{S}_{\mathsf{Cond}_{\text{ACL}}^{\mathbf{UC}}}$ ) and to give an explicit complexity bound for it. For the calculi for the variants $\mathsf{Cond}_{\text{ACL}}^{\mathbf{U4}}$ , $\mathsf{Cond}_{\text{ACL}}^{\mathbf{IC}}$ , and $\mathsf{Cond}_{\text{ACL}}^{\mathbf{I4}}$ , termination is an open problem at present, and we plan to study it in future work.

In general, cut-freeness alone does not ensure the termination of proof search in a sequent calculus; the presence of labels and of rules such as ( **says** $L$), $(\rightarrow L)$, $(Unit)$, $(ID), \ldots$, which increase the complexity of the sequent in a backward proof search, are potential causes of a non-terminating proof search. However, we can prove that the above mentioned "critical" rules can be applied in a controlled way, then the rules introduce only a finite number of labels.

First of all, by Proposition 3, the condition (S-DT) can be expressed as

$$\forall t, s \in S, \text{ if } sR_A t \text{ and } t \in [|B|], \text{ then } sR_{A \wedge B} t \qquad \text{(S-DT)}$$

As a consequence, the calculus $\widehat{\mathcal{S}_{\mathsf{Cond}_{\mathbf{UC}_{\mathrm{ACL}}}}}$ replaces the rule $(DT)$ in Figure 3 with the following one:

$$\dfrac{\Gamma, x \xrightarrow{A} y \vdash \Delta, y : B \qquad \Gamma, x \xrightarrow{A} y, x \xrightarrow{A \wedge B} y \vdash \Delta}{\Gamma, x \xrightarrow{A} y \vdash \Delta}\,(DT)$$

where $A \wedge B \in \mathcal{L}_{\mathbf{P}}$.

Let us now consider a first source of non-termination, namely the possible generation of an infinite branch due to the generation of infinitely-many labels, for instance introduced by a sequence of applications of $(\rightarrow L)$, $(\rightarrow R)$ and $(TR)$. As an example, consider the following derivation (in the applications of $(\rightarrow L)$ we only show the premise in the middle):

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\vdots}{w \geq z, z \geq x, z \geq y, y \geq x, x \geq u, x : (A_4 \rightarrow A_3) \rightarrow A_2, y : A_1, z : A_4, w : A_4 \vdash y : B, z : A_3, w : A_3}\,(TR)}{z \geq x, z \geq y, y \geq x, x \geq u, x : (A_4 \rightarrow A_3) \rightarrow A_2, y : A_1, z : A_4 \vdash y : B, z : A_3, z : A_4 \rightarrow A_3}\,(\rightarrow R)}{z \geq x, z \geq y, y \geq x, x \geq u, x : (A_4 \rightarrow A_3) \rightarrow A_2, y : A_1, z : A_4 \vdash y : B, z : A_3}\,(\rightarrow L)}{z \geq y, y \geq x, x \geq u, x : (A_4 \rightarrow A_3) \rightarrow A_2, y : A_1, z : A_4 \vdash y : B, z : A_3}\,(TR)}{y \geq x, x \geq u, x : (A_4 \rightarrow A_3) \rightarrow A_2, y : A_1 \vdash y : B, y : A_4 \rightarrow A_3}\,(\rightarrow R)}{y \geq x, x \geq u, x : (A_4 \rightarrow A_3) \rightarrow A_2, y : A_1 \vdash y : B}\,(\rightarrow L)}{x \geq u, x : (A_4 \rightarrow A_3) \rightarrow A_2 \vdash x : A_1 \rightarrow B}\,(\rightarrow R)}{\vdash u : ((A_4 \rightarrow A_3) \rightarrow A_2) \rightarrow (A_1 \rightarrow B)}\,(\rightarrow R)$$

The problem is exactly the same that affects calculi for intuitionistic propositional logic in [20], as well as labelled calculi for modal logics K4 and S4 in [32], where specific rules are devoted to capture the transitivity of the order relation $\leq$ as well as of the accessibility relation $R$.

In our calculus $\mathcal{S}_{\mathsf{Cond}_{\mathbf{UC}_{\mathrm{ACL}}}}$, the same problem is extended to the interplay between the rules ( **says** $L$), ( **says** $R$), $(INT)$ and $(Unit)$, as shown in the following example (again, we only present one branch of the tree):

$$
\begin{array}{cl}
\vdots & \\ \hline
x \xrightarrow{A} w, \ldots, x : A \,\mathbf{says}\, ((A \,\mathbf{says}\, B) \to \bot), w : (A \,\mathbf{says}\, B) \to \bot \vdash y : C, z : B, w : B & (\to L) \\ \hline
x \xrightarrow{A} w, z \geq x, z \geq y, y \geq x, z \xrightarrow{A} w, y \xrightarrow{A} z, \ldots, x : A \,\mathbf{says}\, ((A \,\mathbf{says}\, B) \to \bot) \vdash y : C, z : B, w : B & (\,\mathbf{says}\, L) \\ \hline
z \geq x, z \geq y, y \geq x, z \xrightarrow{A} w, y \xrightarrow{A} z, \ldots, x : A \,\mathbf{says}\, ((A \,\mathbf{says}\, B) \to \bot) \vdash y : C, z : B, w : B & (INT) \\ \hline
z \geq y, y \geq x, z \xrightarrow{A} w, y \xrightarrow{A} z, \ldots, x : A \,\mathbf{says}\, ((A \,\mathbf{says}\, B) \to \bot) \vdash y : C, z : B, w : B & (TR) \\ \hline
y \geq x, z \xrightarrow{A} w, y \xrightarrow{A} z, \ldots, x : A \,\mathbf{says}\, ((A \,\mathbf{says}\, B) \to \bot) \vdash y : C, z : B, w : B & (Unit) \\ \hline
\ldots, x : A \,\mathbf{says}\, ((A \,\mathbf{says}\, B) \to \bot), z : (A \,\mathbf{says}\, B) \to \bot \vdash y : C, z : B, z : A \,\mathbf{says}\, B & (\,\mathbf{says}\, R) \\ \hline
\ldots, x : A \,\mathbf{says}\, ((A \,\mathbf{says}\, B) \to \bot), z : (A \,\mathbf{says}\, B) \to \bot \vdash y : C, z : B & (\to L) \\ \hline
y \geq x, x \xrightarrow{A} z, x \xrightarrow{A} y, y \xrightarrow{A} z, x : A \,\mathbf{says}\, ((A \,\mathbf{says}\, B) \to \bot), \ldots \vdash y : C, z : B & (\,\mathbf{says}\, L) \\ \hline
y \geq x, x \xrightarrow{A} y, y \xrightarrow{A} z, x : A \,\mathbf{says}\, ((A \,\mathbf{says}\, B) \to \bot), \ldots \vdash y : C, z : B & (INT) \\ \hline
x \xrightarrow{A} y, y \xrightarrow{A} z, x : A \,\mathbf{says}\, ((A \,\mathbf{says}\, B) \to \bot), \ldots \vdash y : C, z : B & (Unit) \\ \hline
x \geq u, x \xrightarrow{A} y, x : A \,\mathbf{says}\, ((A \,\mathbf{says}\, B) \to \bot), y : (A \,\mathbf{says}\, B) \to \bot \vdash y : C, y : A \,\mathbf{says}\, B & (\,\mathbf{says}\, R) \\ \hline
x \geq u, x \xrightarrow{A} y, x : A \,\mathbf{says}\, ((A \,\mathbf{says}\, B) \to \bot), y : (A \,\mathbf{says}\, B) \to \bot \vdash y : C & (\to L) \\ \hline
x \geq u, x \xrightarrow{A} y, x : A \,\mathbf{says}\, ((A \,\mathbf{says}\, B) \to \bot) \vdash y : C & (\,\mathbf{says}\, L) \\ \hline
x \geq u, x : A \,\mathbf{says}\, ((A \,\mathbf{says}\, B) \to \bot) \vdash x : A \,\mathbf{says}\, C & (\,\mathbf{says}\, R) \\ \hline
\vdash u : (A \,\mathbf{says}\, ((A \,\mathbf{says}\, B) \to \bot)) \to (A \,\mathbf{says}\, C) & (\to R)
\end{array}
$$

