A conditional constructive logic for access control and its sequent calculus

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. In this paper we study the applicability of constructive conditional logics as a general framework to define decision procedures in access control logics. To this purpose, we formalize the assertion A **says** ϕ, whose intended meaning is that *principal* A *says that* ϕ, as a conditional implication. We introduce $\mathsf{Cond}_{\mathrm{ACL}}$, which is a conservative extension of the logic *ICL* recently introduced by Garg and Abadi. We identify the conditional axioms needed to capture the basic properties of the "says" operator and to provide a proper definition of boolean principals. We provide a Kripke model semantics for the logic and we prove that the axiomatization is sound and complete with respect to the semantics. Moreover, we define a sound, complete, cut-free and terminating sequent calculus for $\mathsf{Cond}_{\mathrm{ACL}}$, which allows us to prove that the logic is decidable. We argue for the generality of our approach by presenting canonical properties of some further well known access control axioms. The identification of canonical properties provides the possibility to craft access control logics that adopt *any* combination of axioms for which canonical properties exist.

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. In order to specify and reason about such systems, many formal frameworks have been proposed [2, 5, 15, 18, 19]. A common feature of most well-known approaches is the employment of constructive logics enriched with formulas of the form A **says** φ, intuitively meaning that the principal A *asserts* or *supports* φ to hold in the system. In [1] 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 [11] 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 [6], which introduces a logical framework, FSL, based on multi-modal logic methodology.

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 [20] can provide a general framework to define axiomatization, semantics and proof methods for access control logics. As a starting point, we concentrate on a specific combination of axioms, those of the logic $\mathsf{Cond}_{\mathrm{ACL}}$, which is a conservative extension of the logic *ICL* introduced in [11]. In Section 5 we will point out a few possible extra axioms, which are well known in the access control literature, and we provide semantic conditions for them.

$\mathsf{Cond}_{\mathrm{ACL}}$ integrates access control logics with intuitionistic conditional logics. We formalize the **says** operator as a conditional normal modality so that A **says** ϕ is regarded as a conditional implication $A \Rightarrow \phi$, meaning that proposition ϕ holds in all the preferred worlds for the principal A. The generality of this approach allows a natural formalization of boolean principals [11], that is, principals which are formed by boolean combination of atomic principals.

From the access control point of view, the **says** operator satisfies some basic axioms of access control logics [11, 10]. We define a sound and complete Kripke semantics for $\mathsf{Cond}_{\mathrm{ACL}}$ as well as a sound, complete, cut-free labelled sequent calculus for it. We are also able to obtain a decision procedure and a complexity upper bound for $\mathsf{Cond}_{\mathrm{ACL}}$, namely that provability in $\mathsf{Cond}_{\mathrm{ACL}}$ is decidable in PSPACE. This is in agreement with [11], which provides a PSPACE complexity result for the logic ICL.

The paper is structured as follows. In Section 2 we introduce the axiomatization and the semantics for the intuitionistic conditional logic $\mathsf{Cond}_{\mathrm{ACL}}$ and we compare it with existing approaches. In Section 3 we show that the axiomatization is sound and complete with respect to the semantics. In Section 4 we define a cut-free sequent calculus for $\mathsf{Cond}_{\mathrm{ACL}}$, we prove its soundness, completeness and termination, and we provide a complexity upper bound. In Section 5 we provide semantic conditions for some further axioms of access control logics. Section 6 contains the conclusions and a discussion of related work.

2 The logic $\mathsf{Cond}_{\mathrm{ACL}}$

In this section, we introduce the conditional intuitionistic logic $\mathsf{Cond}_{\mathrm{ACL}}$ for access control by defining its axiomatization and Kripke semantics. 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** ϕ, both A and ϕ are arbitrary formulas. For instance, we can write, $A \wedge B$ **says** ϕ to mean that principals A and B jointly say that ϕ, and $A \vee B$ **says** ϕ to mean that principals A and B independently say that ϕ. Indeed, conditional logics provide a natural generalization of multimodal logics to the case when modalities are labelled by arbitrary formulas.

2.1 Axiom System

We define the language $\mathcal{L}$ of the logic $\mathsf{Cond}_{\mathrm{ACL}}$. Let ATM be a set of atomic propositions. 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 A, φ, φ_1 and φ_2 are formulas of $\mathcal{L}$, then $\neg\varphi$, $\varphi_1 \wedge \varphi_2$, $\varphi_1 \vee \varphi_2$, $\varphi_1 \rightarrow \varphi_2$, and A **says** φ are formulas of $\mathcal{L}$.

The intended meaning of the formula A **says** φ, where A and φ are arbitrary formulas, is that *principal A says that φ*, namely, "the principal A asserts or supports φ" [11]. Although the principal A is an arbitrary formula, in order to stress the fact that a formula is playing the role of a principal, we will denote it by $A, B, C, \ldots$ while we will use greek letters for arbitrary formulas.

The axiomatization of $\mathsf{Cond}_{\mathrm{ACL}}$ contains few basic axioms for access control logics [11, 1], 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 separetely. As a consequence, the resulting axiomatization might be redundant.

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

(TAUT)	all tautologies of intuitionistic logic
(K)	A **says** $(\alpha \to \beta) \to (A$ **says** $\alpha \to A$ **says** $\beta)$
(UNIT)	$\alpha \to (A$ **says** $\alpha)$
(C)	A **says** $(A$ **says** $\alpha \to \alpha)$
(MP)	If $\vdash \alpha$ and $\vdash \alpha \to \beta$ then $\vdash \beta$
(RCEA)	If $\vdash A \leftrightarrow B$ then $\vdash (A$ **says** $\gamma) \leftrightarrow (B$ **says** $\gamma)$
(RCK)	If $\vdash \alpha \to \beta$ then $\vdash (A$ **says** $\alpha) \to (A$ **says** $\beta)$

We say that a formula α is a theorem of the logic, and write $\vdash \alpha$ if there is a derivation of α from the above axioms and rules. We say that α can be derived from a set of formulas Γ, and write $\Gamma \vdash \alpha$, if there are $\gamma_1, \ldots \gamma_n$ in Γ such that $\vdash \gamma_1 \wedge \ldots \wedge \gamma_n \to \alpha$. 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. (RCEA) makes the formulas A **says** ϕ and B **says** ϕ equivalent when the principals A and B are equivalent. The axiom (K) belongs to the axiomatization of all normal modal logics and it is derivable in "normal" conditional logics. (UNIT) and (K) are the characterizing axioms of the logic ICL [11], while (C) has been included in the axiomatization of the logic DTL_0 in [10]. The choice of the above axiom is meaningful in the context of access control, in fact it can be proved that:

Theorem 1. *Cond_{ACL} is a conservative extension of* ICL, *i.e.* $\vdash_{\mathrm{ICL}} \varphi$ *implies* $\vdash \varphi$.

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** ϕ is that *A and B jointly (combining their statements) say that ϕ*. It comes from the interpretation of the statement as a conditional implication: A and B (jointly) conditionally prove ϕ. Instead, our interpretation of the statement $A \vee B$ **says** ϕ is that *A and B disjointly (independently) say that ϕ*, which comes from the reading of the conditional formula as A and B (disjointly) conditionally prove ϕ.

Concerning the statement $A \vee B$ **says** ϕ, we expect that if both A says ϕ and B says ϕ, then A and B disjointly (independently) say that ϕ. 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 [20]. 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 ϕ if and only if A says that ϕ and B says that ϕ .

