

# New Modalities for Access Control Logics: Permission, Control and Ratification

Valerio Genovese<sup>1</sup> and Deepak Garg<sup>2</sup>

<sup>1</sup> University of Luxembourg and University of Torino

<sup>2</sup> Carnegie Mellon University

**Abstract.** We present a new modal access control logic  $ACL^+$  to specify, reason about and enforce access control policies. The logic includes new modalities for permission, control, and ratification to overcome some limits of current access control logics. We present a Hilbert-style proof system for  $ACL^+$  and a sound and complete Kripke semantics for it. We exploit Kripke semantics to define  $Seq\text{-}ACL^+$ : a sound, complete, cut-free and terminating calculus for  $ACL^+$ , proving that  $ACL^+$  is decidable. We point at a Prolog implementation of  $Seq\text{-}ACL^+$  and discuss possible extensions of  $ACL^+$  with axioms for subordination between principals.

**Keywords:** Access Control, Delegation, Modal Logic

## 1 Introduction

Logic plays a prominent role in the specification, reasoning and enforcement of access control policies in distributed systems. In the last two decades, several logic-based formal systems for access control have been proposed (see [1,3] and [7] for surveys), each with its own primitives, semantics and, in some cases, specific application domains. The great variety (and complexity) of such systems makes it difficult to integrate, compare and objectively evaluate them. As is evident from recent research in access control [2,8,11,14,17], modal logic is a powerful framework to study expressiveness, decidability, complexity and semantics of access control logics. Although modal logic has proved useful for theoretical study of access control, it is not widely used in practice to enforce authorization policies (some notable exceptions are [5,6,13,21,22]).

The main reason for this gap is that although several epistemic modalities (e.g., says [18], said and knows [17]) have been studied in the context of access control, key access control concepts like permission, control or trust are not first-class citizens of modal access control languages and must be defined using epistemic modalities. This creates implicit relationships between the concepts and possibly leads to security risks (see [2] for some examples).

In this paper, we take a step towards addressing this shortcoming by proposing a constructive modal logic,  $ACL^+$ , which extends a standard access control logic with new connectives for permission, control and trust on principals' statements, and admits a decidable calculus. We start by presenting a brief outline of the methodology of access control through logics in Section 2, and a specific connective says [18] that is central

to almost all access control logics. In Section 3 we point at three shortcomings of says-based access control logics that, in our opinion, limit their applicability in practical scenarios, thus motivating the need for the new modalities. In Section 4 we present the new modalities, their axioms and inference rules in a Hilbert-style calculus for  $\text{ACL}^+$ . Moreover, we show through examples how  $\text{ACL}^+$  avoids the shortcomings reported in Section 3.

Section 5 presents sound and complete Kripke semantics for  $\text{ACL}^+$ . Kripke semantics, although useful for establishing several metatheorems of access control logics, are not operational and cannot be used directly in algorithms to reason about authorization problems. Accordingly, in Section 6 we present  $\text{Seq-ACL}^+$ , a sound, complete, cut-free and terminating calculus for  $\text{ACL}^+$ . In Section 7 we present extensions of  $\text{ACL}^+$  with axioms that force subordination between principals. Section 8 discusses briefly some related work and Section 9 concludes the paper. A full version of this paper with proofs of theorems and an implementation of the decision procedure for  $\text{ACL}^+$  are available from the authors' webpages.

## 2 Distributed Access Control Model

We consider a decentralized model of access control, where policy information is *distributed* among several principals. Principals support policy statements and credentials by writing them in certificates signed with their respective private keys. Since policy statements and credentials may be complex, and may assert facts conditional upon statements of other principals, *logic* is a natural choice to model policies. If principal  $A$  supports policy (or credential)  $\varphi$ , this is represented in the logic as the formula  $A$  says  $\varphi$  [18]. Technically,  $A$  says  $\bullet$  is a family of principal-indexed modalities that has been included in several access control logics, albeit with slightly varying semantic interpretations.

An access is authorized (justified) if and only if it is *entailed* by available policy statements and credentials. The question of authorizing an access  $\varphi$  for principal  $A$  from a policy  $\Gamma$  can be cast formally as follows: Is it the case that  $\Gamma$  and  $A$  says  $\varphi$  entail  $\varphi$ ? Or, in symbolic notation, is there a *proof* that  $\Gamma, A$  says  $\varphi \vdash \varphi$ ?

*Example 1.* Consider the following policy:

1. If the *Admin* says that *file1* can be read, then this must be the case<sup>1</sup>.
2. *Admin* trusts *Bob* to decide whether *file1* can be read.

In a propositional logic  $\mathcal{L}$  enriched with the says modality and equipped with an entailment relation  $\vdash_{\mathcal{L}}$ , we can express the above policy as follows [2]:

1.  $(\text{Admin says read\_file1}) \rightarrow \text{read\_file1}$
2.  $\text{Admin says } ((\text{Bob says read\_file1}) \rightarrow \text{read\_file1})$

Further, *Bob* asking to read *file1* can be represented as *Bob* says *read\\_file1*. The reference monitor may authorize *Bob* on this request if and only if

$$(1), (2), \text{Bob says read\_file1} \vdash_{\mathcal{L}} \text{read\_file1}$$

---

<sup>1</sup> In other words, *Admin* has direct permission to read *file1*.