In order to tackle this problem, we adopt a standard technique, based on the observation that each infinite sequence of labels is *periodic*, that is to say there are two worlds $x$ and $y$ such that $y \geq x$ ($x \xrightarrow{A} y$, respectively) and, for all formulas $\phi$, $\phi$ holds in the world represented by $x$ if and only if $\phi$ holds in the world represented by $y$. To ensure termination, we impose a restriction on the application of the rules $(\to R)$ and ( **says** $R$). Given a sequent $\Gamma \vdash \Delta$ and two labels $x$ and $y$ such that $y \geq x \in \Gamma$, we define the distance $d(y, x)$ as the length of the *longest* sequence of formulas in $\Gamma$ "connecting" the two labels, i.e. $d(y, x) = n$ if $y \circ z_1, z_1 \circ z_2, \ldots, z_{n-1} \circ x \in \Gamma$, with $\circ \in \{\geq, \xrightarrow{A_i}\}$[8] is the longest path between $y$ and $x$ in $\Gamma$. Given a derivation starting with $\vdash u : \phi$, let $\tau$ be the height of the parse tree of $\phi$. We show that we can restrict the application of $(\to R)$ to $\Gamma \vdash \Delta, x : \alpha \to \beta$ (of ( **says** $R$) to $\Gamma \vdash \Delta, x : \alpha$ **says** $\beta$, respectively) to the case in which $d(x, u) \leq \tau$, that is to say it is useless to introduce a new label when the distance between $x$ and $u$ is higher than the height of the parse tree of the initial formula.

We only sketch the argument that allows us to restrict the application of $(\to R)$ and ( **says** $R$) as stated above. A detailed discussion can be found in [16]. Let us first prove that the following rule:

[8] In computing $d(y, x)$ we take into account both *order formulas* and *transition formulas*. As mentioned, this is due to the presence of $(Unit)$, which implies that the former is a superset of the latter.

$$\dfrac{\Gamma, x : \alpha \to \beta \vdash \Delta, y \geq x \qquad \Gamma, x : \alpha \to \beta, y : \alpha \to \beta \vdash \Delta, y : \alpha \qquad \Gamma, x : \alpha \to \beta, y : \alpha \to \beta, y : \beta \vdash \Delta}{\Gamma, x : \alpha \to \beta \vdash \Delta}\ (\widetilde{\to L})$$

is admissible in $\mathcal{S}_{\mathsf{Cond}^{\mathbf{UC}}_{\mathrm{ACL}}}$ , that is to say:

**Lemma 13.** *If the following sequents:*

1. $\Gamma, x : \alpha \to \beta \vdash \Delta, y \geq x$
2. $\Gamma, x : \alpha \to \beta, y : \alpha \to \beta \vdash \Delta, y : \alpha$
3. $\Gamma, x : \alpha \to \beta, y : \alpha \to \beta, y : \beta \vdash \Delta$

*are derivable in* $\mathcal{S}_{\mathit{Cond}^{\mathbf{UC}}_{ACL}}$ *, then also the sequent* $\Gamma, x : \alpha \to \beta \vdash \Delta$ *is derivable in* $\mathcal{S}_{\mathit{Cond}^{\mathbf{UC}}_{ACL}}$ *.*

*Proof.* First of all, we prove that the sequent $\Gamma, x : \alpha \to \beta \vdash \Delta, x : \top \to (\alpha \to \beta)$ is derivable in $\mathcal{S}_{\mathsf{Cond}^{\mathbf{UC}}_{\mathrm{ACL}}}$ . This is shown by the following derivation:

$$\dfrac{\dfrac{\dfrac{\dfrac{\ldots, z \geq x \vdash \ldots, z \geq x \qquad \ldots, z : \alpha \vdash \ldots, z : \alpha \qquad \ldots, z : \beta \vdash \ldots, z : \beta}{\Gamma, z \geq x, y \geq x, z \geq y, x : \alpha \to \beta, y : \top, z : \alpha \vdash \Delta, z : \beta}\ (\to L)}{\Gamma, y \geq x, z \geq y, x : \alpha \to \beta, y : \top, z : \alpha \vdash \Delta, z : \beta}\ (TR)}{\Gamma, y \geq x, x : \alpha \to \beta, y : \top \vdash \Delta, y : \alpha \to \beta}\ (\to R)}{\Gamma, x : \alpha \to \beta \vdash \Delta, x : \top \to (\alpha \to \beta)}\ (\to R)$$

By the admissibility of weakening (Theorem 5), we have a derivation in $\mathcal{S}_{\mathsf{Cond}^{\mathbf{UC}}_{\mathrm{ACL}}}$ for $(i)$ $\Gamma, x : \alpha \to \beta \vdash \Delta, y : \alpha, x : \top \to (\alpha \to \beta)$ and for $(ii)$ $\Gamma, x : \alpha \to \beta, y : \beta \vdash \Delta, x : \top \to (\alpha \to \beta)$.

Again by weakening, since 1. is derivable, also $(1')$ $\Gamma, x : \alpha \to \beta, x : \top \to (\alpha \to \beta) \vdash \Delta, y : \alpha, y \geq x$ and $(1'')$ $\Gamma, x : \alpha \to \beta, x : \top \to (\alpha \to \beta), y : \beta \vdash \Delta, y \geq x$ are derivable in $\mathcal{S}_{\mathsf{Cond}^{\mathbf{UC}}_{\mathrm{ACL}}}$ . The same for $(2')$ $\Gamma, x : \alpha \to \beta, y : \alpha \to \beta, x : \top \to (\alpha \to \beta) \vdash \Delta, y : \alpha$ and $(3')$ $\Gamma, x : \alpha \to \beta, y : \alpha \to \beta, x : \top \to (\alpha \to \beta), y : \beta \vdash \Delta$. Since $\top$ is an abbreviation for $P \to P$, it immediately follows that $(*)$ $\Gamma, x : \alpha \to \beta, x : \top \to (\alpha \to \beta) \vdash \Delta, y : \alpha, y : \top$ and $(**)$ $\Gamma, x : \alpha \to \beta, x : \top \to (\alpha \to \beta), y : \beta \vdash \Delta, y : \top$ are derivable in $\mathcal{S}_{\mathsf{Cond}^{\mathbf{UC}}_{\mathrm{ACL}}}$ .

Since $(cut)$ is admissible (Theorem 9), we can prove that the sequent $(a)$ $\Gamma, x : \alpha \to \beta \vdash \Delta, y : \alpha$ is derivable in $\mathcal{S}_{\mathsf{Cond}^{\mathbf{UC}}_{\mathrm{ACL}}}$ :

$$\dfrac{(i)\ \Gamma, x : \alpha \to \beta \vdash \Delta, y : \alpha, x : \top \to (\alpha \to \beta) \qquad \dfrac{\begin{matrix}(1')\ \Gamma, x : \alpha \to \beta, x : \top \to (\alpha \to \beta) \vdash \Delta, y : \alpha, y \geq x \\ (*)\ \Gamma, x : \alpha \to \beta, x : \top \to (\alpha \to \beta) \vdash \Delta, y : \alpha, y : \top \\ (2')\ \Gamma, x : \alpha \to \beta, y : \alpha \to \beta, x : \top \to (\alpha \to \beta) \vdash \Delta, y : \alpha\end{matrix}}{\Gamma, x : \alpha \to \beta, x : \top \to (\alpha \to \beta) \vdash \Delta, y : \alpha}\ (\to L)}{(a)\ \Gamma, x : \alpha \to \beta \vdash \Delta, y : \alpha}\ (cut)$$