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

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

which, although is a very controversial axiom of conditional logics, called monotonicity[4], can be proved to be harmless in this intuitionistic setting. Also, we would like to have the property that if $A \wedge B$ **says** ϕ then, by combining the statements of A and B, ϕ can be concluded. This is not equivalent to saying that either A says ϕ or B says ϕ. 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. In the following we show that the wanted property can be captured in a propositional axiomatization.

Although a principal is an arbitrary formula and it also includes negation and implication, no specific properties are intended for such formulas, and no specific axioms are introduced for them.

The axiomatization of $\mathsf{Cond}_{\mathrm{ACL}}$ includes (in addition) 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) $A \textbf{ says } A$

The first three axioms are those introduced above. (DT) and (ID) are used together to enforce the property that if $A \wedge B$ **says** ϕ then, by combining the statements of A and B, ϕ can be concluded. The two axioms allow propositions representing principals to occur on the right of the **says** modality. The intended meaning of (DT) is that, if $A \wedge B$ **says** ϕ, then A says that ϕ holds in all B worlds (worlds visible to the principal B). The meaning of (ID) is that "A says that principal A is visible". We will come back to the intended meaning of these axioms when describing the semantic conditions associated with the axioms. Nonetheless, our axiomatization does account for arbitrary Boolean combinations of principals (as in [11]), as a principal A can be an arbitrary formula. As a difference, we do not force any specific interpretation for implication within principals, which instead in ICL$^{\mathcal{B}}$ [11] is used to capture the "speaks for" operator. Observe that, by the normality of the conditional **says** modality, the principal $A \wedge B$ is, for instance, equivalent to the principal $A \wedge B \wedge A$. This is an advantage of conditional logic over a multi-modal logic in which principals are simply regarded as labels of modalities.

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

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 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$^{\mathcal{B}}$ [11], which actually adopts the opposite interpretation of $\wedge$ and $\vee$: in Garg and Abadi's logic ICL$^{\mathcal{B}}$, $A \wedge B$ **says** ϕ is the same as A **says** $\phi \wedge B$ **says** ϕ, while $A \vee B$ **says** ϕ means that, by combining the statements of A and B, ϕ can be concluded. Due to this, let us say, superficial 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. 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.

2.2 Semantics

The semantics of the logic $\mathsf{Cond}_{\mathrm{ACL}}$ is defined as follows.

Definition 1. *A* $\mathsf{Cond}_{\mathrm{ACL}}$ *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. $\mathcal{M}, t \models \neg\varphi$ *iff, for all* s *such that* $t \leq s$, $\mathcal{M}, s \not\models \varphi$
6. $\mathcal{M}, t \not\models \bot$
7. $\mathcal{M}, t \models A$ **says** ψ *iff, for all* s *such that* tR_As, $\mathcal{M}, s \vDash \psi$.

We say that ϕ *is valid in a model* $\mathcal{M}$ *if* $\mathcal{M}, t \models \phi$ *for all* $t \in S$*. We say that* ϕ *is* valid tout court *(and write* $\models \phi$*) if* ϕ *is valid in every model. We extend the notion of validity to a set of formulas* Γ *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* ϕ *is a* logical consequence *of* Γ *(and write* $\Gamma \models \phi$*) if, for all models* $\mathcal{M}$*, for all worlds* t*, if* $\mathcal{M}, t \models \Gamma$*, then* $\mathcal{M}, t \models \phi$*.*
The relations $\leq$ *and* R_A *must satisfy the following conditions:*

(S-Int) $\forall t, s, z \in S$, if $s \leq t$ and tR_Az then sR_Az;
(S-UNIT) $\forall t, s \in S$, if sR_At, then $s \leq t$;
(S-C) $\forall t, s, z \in S$, if sR_At and $t \leq z$, then zR_Az;
(S-CA) $R_{A\vee B}(t) = R_A(t) \cup R_B(t)$.
(S-Mon) $\forall t, s, z \in S$, if $sR_{A\wedge B}t$, then sR_At and sR_Bt;

(S-DT) $\forall t, s, z \in S$, if sR_At and $t \leq z$, and $z \in [|B|]$, then $sR_{A\wedge B}z$;
(S-ID) $\forall t, s \in S$, if sR_At, then $t \in [|A|]$;
(S-RCEA) if $[|A|] = [|B|]$, then $R_A = R_B$.

Condition (S-Int) enforces the property that when a formula A **says** ϕ is true in a world t, it is also true in all worlds reachable from s 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. (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 an *arbitrary* 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_At 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 departs from the semantic condition usually given to these axioms in conditional logic. This is due to the fact that $\mathsf{Cond}_{\mathrm{ACL}}$ is an intuitionistic conditional logic and the implication occurring within axioms is intuitionistic implication.

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:

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

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

Proposition 1. *In the axiomatization of* $\mathsf{Cond}_{\mathrm{ACL}}$ *, 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* $sR_{A\wedge B}t$.

This allows the semantic condition (S-DT) to be equivalently expressed as follows:

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

It is worth noticing that the notion of logical consequence defined above can be used to verify that a request ϕ of a principal A is compliant with a set of policies. Intuitively, given a set of formulas Γ representing policies, we say that A is compliant with Γ iff Γ, A **says** $\phi \models \phi$. For instance, if Γ contains the following formulas:

- $Admin_1$ **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** $delete\_file_1)) \rightarrow delete\_file_1)$

we obtain that $\Gamma, user_1$ **says** $delete\_file_1 \models delete\_file_1$.

[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 [8] Section 4.4).

3 Soundness and Completeness

In this section we prove that the axiomatization of the logic $\mathsf{Cond}_{\mathrm{ACL}}$ given above is sound and complete with respect to the semantics of Definition 1. The completeness proof we present is based on the proof of completeness for the Kripke semantics of intuitionistic logic in [22] and extends it to deal with the modalities **says** in the language and, more precisely, with the interplay between the relation $\leq$ and the accessibility relations R_A associated with the modalities.

Definition 2 (Consistency). *Let Γ be a set of well formed formulas. Γ is consistent iff $\Gamma \nvdash \bot$. If Γ has an infinite number of formulas, we say that Γ is consistent iff there are no finite $\Gamma_0 \subset \Gamma$ such that $\Gamma_0 \vdash \bot$.*

Definition 3 (Saturation). *Let Γ be a set of well formed formulas, we say that Γ is saturated iff 1. Γ is consistent (Definition 2); 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 Γ be a set of well formed formulas. Suppose $\Gamma \nvdash \varphi$, then there is a saturated set Γ^* such that $\Gamma^* \nvdash \varphi$.*

Definition 4 (Canonical model construction). *Let Γ_0 be any saturated set of formulas. Then we define $\mathbf{M} = (S, \leq, \{R_A\}, h)$ such that: S is the set of all saturated $\Gamma \supseteq \Gamma_0$; $\Gamma_1 \leq \Gamma_2$ 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 (proofs are in the Appendix):

Lemma 2. *For all $\Gamma \in S$ and each formula $\varphi \in \mathcal{L}$, we have that $\mathbf{M}, \Gamma \models \varphi$ iff $\varphi \in \Gamma$.*

Lemma 3. *Let $\mathbf{M}$ be the canonical model as defined in Definition 4. $\mathbf{M}$ satisfies the conditions (S-Int), (S-UNIT), (S-C), (S-CA), (S-Mon), (S-DT), (S-ID), and (S-RCEA).*

By the above lemmas, we can conclude tha the axiomatization of the logic $\mathsf{Cond}_{\mathrm{ACL}}$ given in Section 2.1 is complete with respect to the semantics in Definition 1:

Theorem 3 (Soundness and Completeness). *Given a formula $\varphi \in \mathcal{L}$, $\models \varphi$ iff $\vdash \varphi$.*

Proof. Soundness is straightforward. Concerning the completeness, for a contradiction, suppose $\nvdash \varphi$. Then by Lemma 1 there is a saturated extension Γ^* such that $\Gamma^* \nvdash \varphi$, hence $\varphi \notin \Gamma^*$. By Definition 4 and Lemmas 2 and 3, we conclude that there is a (canonical) model $\mathbf{M} = (S, \leq, \{R_A\}, h)$, with $\Gamma^* \in S$, such that $\mathbf{M}, \Gamma^* \not\models \varphi$. It follows that φ is not logically valid, i.e. $\not\models \varphi$. □

4 A sequent calculus for $\mathsf{Cond}_{\mathrm{ACL}}$

In this section we present a cut-free sequent calculus for $\mathsf{Cond}_{\mathrm{ACL}}$. 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 [21]. We also show that we can control the application of some crucial rules of $\mathcal{S}_{\mathsf{Cond}_{\mathrm{ACL}}}$, obtaining a terminating calculus $\widehat{\mathcal{S}_{\mathsf{Cond}_{\mathrm{ACL}}}}$. This calculus describes a decision procedure for $\mathsf{Cond}_{\mathrm{ACL}}$, and allows us to conclude that provability is decidable in $O(n^2 log n)$ space.

In addiction to the language $\mathcal{L}$ of the logic $\mathsf{Cond}_{\mathrm{ACL}}$, we consider a denumerable alphabet of labels $\mathcal{A}$, 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 Γ, a request φ of compliance of a principal A (i.e. we want to verify whether Γ, 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 ϕ, B **says** ϕ appears in Γ.

The calculus $\mathcal{S}_{\mathsf{Cond}_{\mathrm{ACL}}}$ manipulates three types of labelled formulas: 1. *world formulas*, denoted by $x : \alpha$, where $x \in \mathcal{A}$ and $\alpha \in \mathcal{L}$, used to represent that the formula α 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 $\Gamma \Rightarrow \Delta$, where Γ and Δ are multisets of labelled formulas. The intuitive meaning of a sequent $\Gamma \Rightarrow \Delta$ is: every model that satisfies all labelled formulas of Γ in the respective worlds (specified by the labels) satisfies at least one of the labelled formulas of Δ (in those worlds). This is made precise by the notion of *validity* of a sequent given in the next definition:

Definition 5 (Sequent validity). *Given a model $\mathcal{M} = (S, \leq, \{R_A\}, h)$ for $\mathcal{L}$, and a label alphabet $\mathcal{A}$, we consider a* mapping $I : \mathcal{A} \rightarrow S$. *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 $I(x)R_AI(y)$; • $\mathcal{M} \models_I y \geq x$ iff $I(x) \leq I(y)$. We say that $\Gamma \Rightarrow \Delta$ is* valid *in $\mathcal{M}$ if, for every mapping $I : \mathcal{A} \rightarrow S$, 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 $\Gamma \Rightarrow \Delta$ is valid in* $\mathsf{Cond}_{\mathrm{ACL}}$ *if it is valid in every $\mathcal{M}$.*

In Figure 1 we present the rules of the calculus $\mathcal{S}_{\mathsf{Cond}_{\mathrm{ACL}}}$ for $\mathsf{Cond}_{\mathrm{ACL}}$. As usual, we say that a sequent $\Gamma \Rightarrow \Delta$ 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 $\Gamma_1 \Rightarrow \Delta_1, \Gamma_2 \Rightarrow \Delta_2, \ldots, \Gamma_n \Rightarrow \Delta_n, \ldots$ Each node $\Gamma_i \Rightarrow \Delta_i$ is obtained from its immediate successor $\Gamma_{i-1} \Rightarrow \Delta_{i-1}$ by applying *backward* a rule of $\mathcal{S}_{\mathsf{Cond}_{\mathrm{ACL}}}$, having $\Gamma_{i-1} \Rightarrow \Delta_{i-1}$ as the conclusion and $\Gamma_i \Rightarrow \Delta_i$ 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 $\Gamma \Rightarrow \Delta$ has a derivation in $\mathcal{S}_{\mathsf{Cond}_{\mathrm{ACL}}}$ if there is a closed tree having $\Gamma \Rightarrow \Delta$ as a root.

The rule (EQ) is used in order to support the rule (RCEA): if a sequent $\Gamma, x \xrightarrow{A} y \Rightarrow \Delta, x \xrightarrow{B} y$ has to be proved, then the calculus $\mathcal{S}_{\mathsf{Cond}_{\mathrm{ACL}}}$ checks whether A and B are equivalent, i.e. $A \leftrightarrow B$. To this aim, the (EQ) rule introduces a branch in the backward derivation, trying to find a proof for both sequents $u : A \Rightarrow u : B$ and $u : B \Rightarrow u : A$. The restrictions on the rules $(\vee R)$, $(\wedge R)$, $(\neg R)$, $(\rightarrow R)$, (**says** R), and (EQ) are necessary to preserve the soundness of the calculus. As an example, in Figure 2 we show a derivation in $\mathcal{S}_{\mathsf{Cond}_{\mathrm{ACL}}}$ of an instance of the axiom (UNIT). In order to show that the formula $\alpha \rightarrow (A$ **says** $\alpha)$ is valid, we build a derivation in $\mathcal{S}_{\mathsf{Cond}_{\mathrm{ACL}}}$ for the sequent $\Rightarrow u : \alpha \rightarrow (A$ **says** $\alpha)$.

The calculus $\mathcal{S}_{\mathsf{Cond}_{\mathrm{ACL}}}$ is sound and complete with respect to the semantics:

Theorem 4 (Soundness and Completeness of $\mathcal{S}_{\mathsf{Cond}_{\mathrm{ACL}}}$). *A sequent $\Gamma \Rightarrow \Delta$ is valid in the sense of Definition 5 if and only if $\Gamma \Rightarrow \Delta$ is derivable.*