Again, since $(cut)$ is admissible, we prove that $(b)\ \Gamma, x : \alpha \rightarrow \beta, y : \beta \vdash \Delta$ is derivable in $\mathcal{S}_{\mathrm{Cond}^{\mathbf{UC}}_{\mathrm{ACL}}}$ :

$$\dfrac{(ii)\ \Gamma, x : \alpha \rightarrow \beta, y : \beta \vdash \Delta, x : \top \rightarrow (\alpha \rightarrow \beta) \qquad \dfrac{\begin{array}{c}(1'')\ \Gamma, x : \alpha \rightarrow \beta, x : \top \rightarrow (\alpha \rightarrow \beta), y : \beta \vdash \Delta, y \geq x \\ (**)\ \Gamma, x : \alpha \rightarrow \beta, x : \top \rightarrow (\alpha \rightarrow \beta), y : \beta \vdash \Delta, y : \top \\ (3')\ \Gamma, x : \alpha \rightarrow \beta, y : \alpha \rightarrow \beta, x : \top \rightarrow (\alpha \rightarrow \beta), y : \beta \vdash \Delta\end{array}}{\Gamma, x : \alpha \rightarrow \beta, x : \top \rightarrow (\alpha \rightarrow \beta), y : \beta \vdash \Delta}\,(\rightarrow L)}{(b)\ \Gamma, x : \alpha \rightarrow \beta, y : \beta \vdash \Delta}\,(cut)$$

From 1., $(a)$ and $(b)$ we conclude by an application of $(\rightarrow L)$. □

Analogously, we show that the following rule is also admissible in $\mathcal{S}_{\mathrm{Cond}^{\mathbf{UC}}_{\mathrm{ACL}}}$ :

$$\dfrac{\Gamma, x : A\ \textbf{says}\ \alpha \vdash \Delta, x \xrightarrow{A} y \qquad \Gamma, x : A\ \textbf{says}\ \alpha, y : A\ \textbf{says}\ \alpha, y : \alpha \vdash \Delta}{\Gamma, x : A\ \textbf{says}\ \alpha \vdash \Delta}\,(\widetilde{\textbf{says}\ L})$$

**Lemma 14.** *If* $(1)\ \Gamma, x : A\ \textbf{says}\ \alpha \vdash \Delta, x \xrightarrow{A} y$ *and* $(2)\ \Gamma, x : A\ \textbf{says}\ \alpha, y : A\ \textbf{says}\ \alpha, y : \alpha \vdash \Delta$ *are derivable in* $\mathcal{S}_{\mathit{Cond}^{\mathbf{UC}}_{\mathit{ACL}}}$ *, then also* $\Gamma, x : A\ \textbf{says}\ \alpha \vdash \Delta$ *is derivable in* $\mathcal{S}_{\mathit{Cond}^{\mathbf{UC}}_{\mathit{ACL}}}$ *.*

*Proof.* Let us first prove that the sequent $(i)\ \Gamma, x : A\ \textbf{says}\ \alpha \vdash \Delta, x : A\ \textbf{says}\ (A\ \textbf{says}\ \alpha)$ has a derivation in $\mathcal{S}_{\mathrm{Cond}^{\mathbf{UC}}_{\mathrm{ACL}}}$ , as shown by the following derivation:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\ldots, x \xrightarrow{A} z \vdash \ldots, x \xrightarrow{A} z \qquad \ldots, z : \alpha \vdash \Delta, z : \alpha}{\Gamma, x : A\ \textbf{says}\ \alpha, z \geq y, x \xrightarrow{A} z, x \xrightarrow{A} y, y \xrightarrow{A} z \vdash \Delta, z : \alpha}\,(\textbf{says}\ L)}{\Gamma, x : A\ \textbf{says}\ \alpha, y \geq x, x \xrightarrow{A} y, y \xrightarrow{A} z \vdash \Delta, z : \alpha}\,(INT)}{\Gamma, x : A\ \textbf{says}\ \alpha, x \xrightarrow{A} y, y \xrightarrow{A} z \vdash \Delta, z : \alpha}\,(Unit)}{\Gamma, x : A\ \textbf{says}\ \alpha, x \xrightarrow{A} y \vdash \Delta, y : A\ \textbf{says}\ \alpha}\,(\textbf{says}\ R)}{(i)\ \Gamma, x : A\ \textbf{says}\ \alpha \vdash \Delta, x : A\ \textbf{says}\ (A\ \textbf{says}\ \alpha)}\,(\textbf{says}\ R)$$

Since weakening is admissible in $\mathcal{S}_{\mathrm{Cond}^{\mathbf{UC}}_{\mathrm{ACL}}}$ (Theorem 5), from $(i)$ we obtain a derivation also for $(ii)\ \Gamma, x : A\ \textbf{says}\ \alpha, y : \alpha \vdash \Delta, x : A\ \textbf{says}\ (A\ \textbf{says}\ \alpha)$.

Again, since weakening is admissible in $\mathcal{S}_{\mathrm{Cond}^{\mathbf{UC}}_{\mathrm{ACL}}}$ , from $(1)$ we obtain a derivation of $(1')\ \Gamma, x : A\ \textbf{says}\ \alpha, x : A\ \textbf{says}\ (A\ \textbf{says}\ \alpha), y : \alpha \vdash \Delta, x \xrightarrow{A} y$, and from $(2)$ we obtain a derivation for $(2')\ \Gamma, x : A\ \textbf{says}\ \alpha, y : A\ \textbf{says}\ \alpha, x : A\ \textbf{says}\ (A\ \textbf{says}\ \alpha), y : \alpha \vdash \Delta$. Since $(cut)$ is admissible (Theorem 9), we can conclude as follows:

$$\dfrac{(1)\ \Gamma, x : A\ \textbf{says}\ \alpha \vdash \Delta, x \xrightarrow{A} y \qquad \dfrac{\begin{array}{c}(ii)\ \Gamma, x : A\ \textbf{says}\ \alpha, y : \alpha \vdash \\ \Delta, x : A\ \textbf{says}\ (A\ \textbf{says}\ \alpha)\end{array} \qquad \dfrac{\begin{array}{c}(1')\ \Gamma, x : A\ \textbf{says}\ \alpha, x : A\ \textbf{says}\ (A\ \textbf{says}\ \alpha), y : \alpha \vdash \Delta, x \xrightarrow{A} y \\ (2')\ \Gamma, x : A\ \textbf{says}\ \alpha, y : A\ \textbf{says}\ \alpha, x : A\ \textbf{says}\ (A\ \textbf{says}\ \alpha), y : \alpha \vdash \Delta\end{array}}{\Gamma, x : A\ \textbf{says}\ \alpha, x : A\ \textbf{says}\ (A\ \textbf{says}\ \alpha), y : \alpha \vdash \Delta}\,(\textbf{says}\ L)}{\Gamma, x : A\ \textbf{says}\ \alpha, y : \alpha \vdash \Delta}\,(cut)}{\Gamma, x : A\ \textbf{says}\ \alpha \vdash \Delta}\,(\textbf{says}\ L)$$

□

We can now prove the following theorem:

**Theorem 11.** *Let* $\vdash u : \phi$ *be a sequent and let* $\tau$ *be the height of the parse tree of* $\phi$*. In order to check whether* $\vdash u : \phi$ *is derivable, the rules* $(\rightarrow R)$ *and* ( **says** $R$) *can be reformulated as follows:*

$$\frac{\Gamma, y \geq x, y : \alpha \vdash \Delta, y : \beta}{\Gamma \vdash \Delta, x : \alpha \rightarrow \beta}\,(\rightarrow R) \qquad\qquad \frac{\Gamma, x \xrightarrow{A} y \vdash \Delta, y : \alpha}{\Gamma \vdash \Delta, x : A\ \textbf{says}\ \alpha}\,(\ \textbf{says}\ R)$$

*where the following conditions hold:*

1. $y$ *is new, that is to say it does not occur in* $\Gamma$ *and* $\Delta$*;*
2. $d(x, u) \leq \tau$*.*

*Proof.* (Sketch) Let us consider a sequent of the form $\Gamma, x_0 : \alpha_1 \circ \alpha_2 \circ \ldots \circ \alpha_n, x_0 : \beta \vdash \Delta$, where $\circ \in \{\rightarrow,$ **says** $\}$, and suppose that a formula $\gamma \circ \delta$ occurs negatively in $\beta$, that is to say in a way such that the application of the rules of the calculi could lead to a sequent of the form $\Gamma', x_0 : \alpha_1 \circ \alpha_2 \circ \ldots \circ \alpha_n, x_0 : \beta \vdash \Delta', x_0 : \gamma \circ \delta$. Suppose also that, for all $l$ such that $x_0 : \chi_1 \circ \chi_2 \circ \ldots \circ \chi_l \in \Gamma$, we have that $l \leq n$. Furthermore, by Lemmas 13 and 14, we can consider, without loss of generality, only proofs in which any application of $(\circ L)$ is replaced by an application of the corresponding $(\widetilde{\circ L})$. An application of $(\circ R)$ to $x_0 : \gamma \circ \delta$ introduces (backward) a new label $x_1$, as well as a formula $x_1 \geq x_0$, either (i) directly, in case $\circ = \rightarrow$, or (ii) by an application of $(Unit)$ in case $\circ =$ **says** and the transition formula $x_0 \xrightarrow{\gamma} x_1$ has been introduced (backward) by the application of ( **says** $R$). The rule $(\widetilde{\circ L})$ can be applied to both the principal formulas $x_0 : \alpha_1 \circ \alpha_2 \circ \ldots \circ \alpha_n$ and $x_0 : \beta$ by using the label $x_1$, obtaining a branch containing a sequent whose left hand side contains the following formulas:

$x_0 : \alpha_1 \circ \alpha_2 \circ \ldots \circ \alpha_n, x_0 : \beta$
$x_1 : \alpha_1 \circ \alpha_2 \circ \ldots \circ \alpha_n, x_1 : \alpha_2 \circ \ldots \circ \alpha_n, x_0 : \beta, x_1 : \beta$

Since $\gamma \circ \delta$ occurs negatively in $\beta$, a new label $x_2$ can be further introduced by an application of $(\circ R)$ to $x_1 : \gamma \circ \delta$, thus introducing (backward) a formula $x_2 \geq x_1$, again either directly by $(\rightarrow R)$ or by means of an application of $(Unit)$ with ( **says** $R$). In case $\circ =$ **says** , by an application of $(INT)$, also $x_0 \xrightarrow{\gamma} x_2$ is added to the branch. By an application of $(TR)$, also $x_2 \geq x_0$ is introduced. The rule $(\widetilde{\circ L})$ can be further applied by using $x_2$ to both the principal formulas $x_0 : \alpha_1 \circ \alpha_2 \circ \ldots \circ \alpha_n$ and $x_0 : \beta$. We obtain a branch containing a sequent whose left hand side contains the following formulas:

$x_0 : \alpha_1 \circ \alpha_2 \circ \ldots \circ \alpha_n, x_0 : \beta$
$x_1 : \alpha_1 \circ \alpha_2 \circ \ldots \circ \alpha_n, x_1 : \alpha_2 \circ \ldots \circ \alpha_n, x_0 : \beta, x_1 : \beta$
$x_2 : \alpha_1 \circ \alpha_2 \circ \ldots \circ \alpha_n, x_2 : \alpha_2 \circ \ldots \circ \alpha_n, x_2 : \alpha_3 \circ \ldots \circ \alpha_n, x_0 : \beta, x_1 : \beta, x_2 : \beta$

And so on, obtaining a branch containing $x_{n-1} \geq x_{n-2}, \ldots, x_{n-1} \geq x_0, x_1 \geq x_0$, the formulas:

$x_0 : \alpha_1 \circ \alpha_2 \circ \ldots \circ \alpha_n, x_0 : \beta$
$x_1 : \alpha_1 \circ \alpha_2 \circ \ldots \circ \alpha_n, x_1 : \alpha_2 \circ \ldots \circ \alpha_n, x_0 : \beta, x_1 : \beta$
$x_2 : \alpha_1 \circ \alpha_2 \circ \ldots \circ \alpha_n, x_2 : \alpha_2 \circ \ldots \circ \alpha_n, x_2 : \alpha_3 \circ \ldots \circ \alpha_n, x_0 : \beta, x_1 : \beta, x_2 : \beta$
$\vdots$
$x_{n-2} : \alpha_1 \circ \ldots \circ \alpha_n, x_{n-2} : \alpha_2 \circ \ldots \circ \alpha_n, \ldots, x_{n-2} : \alpha_{n-1} \circ \alpha_n, x_0 : \beta, \ldots, x_{n-2} : \beta$
$x_{n-1} : \alpha_1 \circ \alpha_2 \circ \ldots \circ \alpha_n, x_{n-1} : \alpha_2 \circ \ldots \circ \alpha_n, \ldots, x_{n-1} : \alpha_n, x_0 : \beta, \ldots, x_{n-1} : \beta$

and, in case $\circ =$ **says** , the transition formulas $x_0 \xrightarrow{\gamma} x_1, \ldots, x_0 \xrightarrow{\gamma} x_{n-1}, x_{n-2} \xrightarrow{\gamma} x_{n-1}$. We can conclude that it is useless to apply again the rules $(\circ R)$ to $x_{n-1} : \gamma \circ \delta$, thus generating a new label $x_n$. Indeed, since $n$ is the highest $l$ such that $x_0 : \chi_1 \circ \chi_2 \circ \ldots \circ \chi_l \in \Gamma$, if $x_n : \alpha_n$ is needed to close the branch, also $x_{n-1} : \alpha_n$ can be used to close such branch, because $x_n$ would label exactly the same formulas of $x_{n-1}$, namely:

$x_n : \alpha_1 \circ \alpha_2 \circ \ldots \circ \alpha_n, x_n : \alpha_2 \circ \ldots \circ \alpha_n, \ldots, x_n : \alpha_n, x_0 : \beta, \ldots, x_n : \beta.$ □

Furthermore, we need the following lemmas:

**Lemma 15.** *If a sequent $\Gamma \vdash \Delta, y \geq x$ is derivable in $\mathcal{S}_{Cond^{\mathbf{UC}}_{ACL}}$ , then either $\Gamma \vdash \Delta$ is derivable or $y \geq x \in \Gamma$ or $y = x$.*

*Proof.* (Sketch) Intuitively, in order to prove a sequent $\Gamma \vdash \Delta, y \geq x$, we observe that $y \geq x$ is introduced (looking forward) either by an application of $(\rightarrow L)$ or by weakening. In the latter case, obviously $\Gamma \vdash \Delta$ is derivable too. In the former one, the only way to prove $y \geq x$ in the leftmost premise $\Gamma \vdash \Delta, y \geq x$ is by $(AX_{\geq})$ or $(AX)$. In the first case, we are done, since $x = y$. In the other one, since $(\rightarrow R)$ and $(TR)$ are the only rules introducing a formula $y \geq x$ in the left hand side of a sequent in a backward proof search, and since such rules are invertible (Lemma 7), we can assume, without loss of generality, that they have been applied before $(\rightarrow L)$, therefore $y \geq x$ already belongs to $\Gamma$. The rigorous proof is by induction on the height of the derivation of $\Gamma \vdash \Delta, y \geq x$. □

We can reason analogously for the transition formulas, considering that a formula $x \xrightarrow{A} y$ in the right hand side of a sequent can only be proved (backward) by an application of $(EQ)$:

**Lemma 16.** *If a sequent $\Gamma \vdash \Delta, x \xrightarrow{A} y$ is derivable in $\mathcal{S}_{Cond^{\mathbf{UC}}_{ACL}}$ , then either $\Gamma \vdash \Delta$ is derivable or $x \xrightarrow{A'} y \in \Gamma$.*

The following facts allow to obtain a terminating calculus from $\mathcal{S}_{\mathsf{Cond}^{\mathbf{UC}}_{ACL}}$ :

- The rules of $\mathcal{S}_{\mathsf{Cond}^{\mathbf{UC}}_{ACL}}$ introduce only a finite number of labels in a backward proof search: labels are only introduced by the rules $(\rightarrow R)$ and ( **says** $R$), restricted as stated by Theorem 11 above, by formulas occurring negatively in the initial sequent, which are finite.
- It is useless to apply the rules $(TR)$, $(INT)$, $(Unit)$, $(ID)$, $(C)$, $(CA)$, $(CA-conv)$, $(DT)$, and $(MON)$ more than once on the same principal formula. As an

example, let us consider the rule $(Unit)$: we can restrict its application to $\Gamma, x \xrightarrow{A} y \vdash \Delta$ only to the case in which the rule has not been previously applied to $x \xrightarrow{A} y$ in that branch, i.e. if $y \geq x \notin \Gamma$. Similarly for the other rules.