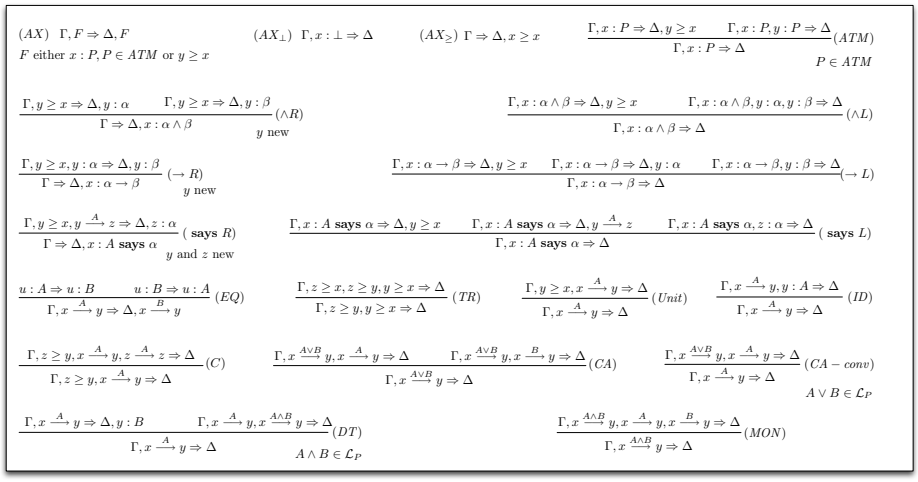

Fig. 1. The sequent calculus $\mathcal{S}_{\mathsf{Cond}_{\mathrm{ACL}}}$. Rules for $\neg$ and $\vee$ are omitted to save space.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\ldots, z \geq x \Rightarrow z : \alpha, z \geq x}(AX) \quad \dfrac{}{\ldots, x : \alpha, z : \alpha \Rightarrow z : \alpha}(AX)}{z \geq x, z \geq y, y \geq x, x \geq u, x : \alpha, y \xrightarrow{A} z \Rightarrow z : \alpha}(ATM)}{z \geq y, y \geq x, x \geq u, x : \alpha, y \xrightarrow{A} z \Rightarrow z : \alpha}(TR)}{y \geq x, x \geq u, x : \alpha, y \xrightarrow{A} z \Rightarrow z : \alpha}(Unit)}{x \geq u, x : \alpha \Rightarrow x : A \textbf{ says } \alpha}(\textbf{ says } R)}{\Rightarrow u : \alpha \rightarrow (A \textbf{ says } \alpha)}(\rightarrow R)$$

Fig. 2. A derivation in $\mathcal{S}_{\mathsf{Cond}_{\mathrm{ACL}}}$ for (UNIT).

Proof. **(Soundness)** By induction on the height of the derivation of $\Gamma \Rightarrow \Delta$. We only present the inductive step for the case in which the derivation of $\Gamma', x \xrightarrow{A} y \Rightarrow \Delta$ ends by an application of $(Unit)$: by inductive hypothesis, the premise $\Gamma', x \xrightarrow{A} y, y \geq x \Rightarrow \Delta$ 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 1, 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.

(Completeness) It is an easy consequence of the admissibility of *cut* and of some basic standard structural properties (height-preserving admissibility of weakening and invertibility of the rules, definitions and details can be found in the Appendix). We have to prove that the axioms are derivable and that the set of derivable formulas is closed under (MP), (RCEA), and (RCK). In Figure 2 we have shown a derivation of the axiom (UNIT). Derivations for (TAUT), (K), (C), (CA), (CA-conv), (Mon), (DT), and (ID) are omitted for lack of space. For (MP), suppose we have a derivation for $(i) \ \Rightarrow x : \alpha$ and $(ii) \ \Rightarrow x : \alpha \rightarrow \beta$. Since weakening is admissible, we have that also $(i') \ \Rightarrow x : \alpha, x : \beta$ and $(ii')\ x : \alpha \Rightarrow x : \alpha \rightarrow \beta, x : \beta$ have a derivation in $\mathcal{S}_{\mathsf{Cond}_{\mathrm{ACL}}}$.

Since (cut) is admissible, we can conclude that $\Rightarrow x : \beta$ is derivable as follows:

$$\dfrac{(i')\ \Rightarrow x : \alpha, x : \beta \qquad \dfrac{(ii')x : \alpha \Rightarrow x : \alpha \to \beta, x : \beta \qquad \dfrac{x : \alpha \to \beta, x : \alpha \Rightarrow x : \beta, x \geq x \quad x : \alpha \to \beta, x : \alpha \Rightarrow x : \beta, x : \alpha \quad x : \alpha \to \beta, x : \alpha, x : \beta \Rightarrow x : \beta}{x : \alpha \to \beta, x : \alpha \Rightarrow x : \beta}(\to L)}{x : \alpha \Rightarrow x : \beta}(cut)}{\Rightarrow x : \beta}(cut)$$

For (RCEA), we proceed as follows. As usual, $\vdash A \leftrightarrow B$ is a shorthand for $\vdash A \to B$ and $\vdash B \to A$. Suppose we have a derivation for $\Rightarrow u : A \to B$ and for $\Rightarrow u : B \to A$. We have shown that we have derivations for $u : A \Rightarrow u : B$ and $u : B \Rightarrow u : A$ (see the Appendix). The following derivation shows that also $\Rightarrow u : (A \textbf{ says } \gamma) \to (B \textbf{ says } \gamma)$ is derivable in $\mathcal{S}_{\mathsf{Cond}_{\mathrm{ACL}}}$ (the other half is symmetric):

$$\dfrac{\dfrac{\dfrac{u : A \Rightarrow u : B \qquad u : B \Rightarrow u : A}{\ldots, y \stackrel{B}{\longrightarrow} z \Rightarrow y \stackrel{A}{\longrightarrow} z, \ldots}(EQ) \qquad \ldots, y \geq x \Rightarrow y \geq x, \ldots \qquad \ldots, z : \gamma \Rightarrow z : \gamma, \ldots}{y \geq x, x \geq u, x : A \textbf{ says } \gamma, y \stackrel{B}{\longrightarrow} z \Rightarrow z : \gamma}(\textbf{ says } L)}{x \geq u, x : A \textbf{ says } \gamma \Rightarrow x : B \textbf{ says } \gamma}(\textbf{ says } R)}{\Rightarrow u : (A \textbf{ says } \gamma) \to (B \textbf{ says } \gamma)}(\to R)$$

For (RCK), suppose there is a derivation for $\Rightarrow y : \alpha \to \beta$. Since $(\to R)$ is invertible, we have also a derivation of $(I)\ z \geq y, z : \alpha \Rightarrow z : \beta$ and, by weakening, of $(I')\ z \geq y, y \geq x, y \stackrel{A}{\longrightarrow} z, x \geq u, x : A \textbf{ says } \alpha, z : \alpha \Rightarrow z : \beta$, from which we conclude:

$$\dfrac{\dfrac{\dfrac{\ldots, y \geq x \Rightarrow y \geq x \ldots \qquad \dfrac{(I')\ z \geq y, y \geq x, y \stackrel{A}{\longrightarrow} z, x \geq u, x : A \textbf{ says } \alpha, z : \alpha \Rightarrow z : \beta}{y \geq x, y \stackrel{A}{\longrightarrow} z, x \geq u, x : A \textbf{ says } \alpha, z : \alpha \Rightarrow z : \beta}(Unit)}{\ldots, y \stackrel{A}{\longrightarrow} z \Rightarrow y \stackrel{A}{\longrightarrow} z, \ldots}(\textbf{ says } L)}{y \geq x, y \stackrel{A}{\longrightarrow} z, x \geq u, x : A \textbf{ says } \alpha \Rightarrow z : \beta}(\textbf{ says } R)}{x \geq u, x : A \textbf{ says } \alpha \Rightarrow x : A \textbf{ says } \beta}(\to R)}{\Rightarrow u : (A \textbf{ says } \alpha) \to (A \textbf{ says } \beta)}$$

□

Completeness of $\mathcal{S}_{\mathsf{Cond}_{\mathrm{ACL}}}$ with respect to $\mathsf{Cond}_{\mathrm{ACL}}$ models of Definition 1 immediately follows from the completeness of the axiomatization of $\mathsf{Cond}_{\mathrm{ACL}}$ with respect to the semantics, shown in Theorem 3. We have that a formula $\varphi \in \mathcal{L}$ is valid if and only if the sequent $\Rightarrow u : \varphi$ has a derivation in $\mathcal{S}_{\mathsf{Cond}_{\mathrm{ACL}}}$.