- A backward application of $(CA - conv)$ introduces $x \xrightarrow{A \vee B} y$ in the premise, where $x \xrightarrow{A \vee B} y$ does not belong to the conclusion, but where $A \vee B$ is a principal belonging to $\mathcal{L}_{\mathbf{P}}$. The same for $(CA)$. The same for $(DT)$ and $(MON)$, introducing $x \xrightarrow{A \wedge B} y$. Since $\mathcal{L}_{\mathbf{P}}$ is finite, these rules will be applied a finite number of times in the same branch.
- The rule $(\rightarrow L)$, applied to a sequent $\Gamma, x : \alpha \rightarrow \beta \vdash \Delta$, leads to a premise $\Gamma, x : \alpha \rightarrow \beta \vdash \Delta, y \geq x$, and can thus be reapplied without any control. However, it is useless to apply $(\rightarrow L)$ on the same formula $x : \alpha \rightarrow \beta$ more than once in each branch in a backward proof search, introducing the same formula $y \geq x$ in the leftmost premise. Moreover, by Lemma 15 we can restrict the choice of the order formula $y \geq x$ introduced in a way such that either $y \geq x \in \Gamma$ or $y = x$: this is explained by the fact that no rule of $\mathcal{S}_{\mathsf{Cond}^{\mathbf{UC}}_{\mathrm{ACL}}}$ have a formula $y \geq x$ in the right hand side of a sequent as a principal formula. Therefore, the only way to prove it in a backward search is either by $(AX)$, i.e. by a sequent also having $y \geq x$ in its left hand side (then, we can choose among $y \geq x$ already in $\Gamma$) or by $(AX_{\geq})$, thus choosing $y = x$. The same for $(ATM)$.
- Similarly to the previous point, it is useless to apply $(\textbf{ says } L)$ on the same formula $x : A \textbf{ says } \gamma$ more than once in each branch, introducing (backward) the same formula $x \xrightarrow{A} y$ in the leftmost premise. Moreover, by Lemma 16, the choice of the transition $x \xrightarrow{A} y$ to be used is restricted to formulas such that, for some formula $A'$, there exists $x \xrightarrow{A'} y \in \Gamma$. Intuitively, this follows from the fact that a transition formula on the right hand side of a sequent can only be proved by an application of $(EQ)$. Moreover, since $(EQ)$ only involves transition formulas, the premise introducing $x \xrightarrow{A} y$ can be reduced to $x \xrightarrow{A'} y \vdash x \xrightarrow{A} y$. A similar restriction applies also to $(MON)$ and $(CA)$.

The resulting terminating calculus $\widehat{\mathcal{S}_{\mathsf{Cond}^{\mathbf{UC}}_{\mathrm{ACL}}}}$ is shown in Figure 7. It is worth noticing that $(AX)$ is restricted to atomic formulas, and that $(AX_{\geq})$ is not needed due to the reformulation of the other rules.

By the above facts, it follows that:

**Theorem 12.** *A sequent $\Gamma \vdash \Delta$ is derivable in $\mathcal{S}_{\mathit{Cond}^{\mathbf{UC}}_{\mathit{ACL}}}$ if and only if $\Gamma \vdash \Delta$ is derivable in $\widehat{\mathcal{S}_{\mathit{Cond}^{\mathbf{UC}}_{\mathit{ACL}}}}$.*

**Theorem 13.** *The sequent calculus $\widehat{\mathcal{S}_{\mathit{Cond}^{\mathbf{UC}}_{\mathit{ACL}}}}$ ensures a terminating proof search, then the logic $\mathsf{Cond}^{\mathbf{UC}}_{\mathrm{ACL}}$ is decidable.*

*Proof.* Given a formula $\phi$, just observe that there is only a finite number of derivations of the sequent $\vdash u : \phi$, as both the length of a proof and the number of labelled formulas which may occur in it is finite. □

$$(AX)\ \Gamma, x : P \vdash \Delta, x : P \quad \text{if } P \in ATM$$

$$(AX_{\bot})\ \Gamma, x : \bot \vdash \Delta$$

$$\frac{\Gamma, x : P, y : P \vdash \Delta}{\Gamma, x : P \vdash \Delta}\ (ATM) \quad \text{if } y : P \notin \Gamma \text{ and } y \geq x \in \Gamma,\ P \in ATM$$

$$\frac{\Gamma, y \geq x, y \xrightarrow{A} z, x \xrightarrow{A} z \vdash \Delta}{\Gamma, y \geq x, y \xrightarrow{A} z \vdash \Delta}\ (INT) \quad \text{if } x \xrightarrow{A} z \notin \Gamma$$

$$\frac{\Gamma, z \geq x, z \geq y, y \geq x \vdash \Delta}{\Gamma, z \geq y, y \geq x \vdash \Delta}\ (TR) \quad \text{if } z \geq x \notin \Gamma$$

$$\frac{\Gamma \vdash \Delta, x : \alpha \qquad \Gamma \vdash \Delta, x : \beta}{\Gamma \vdash \Delta, x : \alpha \wedge \beta}\ (\wedge R)$$

$$\frac{\Gamma, x : \alpha, x : \beta \vdash \Delta}{\Gamma, x : \alpha \wedge \beta \vdash \Delta}\ (\wedge L)$$

$$\frac{\Gamma \vdash \Delta, x : \alpha, x : \beta}{\Gamma \vdash \Delta, x : \alpha \vee \beta}(\vee R)$$

$$\frac{\Gamma, x : \alpha \vdash \Delta \qquad \Gamma, x : \beta \vdash \Delta}{\Gamma, x : \alpha \vee \beta \vdash \Delta}(\vee L)$$

$$\frac{\Gamma, y \geq x, y : \alpha \vdash \Delta, y : \beta}{\Gamma \vdash \Delta, x : \alpha \rightarrow \beta}\ (\rightarrow R) \quad y \text{ new},\ \text{if } d(x,u) \leq \tau$$

$$\frac{\Gamma, x : \alpha \rightarrow \beta \vdash \Delta, y : \alpha \qquad \Gamma, x : \alpha \rightarrow \beta, y : \beta \vdash \Delta}{\Gamma, x : \alpha \rightarrow \beta \vdash \Delta}\ (\rightarrow L) \quad \text{if } y \geq x \in \Gamma$$

$$\frac{\Gamma, x \xrightarrow{A} y \vdash \Delta, y : \alpha}{\Gamma \vdash \Delta, x : A \textbf{ says } \alpha}\ (\textbf{ says } R) \quad y \text{ new},\ \text{if } d(x,u) \leq \tau$$

$$\frac{x \xrightarrow{A'} y \vdash x \xrightarrow{A} y \qquad \Gamma, x : A \textbf{ says } \alpha, y : \alpha \vdash \Delta}{\Gamma, x : A \textbf{ says } \alpha \vdash \Delta}(\textbf{ says } L) \quad \text{if } x \xrightarrow{A'} y \in \Gamma$$

$$\frac{u : A \vdash u : B \qquad u : B \vdash u : A}{\Gamma, x \xrightarrow{A} y \vdash \Delta, x \xrightarrow{B} y}\ (EQ) \quad u \text{ new}$$