4.1 Termination and complexity of $\mathcal{S}_{\mathsf{Cond}_{\mathrm{ACL}}}$

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 $(\textbf{ says } L)$, $(\to L)$, $(Unit)$, $(ID), \ldots$, 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, and then that the rules of $\mathcal{S}_{\mathsf{Cond}_{\mathrm{ACL}}}$ introduce only a finite number of labels. These facts allow us to describe a decision procedure $\widehat{\mathcal{S}_{\mathsf{Cond}_{\mathrm{ACL}}}}$ for the logic $\mathsf{Cond}_{\mathrm{ACL}}$, and to give an explicit complexity bound for it. First of all, we need the following lemmas:

Lemma 4. *If a sequent $\Gamma \Rightarrow \Delta, y \geq x$ is derivable in $\mathcal{S}_{\mathsf{Cond}_{ACL}}$, then either $\Gamma \Rightarrow \Delta$ is derivable or $y \geq x \in \Gamma$ or $y = x$.*

Lemma 5. *If a sequent $\Gamma \Rightarrow \Delta, y \xrightarrow{A} z$ is derivable in $\mathcal{S}_{\mathsf{Cond}_{ACL}}$, then either $\Gamma \Rightarrow \Delta$ is derivable or $y \xrightarrow{A'} z \in \Gamma$.*

The following facts allow to obtain a terminating calculus from $\mathcal{S}_{\mathsf{Cond}_{\mathrm{ACL}}}$:
• The rules of $\mathcal{S}_{\mathsf{Cond}_{\mathrm{ACL}}}$ introduce only a finite number of labels in a backward proof search: labels are only introduced by the rules $(\otimes R)$, where $\otimes$ stands for $\{\neg, \rightarrow, \wedge, \vee\}$, by formulas occurring negatively in the initial sequent, which are finite.
• It is useless to apply the rules (TR), $(Unit)$, (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 $\Gamma, x \xrightarrow{A} y \Rightarrow \Delta$ 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 $A \vee B$ in the premise, where $A \vee B$ is a principal belonging to $\mathcal{L}_{\mathbf{P}}$. The same for (DT), introducing $A \wedge B$. Since $\mathcal{L}_{\mathbf{P}}$ is finite, these rules will be applied a finite number of times in the same branch.
• Each of the rules $(\otimes L)$, applied to a sequent $\Gamma, x : \phi \Rightarrow \Delta$, leads to a premise of the form $\Gamma, x : \phi \Rightarrow \Delta, y \geq x$, and can thus be reapplied without any control. However, it is useless to apply $(\otimes L)$ on the same formula $x : \phi$ 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 4 we can restrict the choice of the order formula $y \geq x$ to introduce in a way such that either $y \geq x \in \Gamma$ or $y = x$: this is explained by the fact that no rule of $\mathcal{S}_{\mathsf{Cond}_{\mathrm{ACL}}}$ 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 Γ) or by $(AX_{\geq})$, thus choosing $y = x$. The same for (ATM).

This is not enough to ensure termination. Indeed, a sequence of applications of $(\otimes L)$, $(\otimes R)$ and (TR) might lead to the generation of infinite labels in a branch. As an example, consider the sequent $x : (P \rightarrow Q) \rightarrow R \Rightarrow$, to which $(\rightarrow L)$ can be applied by using x itself, obtaining $x : (P \rightarrow Q) \rightarrow R \Rightarrow x : P \rightarrow Q$ in the premise in the middle. We can then apply $(\rightarrow R)$, obtaining $y \geq x, x : (P \rightarrow Q) \rightarrow R, y : P \Rightarrow y : Q$, where y is a new label. y can then be used to apply $(\rightarrow L)$, leading to a premise $y \geq x, x : (P \rightarrow Q) \rightarrow R, y : P \Rightarrow y : Q, y : P \rightarrow Q$, to which a further application of $(\rightarrow R)$ introduces a new label z in the premise $z \geq y, y \geq x, x : (P \rightarrow Q) \rightarrow R, y : P, z : P \Rightarrow y : Q, z : Q$. An application of (TR) introduces $z \geq x$ in the left-hand side of the sequent, then $(\rightarrow L)$ can be applied to $x : (P \rightarrow Q) \rightarrow R$ by using z, obtaining the sequent $z \geq x, z \geq y, y \geq x, x : (P \rightarrow Q) \rightarrow R, y : P, z : P \Rightarrow y : Q, z : Q, z : P \rightarrow Q$, to which $(\rightarrow R)$ can be further applied to introduce a new label $z' \geq z$, then $z' \geq x$ by (TR) and so on. Termination is ensured by the following side condition on the application of the rules $(\otimes L)$. Given a sequent $\Gamma \Rightarrow \Delta$ and two labels x and y such that $y \geq x \in \Gamma$, we define the distance $d(y, x)$ between the two labels as: $d(x, x) = 0$ and $d(y, x) = n$ if n is the length of the *longest* sequence of *order formulas* in Γ "connecting" the two labels, i.e. $y \geq z_1, z_1 \geq z_2, \ldots, z_{n-1} \geq x \in \Gamma$. Given a derivation starting with $\Rightarrow x_0 : \phi$, let τ be the heigth of the parse tree of ϕ. We

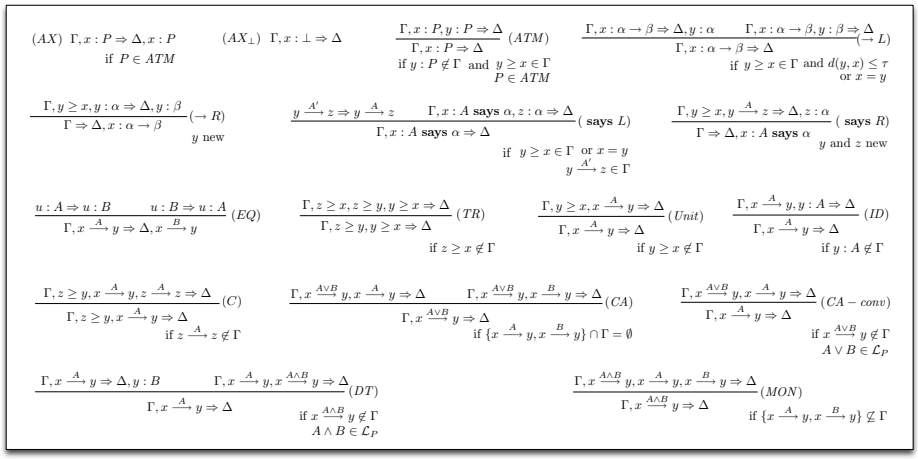

Fig. 3. The terminating calculus $\widehat{\mathcal{S}_{\mathsf{Cond}_{\mathrm{ACL}}}}$. To save space, we omit the rules for $\wedge$. (AX) is restricted to atomic formulas. $(AX_{\geq})$ is no needed due to the reformulation of the other rules.

can show that we can restrict the application of a rule $(\otimes L)$ to $x : \alpha \otimes \beta$ to the case in which the label y used in the premise(s) is such that $d(y, x) \leq \tau$, that is to say it is useless to apply the rule by using a label whose distance with x is higher than the height of the parse tree of the initial formula.

• Similarly to the previous point, it is useless to apply (**says** L) on the same formula $x : A$ **says** α more than once in each branch, introducing (backward) the same formulas $y \geq x$ and $y \xrightarrow{A} z$ in the leftmost and in the inner premises, respectively. Moreover, by Lemma 5, the choice of the transition $y \xrightarrow{A} z$ to be used is restricted to formulas such that, for some formula A', there exists $y \xrightarrow{A'} z \in \Gamma$. 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 $y \xrightarrow{A} z$ can be reduced to $y \xrightarrow{A'} z \Rightarrow y \xrightarrow{A} z$.