$$\frac{x \xrightarrow{A'} y \vdash x \xrightarrow{A \wedge B} y \qquad \Gamma, x \xrightarrow{A} y, x \xrightarrow{B} y \vdash \Delta}{\Gamma \vdash \Delta}(MON) \quad A \wedge B \in \mathcal{L}_P,\ \text{if } \{x \xrightarrow{A} y, x \xrightarrow{B} y\} \nsubseteq \Gamma \text{ and } x \xrightarrow{A'} y \in \Gamma$$

$$\frac{\Gamma, x \xrightarrow{A} y \vdash \Delta, y : B \qquad \Gamma, x \xrightarrow{A} y, x \xrightarrow{A \wedge B} y \vdash \Delta}{\Gamma, x \xrightarrow{A} y \vdash \Delta}\ (DT) \quad \text{if } x \xrightarrow{A \wedge B} y \notin \Gamma,\ A \wedge B \in \mathcal{L}_P$$

$$\frac{\Gamma, x \xrightarrow{A} y, y : A \vdash \Delta}{\Gamma, x \xrightarrow{A} y \vdash \Delta}\ (ID) \quad \text{if } y : A \notin \Gamma$$

$$\frac{\Gamma, z \geq y, x \xrightarrow{A} y, z \xrightarrow{A} z \vdash \Delta}{\Gamma, z \geq y, x \xrightarrow{A} y \vdash \Delta}(C) \quad \text{if } z \xrightarrow{A} z \notin \Gamma$$

$$\frac{\Gamma, x \xrightarrow{A \vee B} y, x \xrightarrow{A} y \vdash \Delta}{\Gamma, x \xrightarrow{A} y \vdash \Delta}\ (CA - conv) \quad \text{if } x \xrightarrow{A \vee B} y \notin \Gamma,\ A \vee B \in \mathcal{L}_P$$

$$\frac{x \xrightarrow{A'} y \vdash x \xrightarrow{A \vee B} y \qquad \Gamma, x \xrightarrow{A} y \vdash \Delta \qquad \Gamma, x \xrightarrow{B} y \vdash \Delta}{\Gamma \vdash \Delta}(CA) \quad A \vee B \in \mathcal{L}_P,\ \text{if } \{x \xrightarrow{A} y, x \xrightarrow{B} y\} \cap \Gamma = \emptyset \text{ and } x \xrightarrow{A'} y \in \Gamma$$

$$\frac{\Gamma, y \geq x, x \xrightarrow{A} y \Rightarrow \Delta}{\Gamma, x \xrightarrow{A} y \Rightarrow \Delta}\ (Unit) \quad \text{if } y \geq x \notin \Gamma$$

**Fig. 7.** The terminating calculus $\mathcal{S}_{\widehat{\mathsf{Cond}^{\mathbf{UC}}_{\mathrm{ACL}}}}$. In order to prove that a formula $\phi$ is valid in $\mathsf{Cond}^{\mathbf{UC}}_{\mathrm{ACL}}$, the calculus checks whether there is a derivation of $\vdash u : \phi$. Therefore, $u$ is the label in the initial sequent.

This itself gives the decidability of $\mathsf{Cond}_{\mathrm{ACL}}^{\mathbf{UC}}$. We have also developed a Prolog prototype implementing the decision procedure $\widehat{\mathcal{S}_{\mathsf{Cond}_{\mathrm{ACL}}^{\mathbf{UC}}}}$ [17].

We can give an explicit space complexity bound for $\mathsf{Cond}_{\mathrm{ACL}}^{\mathbf{UC}}$. As usual, a proof may have an exponential size because of the branching introduced by the rules. However we can obtain a much sharper space complexity bound since we do not need to store the whole proof, but only a sequent at a time plus additional information to carry on the proof search; this standard technique is similar to the one adopted in [19, 26]:

**Theorem 14.** *Let $n$ be the length of the string representing a sequent $\Gamma \vdash \Delta$. The problem of deciding provability of $\Gamma \vdash \Delta$ in $\mathsf{Cond}_{\mathrm{ACL}}^{\mathbf{UC}}$ is decidable in $O(n^4 \ \log n)$ space.*

*Proof.* First, observe that, in the proof search of $\vdash u : \phi$, with $\mid \phi \mid = n$, new labels are introduced only by (sub)formulas occurring negatively in $\phi$. Let $\tau$ be the height of the parse tree of $\phi$. Theorem 11 states that, given a formula (of the form either $x : \alpha \rightarrow \beta$ or $x : A$ **says** $\gamma$) introducing a new label in the branch, it can be applied only if the distance between $x$ and the label $u$ in the sequent of the root is less or equal to $\tau$. Obviously, $\tau$ is bounded by $n$. Theorefore, each (sub)formula occurring negatively in $\phi$ generates at most $n$ labels, then, since there are $O(n)$ (sub)formulas, the number of different labels introduced in a branch is $O(n^2)$. Suppose also that $\mid \mathcal{L}_{\mathbf{P}} \mid$ is bounded by $O(n)$. All possible (sub)formulas in $\phi$ are, obviously, $O(n)$, therefore the number of different labelled formulas is $O(n^3)$. The rules of $\widehat{\mathcal{S}_{\mathsf{Cond}_{\mathrm{ACL}}^{\mathbf{UC}}}}$ can be applied to each labelled formula: at most $n$ rules are applied to each formula, then we have that the length of each branch of a proof tree is bounded by $O(n^4)$.

In searching a proof, there are two kinds of branching to consider: AND-branching caused by the rules with multiple premises and OR-branching (backtracking points in a depth first search) caused by the choice of the rule to apply. We store only one sequent at a time and maintain a stack containing information sufficient to reconstruct the branching points of both types. Each stack entry contains the principal formula, the name of the rule applied and an index which allows to reconstruct the other branches on return to the branching points. The stack entries represent thus backtracking points and the index within the entry allows one to reconstruct both the AND branching and to check whether there are alternatives to explore (OR branching). The working sequent on a return point is recreated by replaying the stack entries from the bottom of the stack using the information in the index (for instance, in the case of ( **says** $L$) applied to the principal formula $x : A$ **says** $\gamma$, the index will indicate which premise-first or second-we have to expand and the label $y$ involved in the formula $x \xrightarrow{A} y$).

A proof begins with the end sequent $\vdash u : \phi$ and the empty stack. Each rule application generates a new sequent and extends the stack. If the current sequent is an axiom we pop the stack until we find an AND branching point to be expanded. If there are not, the end sequent $\vdash u : \phi$ is derivable and we have finished. If the current sequent is not an axiom and no rule can be applied to it, we pop the stack entries and we continue at the first available entry with some alternative left (a backtracking point). If there are no such entries, the end sequent is not derivable.

The entire process must terminate since: (i) the depth of the stack is bounded by the length of a branch proof, thus it is $O(n^4)$, (ii) the branching is bounded by the number of rules, the number of premises of any rule and the number of labelled formulas occurring in one sequent, the last being $O(n^3)$.