The resulting terminating calculus $\widehat{\mathcal{S}_{\mathsf{Cond}_{\mathrm{ACL}}}}$ is shown in Figure 3. This itself gives the decidability of $\mathsf{Cond}_{\mathrm{ACL}}$.

Theorem 5. *The sequent calculus $\widehat{\mathcal{S}_{\mathsf{Cond}_{\mathrm{ACL}}}}$ ensures a terminating proof search, then the logic $\mathsf{Cond}_{\mathrm{ACL}}$ is decidable.*

Proof. Given a formula ϕ, just observe that there is only a finite number of derivations of the sequent $\Rightarrow x_0 : \phi$, as both the length of a proof and the number of labelled formulas which may occur in it is finite. □

We can give an explicit space complexity bound for $\mathsf{Cond}_{\mathrm{ACL}}$. 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 [16, 21].

Theorem 6. *Provability in $\mathsf{Cond}_{\mathrm{ACL}}$ is decidable in $O(n^2 \log n)$ space.*

5 Other Axioms

This work can be considered as a first step towards providing a general framework for the definition of axiomatization, semantics and proof methods for access control logics by the application of constructive conditional logics. While here we have considered the logic $\mathsf{Cond}_{\mathrm{ACL}}$, other axioms have been proposed in the literature and different access control logics have been defined through their combination. Among the most relevant axioms we mention the following ones:

(C4) $(A \textbf{ says } (A \textbf{ says } \alpha)) \rightarrow (A \textbf{ says } \alpha)$
(I) $(A \textbf{ says } \alpha) \rightarrow (B \textbf{ says } A \textbf{ says } \alpha)$
(Speaks For) $(A \Rightarrow B) \rightarrow ((A \textbf{ says } \alpha) \rightarrow (B \textbf{ says } \alpha))$
(Handoff) $(A \textbf{ says } (B \Rightarrow A)) \rightarrow (B \Rightarrow A)$

(C4) belongs to the original axiomatization of the logic ICL defined in [11], where it replaces the axiom (C). In [13] it has been shown that the semantical property corresponding to (C4) is the following:

(S-C4) $\forall t, s \in S$, if sR_At, then $\exists z \in S$ such that sR_Az and zR_At

(I) is introduced in the axiomatization of the logic Binder [7], which extends the logic ABLP [3, 17] in order to express the so called *authorization policies*. Notice that this is a weaker version of (Unit). The corresponding semantical property is:

(S-I) $\forall t, s, u \in S$, if tR_Bs and sR_Au, then sR_Au

The connective $\Rightarrow$ occurring in (Speaks For) and (Handoff) is a well known connective introduced in the logic ABLP [3, 17] to reason about transfer of authority from one principal to another. $A \Rightarrow B$ (A speaks for B) means that if A says α, then also B says α for any α. The axioms (Speaks for) and (Handoff) relate the connective $\Rightarrow$ with the **says** modality. The semantic conditions for the axioms (Speaks For) and (Handoff) have been studied in [14].

Our next step will be to extend our conditional framework in order to capture these axioms, so to provide automated deduction tools for the above mentioned logics including them.

6 Related work and Conclusions

Related Work. The formal study of properties of access control logics is a recent research trend. As reported in [12], constructive logics are 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, allows proofs that discard evidence.

Abadi in [1] presents a formal study about connections between many possible axiomatizations of the says, 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 K says $\varphi \rightarrow (\varphi \vee K$ says $\psi)$. The axiom above is called *Escalation* and it represents a rather degenerate interpretation of says, i.e., if a principal says φ then, either φ is permitted 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 [11] translate existing access control logics into S4 by relying on a slight simplification of Gödel's translation from intuitionistic logic to S4, and extending it to formulas of the form A says φ.

Garg [10] adopts an ad-hoc version of constructive S4 called DTL_0 and embeds existing approaches into it. Constructive S4 has been chosen because of its intuitionistic Kripke semantics which DTL_0 extends by adding *views* [10], i.e., a mapping from worlds to sets of principals.

Boella et al. [6] define a logical framework called FSL (Fibred Security Language), based on fibring semantics [9] by looking at says as a (fibred) modal operator.

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 $\Box_K$, if we rely on S4 we would have as an axiom $\Box_K\varphi \rightarrow \varphi$, which means: *everything* that K says is permitted. To overcome this problem, both in [10, 11], Kripke semantics is sweetened 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.

Conclusions. We defined an intuitionistic conditional logic for Access Control called $\mathsf{Cond}_{\mathrm{ACL}}$. The major contribution of our conditional approach w.r.t. works in [10, 11] is the identification of canonical properties for axioms of the logic (in particular Unit and C), i.e., first-order conditions on Kripke structures that are *necessary* and *sufficient* for the corresponding axiom to hold. [6, 13, 14] identify canonical properties for other access control axioms (e.g., C4, speaks-for, hand-off).

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 arbitrary formulas. In spite of this generality, we have shown that provability in $\mathsf{Cond}_{\mathrm{ACL}}$ is decidable in $O(n^2 logn)$ space, in agreement with the results given in [11] for the logic ICL. 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 [18, 4, 15], but the translation in [11] does not provide an embedding in S4 for a logic without Unit. In general, the approach in [11] 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.

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. To this concern, we have followed the approach proposed in [21] for standard normal conditional logics, which we have extended here to deal with an intuitionistic logic as well as with specific access control axioms.

For the time being, $\mathsf{Cond}_{\mathrm{ACL}}$ only includes few widely accepted axioms of access control logics but it can be extended in order to cope with richer axioms, as well as with the well known notion of "speaks for". This is what we plan to do in future work.

References

1. M. Abadi. Variations in access control logic. In *DEON08*, pages 96–109, 2008.
2. M. Abadi, M. Burrows, B. W. Lampson, and G. D. Plotkin. A calculus for access control in distributed systems. In *CRYPTO 91*, pages 1–23, 1991.
3. M. Abadi, M. Burrows, B.W. Lampson, and G.D. Plotkin. A calculus for access control in distributed systems. *ACM Tran. on Progr. Lang. and Systems*, 15(4):706–734, 1993.
4. M.Y. Becker, C.Fournet, and A.D. Gordon. Design and semantics of a decentralized authorization language. In *IEEE CSF 2007)*, pages 3–15, 2007.
5. C. Bertolissi, M. Fernández, and S. Barker. Dynamic event-based access control as term rewriting. In *DBSec07*, pages 195–210, 2007.
6. G. Boella, D. Gabbay, V. Genovese, and L. van der Torre. Fibred security language. *Studia Logica*, 92(3):395–436, 2009.
7. J. DeTreville. Binder, a logic-based security language. In *IEEE Symposium on Security and Privacy*, pages 105–113, 2002.
8. H.B. Enderton. *A Mathematical Introduction to Logic, 2nd Edition*. Academic Press, 2000.
9. D.M. Gabbay. Fibring logics. *Oxford University Press*, 1999.
10. D. Garg. Principal centric reasoning in constructive authorization logic. In *IMLA*, 2008.
11. D. Garg and M. Abadi. A modal deconstruction of access control logics. In *FoSSaCS08*, pages 216–230.
12. D.Garg and F.Pfenning. Non-interference in constructive authorization logic. In *CSFW-19*, pages 283–296, 2006.
13. V. Genovese, L. Giordano, V. Gliozzi, and G. L. Pozzato. A constructive conditional logic for access control: a preliminary report. In *ECAI 2010*, pages 1073–1074.
14. V. Genovese, D. Rispoli, D.M. Gabbay, and L. van der Torre. modal Access Control Logic: Axiomatization, Semantics and FOL Theorem Proving. In *STAIRS 2010*, pages 114–126.
15. Y. Gurevich and A. Roy. Operational semantics for DKAL: Application and analysis. In *TrustBus 2009*, pages 149–158, 2009.
16. J. Hudelmaier. An $\mathcal{O}(n\ log\ n)$-space decision procedure for intuitionistic propositional logic. *Journal of Logic and Computation*, 3(1):63–75, 1993.
17. B.W. Lampson, M. Abadi, M.Burrows, and E.Wobber. Authentication in distributed systems: Theory and practice. *ACM Transactions on Computer Systems*, 10(4):265–310, 1992.
18. C. Lesniewski-Laas, B. Ford, J. Strauss, R. Morris, and M. F. Kaashoek. Alpaca: extensible authorization for distributed services. In *Proc. of ACM CCS 2007*, pages 432–444.
19. N. Li, B. N. Grosof, and J. Feigenbaum. Delegation logic: A logic-based approach to distributed authorization. *ACM Trans. Inf. Syst. Secur.*, 6(1):128–171, 2003.
20. D. Nute. *Topics in Conditional Logic*. Reidel, Dordrecht, 1980.
21. N. Olivetti, G. L. Pozzato, and C. B. Schwind. A Sequent Calculus and a Theorem Prover for Standard Conditional Logics. *ACM Transactions on Computational Logics*, 8(4), 2007.
22. A.S. Troelstra and D. van Dalen. *Constructivism in Mathematics: An Introduction*. 1988.