To evaluate the space requirement, we have that each subformula of the initial labelled formula can be represented by a positional index into the initial labelled formula, which requires $O(\log n)$ bits. Moreover, also each label can be represented by $O(\log n)$ bits. Thus, to store the working sequent we need $O(n^3 \ \log n)$ space, since there may occur $O(n^3)$ labelled subformulas. Similarly, each stack entry requires $O(\log n)$ bits, as the name of the rule requires constant space and the index $O(\log n)$ bits. Having depth $O(n^4)$, to store the whole stack requires $O(n^4 \ \log n)$ space. Thus we obtain that provability in $\mathsf{Cond}_{\mathrm{ACL}}^{\mathbf{UC}}$ is decidable in $O(n^4 \ \log n)$ space. □

Given a formula $\phi \in \mathcal{L}$, since $\widehat{\mathcal{S}_{\mathsf{Cond}_{\mathrm{ACL}}^{\mathbf{UC}}}}$ is sound and complete with respect to the semantics of the logic $\mathsf{Cond}_{\mathrm{ACL}}^{\mathbf{UC}}$ , in order to check whether $\phi$ is valid in $\mathsf{Cond}_{\mathrm{ACL}}^{\mathbf{UC}}$ we can check whether $\vdash u : \phi$ is derivable in $\widehat{\mathcal{S}_{\mathsf{Cond}_{\mathrm{ACL}}^{\mathbf{UC}}}}$. It immediately follows that:

**Theorem 15.** *Given a formula $\phi \in \mathcal{L}$, let $n$ be the length of the string representing $\phi$. The problem of deciding validity of $\phi$ in $\mathsf{Cond}_{\mathrm{ACL}}^{\mathbf{UC}}$ is decidable in $O(n^4 \ \log n)$ space.*

## 6 Related work and Conclusions

**Related Work.** Many formal frameworks have been proposed to specify and reason about access control systems [4, 6, 18, 22, 23]. Recently, as reported in [14], constructive logics have been recognized to be well suited for reasoning about authorization, because constructive proofs preserve the justification of statements during reasoning and, therefore, information about accountability is not lost. Classical logics, instead, allow proofs that discard evidence.

Abadi in [2] presents a formal study about connections between many possible axiomatizations of the "says" operator, as well as higher-level policy constructs such as delegation (*Speaks for*) and control. Abadi provides a strong argument to use constructivism in logic for access control, in fact he shows that from a well-known axiom like (UNIT) in a classical logic we can deduce $A$ **says** $\varphi \rightarrow (\varphi \vee A$ **says** $\psi)$. The axiom above is called *Escalation* and it represents a rather degenerate interpretation of **says** , i.e., if a principal says $\varphi$ then, either $\varphi$ holds or the principal can say *anything*. On the contrary, if we interpret the **says** within an intuitionistic logic we can avoid *Escalation*.

Although several authorization logics employ the says modality, a limited amount of work has been done to study the formal logical properties of **says** , *Speaks for* and other constructs.

Garg and Abadi [13] study a class of access control logics (*ICL*, *ICL*$^{\Rightarrow}$ and *ICL*$^{\mathcal{B}}$) via a sound and complete translation into modal logic S4 by relying on a slight simplification of Gödel's translation from intuitionistic logic to S4, and by extending it to formulas of the form $A$ **says** $\varphi$. The translation to S4 provides decidability and complexity results for this class of logics of access control. Among the conditional access control logics we have presented, the logic $\mathsf{Cond}^{\mathbf{I4}}_{\mathrm{ACL}}$ contains the characterizing access control axioms of *ICL*, namely (UNIT), (K) and (C4). $\mathsf{Cond}^{\mathbf{I4}}_{\mathrm{ACL}}$ derives all the axioms of *ICL* and is srictly stronger than *ICL*. As we have seen in Section 2.3, there are formulas of $ICL^{\Rightarrow}$ that are derivable in $\mathsf{Cond}^{\mathbf{I4}}_{\mathrm{ACL}}$ , but not in $ICL^{\Rightarrow}$. Concerning the treatment of boolean principals, we have discussed in Section 2.2 the differences among our definition and the one in [13].

Garg [12] adopts an ad-hoc version of constructive S4 called $\mathrm{DTL}_0$ and embeds existing approaches into it. Constructive S4 has been chosen because of its intuitionistic Kripke semantics which $\mathrm{DTL}_0$ extends by adding the notion of *view*, i.e., a mapping from principals to sets of worlds. $\mathrm{DTL}_0$ contains, as characterizing axioms, (K), (4) and (C). The axioms (K), (4) and (C) are derivable in $\mathsf{Cond}^{\mathbf{IC}}_{\mathrm{ACL}}$ . In particular, (4) is weaker than (I) and derivable from it. The preorder $\succeq$ among atomic principals can be captured in $\mathsf{Cond}^{\mathbf{IC}}_{\mathrm{ACL}}$ through the "speaks for" relation (which is reflexive and transitive), and satisfies axiom (S) (corresponding to the (Speaks For) axiom). The semantics of $\mathrm{DTL}_0$ has strong similarities with the semantics of $\mathsf{Cond}^{\mathbf{IC}}_{\mathrm{ACL}}$ , although it does not deal with boolean principals. It can be observed that the Kripke models for $\mathrm{DTL}_0$ include the semantic conditions of axioms (ID) and (MP), However, as these axioms are not expressible in the language of $\mathrm{DTL}_0$, they are not derivable from the axiomatization. As a difference, the aim of our proposal is to provide a modular approach to the definition of access control logics and their semantics, in which there is a one to one correspondence among semantic properties and characterizing axioms.

It has to be observed that, adopting a fixed semantics like S4 does not permit to study the correspondence between axioms of access control logics and Kripke structures. Suppose we look at **says** as a principal indexed modality $\Box_A$, if we rely on S4 we would have as an axiom $\Box_A \varphi \rightarrow \varphi$, which means: *everything* that $A$ says holds. To overcome this problem, both in [12, 13], Kripke semantics is weakened with the addition of *views* which relativize the reasoning to a subset of worlds. Although this approach provides sound and complete semantics for a certain combination of axioms (those included in *ICL*), it breaks the useful bound between modality axioms and relations of Kripke structures.

Boella et al. [7] define a logical framework called FSL (Fibred Security Language), based on fibring semantics [11] by looking at "says" as a (fibred) modal operator. FSL is, in general, not decidable and its formalization is limited to Kripke-style semantics. In fact, no proof method for FSL has been provided. Moreover, the representation of the speaks for in FSL is limited to the definition of axiom schemas of the type $A$ **says** $\varphi \rightarrow B$ **says** $\varphi$, which means that, given a reference monitor modeled with FSL, it is not possible to introduce new speaks for relationships at run-time.

**Conclusions.** We have defined four intuitionistic conditional logics for Access Control called $\mathsf{Cond}^{\mathbf{UC}}_{\mathrm{ACL}}$ , $\mathsf{Cond}^{\mathbf{U4}}_{\mathrm{ACL}}$ , $\mathsf{Cond}^{\mathbf{IC}}_{\mathrm{ACL}}$ and $\mathsf{Cond}^{\mathbf{I4}}_{\mathrm{ACL}}$ . We have presented a sound, complete and cut-free sequent calculus for such logics. Also, we have shown that provability in $\mathsf{Cond}^{\mathbf{UC}}_{\mathrm{ACL}}$ is decidable in $O(n^4 logn)$ space, in agreement with the PSPACE results given in [13] for the logic *ICL*. With respect to the work in [12, 13], we identify canonical properties for axioms of the logic, i.e., first-order conditions on Kripke structures that are *necessary* and *sufficient* for the corresponding axiom to hold.

We believe that this methodology has several advantages. First, conditional logics allow a natural formalization of the **says** modality including the specification of boolean principals as formulas as well as a natural treatment of *Speaks for*. Second, the identification of canonical properties for access control axioms provides a natural deconstruction of access control logics. By deconstruction we mean the possibility to craft access control logics that adopt *any* combination of axioms for which canonical properties exist. For instance, not all access control systems adopt (UNIT) as an axiom [22, 5, 18], but the translation in [13] does not provide an embedding in S4 for a logic without (UNIT). In general, the approach in [13] does not provide a methodology to deconstruct access control logics. In our approach, instead, we can formalize a logic and a calculus without (UNIT) which is still sound and complete, by dropping the semantic condition (S-UNIT) and the corresponding rule $(Unit)$ in the calculus, as shown for the logics $\mathsf{Cond}^{\mathbf{IC}}_{\mathrm{ACL}}$ and $\mathsf{Cond}^{\mathbf{I4}}_{\mathrm{ACL}}$ and the respective calculi $\mathcal{S}_{\mathsf{Cond}^{\mathbf{IC}}_{\mathrm{ACL}}}$ and $\mathcal{S}_{\mathsf{Cond}^{\mathbf{I4}}_{\mathrm{ACL}}}$.