APPENDIX

Proofs of Section 2

Proof of Proposition 1. In the axiomatization of Cond_{ACL} , 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. □

Proofs of Section 3

In order to prove Lemma 2, we need to prove the following Lemma:

Lemma 6. *Let Γ be a set of formulas and let $\Delta = \{\varphi : A$ **says** $\varphi \in \Gamma\}$. If $\Delta \vdash \psi$, then $\Gamma \vdash A$ **says** ψ.*

Proof. Suppose there is a derivation of ψ from Δ. Then, there must be a finite set of formulas $\{\varphi_1, \ldots, \varphi_n\} \subseteq \Delta$ such that $\{\varphi_1, \ldots, \varphi_n\} \vdash \psi$. By definition of $\vdash$, $\vdash \varphi_1 \wedge \ldots \wedge \varphi_n \rightarrow \psi$. By (RCK) and (K), $\vdash A$ **says** $\varphi_1 \wedge \ldots \wedge A$ **says** $\varphi_n \rightarrow A$ **says** ψ, 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** ψ. □

Now we can prove Lemma 2 in Section 3:

Proof of Lemma 2. 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 φ. In case φ is an atomic formula, the lemma holds by definition. 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 Γ). For $\varphi \equiv \phi \rightarrow \psi$, suppose $\Gamma \models \phi \rightarrow \psi$. Then for all saturated $\Gamma' \supset \Gamma$ we have that if $\Gamma' \models \phi$, then $\Gamma' \models \psi$. Assume $\Gamma \not\models \phi \rightarrow \psi$, then $\Gamma \cup \{\phi\} \not\models \psi$; let Γ' be a saturated extension of $\Gamma \cup \{\phi\}$ such that $\Gamma' \not\models \psi$, 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 Γ is saturated, by condition 2 in Definition 3, $\phi \rightarrow \psi \in \Gamma$. The converse is trivial. For $\varphi \equiv A$ **says** ϕ, suppose $\Gamma \models A$ **says** ϕ. Hence, for all Γ' 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 3, $\Gamma \not\models A$ **says** ϕ. Then, by Lemma 6, $\Delta \not\models \phi$. By Lemma 1, there is a saturated extension Δ^* of Δ such that $\Delta^* \not\models \phi$, i.e. $\phi \notin \Delta^*$. By definition of R_A, $\Gamma R_A\Delta^*$. This contradicts the fact that, for all Γ' such that $\Gamma R_A\Gamma'$, $\phi \in \Gamma'$. The converse is trivial. □

Proof of Lemma 3. Let $\mathbf{M}$ be the canonical model as defined in Definition 4. $\mathbf{M}$ satisfies the conditions (S-Int), (S-UNIT), (S-C), (S-CA), (S-Mon), (S-DT), (S-ID), and (S-RCEA).

Proof. The proof is straightforward. As an example, let us prove (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. $\{\phi$ such that $A \wedge B$ **says** $\phi \in \Gamma\} \subseteq \Gamma''$. For all such ϕ, by (DT), A **says** $(B \to \phi) \in \Gamma$, hence by definition of R_A, $B \to \phi \in \Gamma'$, and by definition of $\leq$, $B \to \phi \in \Gamma''$. Furthermore, also $B \in \Gamma''$ by Lemma 2. By deductive closure of Γ'', we conclude that $\phi \in \Gamma''$. □

Admissibility of cut in $\mathcal{S}_{\mathsf{Cond_{ACL}}}$

We first need to show some basic structural properties of $\mathcal{S}_{\mathsf{Cond_{ACL}}}$:

Lemma 7 (Height-preserving admissibility of weakening). *If $\Gamma \Rightarrow \Delta$ has a derivation of height h, then $\Gamma \Rightarrow \Delta, F$ and $\Gamma, F \Rightarrow \Delta$ have a derivation of height $h' \leq h$.*

Lemma 8 (Height-preserving label substitution). *If a sequent $\Gamma \Rightarrow \Delta$ has a derivation of height h, then $\Gamma[x/y] \Rightarrow \Delta[x/y]$ has a derivation of height $h' \leq h$, where $\Gamma[x/y] \Rightarrow \Delta[x/y]$ is the sequent obtained from $\Gamma \Rightarrow \Delta$ by replacing all occurrences of the label x by the label y.*

Lemma 9 (Height-preserving invertibility of rules). *Let $\Gamma \Rightarrow \Delta$ be an instance of the conclusion of a rule R of $\mathcal{S}_{\mathsf{Cond_{ACL}}}$, with R different from (EQ). If $\Gamma \Rightarrow \Delta$ is derivable, then the premise(s) of R is (are) derivable with a derivation of (at most) the same height.*

Lemma 10 (Height-preserving admissibility of contraction). *If a sequent $\Gamma \Rightarrow \Delta, F, F$ is derivable in $\mathcal{S}_{\mathsf{Cond_{ACL}}}$, then there is a derivation of no greater height of $\Gamma \Rightarrow \Delta, F$, and if a sequent $\Gamma, F, F \Rightarrow \Delta$ is derivable in $\mathcal{S}_{\mathsf{Cond_{ACL}}}$, then there is a derivation of no greater height of $\Gamma, F \Rightarrow \Delta$.*

Lemma 11. *A sequent $\Rightarrow x : A \to B$ is derivable in $\mathcal{S}_{\mathsf{Cond_{ACL}}}$ if and only if the sequent $x : A \Rightarrow x : B$ is derivable in $\mathcal{S}_{\mathsf{Cond_{ACL}}}$.*

Proof. If $x : A \Rightarrow x : B$ is derivable, then, by Lemma 7, also $x \geq u, x : A \Rightarrow x : B$ is derivable. By an application of $(\to R)$, we obtain a derivation of $\Rightarrow u : A \to B$. By Lemma 8 we conclude with a derivation of $\Rightarrow x : A \to B$.

If $\Rightarrow x : A \to B$ is derivable, then we have also a derivation for $u \geq x, u : A \Rightarrow u : B$ since $(\to R)$ is invertible (Lemma 9). It can be observed that no rule of $\mathcal{S}_{\mathsf{Cond_{ACL}}}$ manipulate the label x, therefore the formula $u \geq x$ is useless. This means that there is a derivation of $u : A \Rightarrow u : B$ and, by Lemma 8, there is a derivation of $x : A \Rightarrow x : B$.

□

By cut we mean the following rule:

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

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. However, in our calculus $\mathcal{S}_{\mathsf{Cond}_{\mathrm{ACL}}}$ the standard proof does not work in case the cutting formula F is a transition formula $x \xrightarrow{A} y$ derived by an application of (EQ) in the left premise, and by an application of one of the following rules: $(C), (CA), (CA-conv), (DT), (MON)$ in the right premise. In the proof of Theorem 7 below, we present one of the cases above as an example, namely the case in which $x \xrightarrow{A} y$ is derived by (EQ) on the left and by (C) on the right. In order to prove the admissibility of cut for $\mathcal{S}_{\mathsf{Cond}_{\mathrm{ACL}}}$, we proceed as follows. First of all, we represent with $\Gamma[x_i \xrightarrow{A} y_i] \Rightarrow \Delta[u_j \xrightarrow{A} v_j]$ a sequent containing *any* number of transitions labelled with the formula A; moreover, if $u : A \Rightarrow u : A'$ and $u : A' \Rightarrow u : A$ are derivable, we denote with $\Gamma^\star \Rightarrow \Delta^\star$ the sequent obtained by replacing *any* number of transitions labelled with A with the same transitions labelled with A' in $\Gamma[x_i \xrightarrow{A} y_i] \Rightarrow \Delta[u_j \xrightarrow{A} v_j]$. We prove that cut is admissible by "splitting" the notion of cut in two propositions:

Theorem 7. *In $\mathcal{S}_{\mathsf{Cond}_{\mathrm{ACL}}}$, the following propositions hold:*

- *(A) If $\Gamma \Rightarrow \Delta, F$ and $\Gamma, F \Rightarrow \Delta$ are derivable, so is $\Gamma \Rightarrow \Delta$, i.e. the rule (cut) is admissible in $\mathcal{S}_{\mathsf{Cond}_{\mathrm{ACL}}}$;*
- *(B) if (I) $\Gamma[x_i \xrightarrow{A} y_i] \Rightarrow \Delta[u_j \xrightarrow{A} v_j]$ is derivable with a derivation of height h, (II) $u : A \Rightarrow u : A'$ and (III) $u : A' \Rightarrow u : A$ are derivable, then $\Gamma^\star \Rightarrow \Delta^\star$ is derivable with a derivation of height $h' \leq h$.*

Proof. By double mutual induction on the complexity of the cut formula and on the height of the derivations. To prove (A), the induction on the height is intended as usual as the sum of the heights of the premises of the cut inference; to prove (B), the induction on the height is intended as the height of the derivation of $\Gamma[x_i \xrightarrow{A} y_i] \Rightarrow \Delta[u_j \xrightarrow{A} v_j]$. We have several cases:

• Base for (A): one of the two premises of (cut) is an axiom. Here we only present the case in which $\Gamma \Rightarrow \Delta, F$ is an instance of (AX) since $F \in \Gamma$. We have that $\Gamma = \Gamma', F$; the right premise of (cut) is, therefore, $\Gamma', F, F \Rightarrow \Delta$ and, since contraction is admissible (Lemma 10), we have that also $\Gamma', F \Rightarrow \Delta$, i.e. $\Gamma \Rightarrow \Delta$, is derivable. The other cases are left to the reader.

• Base for (B): if $\Gamma[x_i \xrightarrow{A} y_i] \Rightarrow \Delta[u_j \xrightarrow{A} v_j]$ is an axiom, so is $\Gamma^\star \Rightarrow \Delta^\star$, since axioms do not involve transition formulas.

• Inductive step for (A): we distinguish the following two cases:

- 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 $\Gamma, F \Rightarrow \Delta$ 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 Γ and Δ. Therefore, we have a proof of $\Gamma \Rightarrow \Delta$ 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.
- F is the principal formula in the last step of *both* derivations of the premises of the cut inference. There are twelve 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 (CA) on the right, j) by (EQ) on the left and by $(CA-conv)$ on the right, k) by (EQ) on the left and by (DT) on the right, l) and by (EQ) on the left and by (MON) on the right. The list is exhaustive. Here we only present one of the most interesting cases h). We have the following derivation:

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

By (2) and Proposition (B), we have a derivation of at most the same height also for $(2')\ \Gamma', z \geq y, x \xrightarrow{A'} y, x \xrightarrow{A} y, z \xrightarrow{A'} z \Rightarrow \Delta$. By Lemma 7, from (1) we have a derivation of $(1')\ \Gamma', z \geq y, x \xrightarrow{A'} y, z \xrightarrow{A'} z \Rightarrow \Delta, x \xrightarrow{A} y$. By cutting $(1')$ and $(2')$, we obtain a derivation of $\Gamma', z \geq y, x \xrightarrow{A'} y, z \xrightarrow{A'} z \Rightarrow \Delta$ (this cut is eliminable by inductive hypothesis on the height of the derivations), then we can conclude by an application of (C).

• Inductive step for (B): we have to consider all possible derivations of $\Gamma[x_i \xrightarrow{A} y_i] \Rightarrow \Delta[u_j \xrightarrow{A} v_j]$. We only present the most interesting case, namely the one the derivation ends as follows:

$$\dfrac{(3)\ u : A \Rightarrow u : A'' \qquad (4)\ u : A'' \Rightarrow u : A}{\Gamma[x_i \xrightarrow{A} y_i], x \xrightarrow{A} y \Rightarrow \Delta[u_j \xrightarrow{A} v_j], x \xrightarrow{A''} y}(EQ)$$

We have to show that there is a derivation also for $\Gamma^\star, x \xrightarrow{A'} y \Rightarrow \Delta^\star, x \xrightarrow{A''} y$. By Proposition B, we have derivations for $(5)\ u : A \Rightarrow u : A'$ and $(6)\ u : A' \Rightarrow u : A$. By weakening (Lemma 7), we have also derivations of at most the same heights of $(3')\ u : A, u : A' \Rightarrow u : A''$, $(4')\ u : A'' \Rightarrow u : A', u : A$, $(5')\ u : A, u : A'' \Rightarrow u : A'$ and $(6')\ u : A' \Rightarrow u : A'', u : A$. We can conclude by replacing the initial cut as follows:

$$\dfrac{\dfrac{\begin{array}{l}(6')\ u : A' \Rightarrow u : A'', u : A \\ (3')\ u : A, u : A' \Rightarrow u : A''\end{array}}{u : A' \Rightarrow u : A''}(cut) \qquad \dfrac{\begin{array}{l}(4')\ u : A'' \Rightarrow u : A', u : A \\ (5')\ u : A, u : A'' \Rightarrow u : A'\end{array}}{u : A'' \Rightarrow u : A'}(cut)}{\Gamma^\star, x \xrightarrow{A'} y \Rightarrow \Delta^\star, x \xrightarrow{A''} y}(EQ)$$

Notice that the two applications of (cut) above can be eliminated by applying the inductive hypothesis on the complexity of the cut formula.

□