We believe that choosing axioms for access control logics depends on the needs of security practitioners. By looking at **says** as a conditional modality, we can offer a formal framework to study the axioms of access control via canonical properties on the semantics, and to build calculi to carry out automated deduction. Of course, for each combination of axioms, the decidability and the complexity of the resulting logic as well as the termination of the calculus have to be determined.

**Acknowledgements.** The work has been partially supported by Regione Piemonte, Project "ICT4Law: ICT Converging on Law: Next Generation Services for Citizens, Enterprises, Public Administration and Policymakers". Valerio Genovese is supported by the National Research Fund, Luxembourg.

## References

1. Martín Abadi. Access Control in a Core Calculus of Dependency. *Electronic Notes in Theorethical Computer Science*, 172:5–31, 2007.
2. Martín Abadi. Variations in access control logic. In Ron van der Meyden and Leendert van der Torre, editors, *Deontic Logic in Computer Science, 9th International Conference, DEON 2008*, volume 5076 of *Lecture Notes in Computer Science (LNCS)*, pages 96–109. Springer, July 2008.
3. Martín Abadi, Michael Burrows, Butler W. Lampson, and Gordon D. Plotkin. A calculus for access control in distributed systems. In Joan Feigenbaum, editor, *Advances in Cryptology - CRYPTO '91, 11th Annual International Cryptology Conference*, volume 576 of *Lecture Notes in Computer Science (LNCS)*, pages 1–23. Springer, August 1991.
4. Martín Abadi, Michael Burrows, Butler W. Lampson, and Gordon D. Plotkin. A calculus for access control in distributed systems. *ACM Transactions on Programming Languages and Systems (TOPLAS)*, 15(4):706–734, 1993.
5. Moritz Y. Becker, Cédric Fournet, and Andrew D. Gordon. Secpal: Design and semantics of a decentralized authorization language. *Journal of Computer Security*, 18(4):619–665, 2010.
6. Clara Bertolissi, Maribel Fernández, and Steve Barker. Dynamic event-based access control as term rewriting. In Steve Barker and Gail-Joon Ahn, editors, *Data and Applications Security XXI, 21st Annual IFIP WG 11.3 Working Conference on Data and Applications Security*, volume 4602 of *Lecture Notes in Computer Science (LNCS)*, pages 195–210. Springer, July 2007.

7. Guido Boella, Dov M. Gabbay, Valerio Genovese, and Leendert van der Torre. Fibred security language. *Studia Logica*, 92(3):395–436, 2009.
8. Brian F. Chellas. Basic conditional logics. *Journal of Philosophical Logic*, 4:133–153, 1975.
9. John DeTreville. Binder, a logic-based security language. In *IEEE Symposium on Security and Privacy*, pages 105–113, 2002.
10. Herbert B. Enderton. *A Mathematical Introduction to Logic, 2nd Edition*. Academic Press, 2000.
11. Dov M. Gabbay. *Fibring Logics*. Oxford University Press, 1999.
12. Deepak Garg. Principal centric reasoning in constructive authorization logic. In *Proceedings of the Workshop on Intuitionistic Modal Logic and Applications (IMLA)*, 2008.
13. Deepak Garg and Martín Abadi. A modal deconstruction of access control logics. In Roberto M. Amadio, editor, *Foundations of Software Science and Computational Structures, 11th International Conference, FOSSACS 2008, Held as Part of the Joint European Conferences on Theory and Practice of Software, ETAPS 2008*, volume 4962 of *Lecture Notes in Computer Science (LNCS)*, pages 216–230. Springer, March - April 2008.
14. Deepak Garg and Frank Pfenning. Non-interference in constructive authorization logic. In *19th IEEE Computer Security Foundations Workshop, (CSFW-19 2006)*, pages 283–296. IEEE Computer Society, July 2006.
15. Valerio Genovese, Laura Giordano, Valentina Gliozzi, and Gian Luca Pozzato. A conditional constructive logic for access control and its sequent calculus. In K. Brünnler and G. Metcalfe, editors, *TABLEAUX 2011 (20th International Conference on Automated Reasoning with Analytic Tableaux and Related Methods)*, volume 6793 of *Lecture Notes in Artificial Intelligence (LNAI)*, pages 164–179, Bern, Switzerland, July 2011. Springer-Verlag.
16. Valerio Genovese, Laura Giordano, Valentina Gliozzi, and Gian Luca Pozzato. Details on Termination in Conditional Access Control Logics, Technical Report, Dip. di Informatica, Univ. di Torino, HTTP://WWW.DI.UNITO.IT/∼POZZATO/TR/TR2012TERMJLC.PDF. 2012.
17. Valerio Genovese, Laura Giordano, Valentina Gliozzi, Gian Luca Pozzato, and Daniele Rispoli. ACL-Lean: a Sound, Complete and Terminating Theorem Prover for Access Control Logics, Technical Report, Dip. di Informatica, Univ. di Torino, HTTP://WWW.DI.UNITO.IT/∼GENOVESE/PUBLICATIONS/2011/TR201101.PDF. 2010.
18. Yuri Gurevich and Arnab Roy. Operational semantics for DKAL: Application and analysis. In Simone Fischer-Hübner, Costas Lambrinoudakis, and Günther Pernul, editors, *Trust, Privacy and Security in Digital Business, 6th International Conference, TrustBus 2009*, volume 5695 of *Lecture Notes in Computer Science (LNCS)*, pages 149–158. Springer, September 2009.
19. Jörg. Hudelmaier. An $\mathcal{O}(n\ log\ n)$-space decision procedure for intuitionistic propositional logic. *Journal of Logic and Computation*, 3(1):63–75, 1993.
20. Stephen Cole Kleene. *Introduction to Metamathematics*. Ishi Press International, 1952.
21. Butler W. Lampson, Martín Abadi, Michael Burrows, and Edward Wobber. Authentication in distributed systems: Theory and practice. *ACM Transactions on Computer Systems (TOCS)*, 10(4):265–310, 1992.
22. Chris Lesniewski-Laas, Bryan Ford, Jacob Strauss, Robert Morris, and M. Frans Kaashoek. Alpaca: extensible authorization for distributed services. In Peng Ning, Sabrina De Capitani di Vimercati, and Paul F. Syverson, editors, *ACM Conference on Computer and Communications Security*, pages 432–444. ACM, October 2007.
23. Ninghui Li, Benjamin N. Grosof, and Joan Feigenbaum. Delegation logic: A logic-based approach to distributed authorization. *ACM Transactions on Information and System Security (TISSEC)*, 6(1):128–171, 2003.
24. Sara Negri. Proof analysis in modal logic. *Journal of Philosophical Logic*, 34:507–544, 2005.

25. Donald Nute. *Topics in Conditional Logic*. Reidel, Dordrecht, 1980.
26. Nicola Olivetti, Gian Luca Pozzato, and Camilla B. Schwind. A Sequent Calculus and a Theorem Prover for Standard Conditional Logics. *ACM Transactions on Computational Logics (TOCL)*, 8(4), 2007.
27. Nicola Olivetti and Camilla B. Schwind. Analytic tableaux for conditional logics. *Technical Report, University of Torino*, 2000.
28. Gian Luca Pozzato. *Conditional and Preferential Logics: Proof Methods and Theorem Proving*, volume 208 of *Frontiers in Artificial Intelligence and Applications*. IOS Press, 2010.
29. Fred B. Schneider, Kevin Walsh, and Emin Gün Sirer. Nexus authorization logic (nal): Design rationale and applications. *ACM Transactions on Information and System Security (TISSEC)*, 14(1):8, 2011.
30. Raymond M. Smullyan. *Forever Undecided*. Oxford University Press, 1988.
31. Anne S. Troelstra and Dirk van Dalen. *Constructivism in Mathematics: An Introduction*. Elsevier, 1988.
32. Luca Viganò. *Labelled non-classical logics*. Kluwer, 2000.