In most access control logics, the above entailment has a proof, so *Bob* will be able to read *file1*. We re-emphasize that the notion of authorization w.r.t. to a submitted request corresponds to the formal notion of *derivability* of the requested access from the available policy.

### 3 Limits of Access Control Logics: Permissions, Control and Information Flow

In this Section we point out three issues that, in our opinion, create a gap between existing work on logic-based approaches to access control as outlined above, and their deployment in practice. We call the first issue the problem of *implicit permissions*: If an action  $\varphi$  is entailed by a policy  $\Gamma$ , then *any* principal is authorized to perform it. The second issue concerns a logical separation of permission to perform an action from the ability to *control* the action, which also includes the permission to delegate the control further. The third issue is concerned with a fine-grained distinction between the *flow of information* (policy statements) from one principal to another, and its *acceptance* by the receiving principal or, in other words, the issue of separating (in the logic) hearsay from trust in the hearsay. We explain these issues one by one, and then present our proposal to address the issues by introducing new modalities into the logic.

#### Issue 1: Implicit permissions

The (standard) definition of permission through entailment presented in Section 2 says that a principal  $A$  can perform action  $\varphi$  if from the prevailing policy  $\Gamma$  and  $A$  says  $\varphi$ ,  $\varphi$  can be established. However, this creates a problem in practice: Once enough credentials exist to authorize an access for some principal, any principal is permitted the same access by the standard definition. For instance, in our earlier example, after *Bob* has created the credential *Bob* says *read\_file1*, any principal  $A$  will be authorized to read *file1*. This is because the existence of a proof of  $\Gamma, \text{Bob says read\_file1} \vdash \text{read\_file1}$  implies, by the law of weakening in the logic, that  $\Gamma, \text{Bob says read\_file1}, A \text{ says read\_file1} \vdash \text{read\_file1}$  is also provable for any principal  $A$ .

The problem here is that the formula asserting the authorization — *read\_file1* — does not include the identity of the principal who is authorized access. We propose to resolve this problem by introducing an explicit, principal-indexed modality for permissions, which we write  $\mathbf{P}_A\varphi$  (Section 4). With this modality, principal  $A$  is authorized to perform action  $\varphi$  iff  $\Gamma \vdash \mathbf{P}_A\varphi$ . By explicitly listing the principal authorized in the conclusion, we eliminate the problem of implicit permissions.

An alternate, related solution, not considered here, but often used in first-order logics for access control, is to treat the permission (e.g., *read\_file1*) as a relation over principals. Instead of writing *read\_file1* we could write *read\_file1(A)* to mean that principal  $A$  is authorized to read *file1*. However, since we are interested in proving decidability for the logic, we avoid first-order logic.

## Issue 2: Control or Delegatable Permissions

Often in access control, it is desirable to give an individual a permission and also the power to further delegate the permission. To this end we propose a new modality  $\mathbf{C}_A\varphi$ , read “ $A$  controls  $\varphi$ ”. The key axioms governing  $\mathbf{C}_A\varphi$  are:

$$\begin{aligned} \vdash \mathbf{C}_A\varphi \rightarrow \mathbf{P}_A\varphi & \quad (C2P) \\ \vdash (\mathbf{C}_A\varphi \wedge (A \text{ says } \mathbf{C}_B\varphi)) \rightarrow \mathbf{C}_B\varphi & \quad (del-C) \end{aligned}$$

The first axiom means that if principal  $A$  controls  $\varphi$ , then it is also permitted  $\varphi$ . This axiom relates control to permission and makes  $\mathbf{C}_A\varphi$  strictly stronger than  $\mathbf{P}_A\varphi$ . The second axiom allows principal  $A$ , who controls  $\varphi$ , to delegate this control to a principal  $B$  simply by asserting this fact. This ability to delegate further distinguishes  $\mathbf{C}_A\varphi$  from  $\mathbf{P}_A\varphi$ .

It is desirable that  $(\mathbf{C}_A\varphi_1 \wedge \mathbf{C}_A\varphi_2) \rightarrow \mathbf{C}_A(\varphi_1 \wedge \varphi_2)$ . For instance, if  $A$  has control over the deletion of files 1 and 2 individually, it should also have control over the deletion of the two files together, thus allowing it to delegate control over deletion of both files at once. A similar property for permissions may be harmful. For instance, if file 2 is the backup of file 1, we may not want to permit their simultaneous deletion ( $\mathbf{P}_A(\varphi_1 \wedge \varphi_2)$ ), even if we allow their deletion individually ( $\mathbf{P}_A\varphi_1 \wedge \mathbf{P}_A\varphi_2$ ). Formally, this difference is manifest in different logical treatments of the two modalities: while  $\mathbf{C}_A$  is a normal *necessitation* modality,  $\mathbf{P}_A$  is a *possibility* modality (see Section 4 for details).

## Issue 3: Information Flow vs Acceptance

Besides the use of the modality  $\mathbf{C}_A$ , authority can also be delegated from one principal to another by nesting the says modality, as in the following statement from Example 1, which delegates the formula *read\_file1* from principal *Admin* to principal *Bob*:

$$2. \text{Admin says } ((\text{Bob says } \text{read\_file1}) \rightarrow \text{read\_file1})$$

Intuitively, we expect (as in Example 1) that this formula together with *Bob says read\_file1* should imply that *Admin says read\_file1*. However, performing this inference requires us to infer from *Bob says read\_file1* that *Admin says Bob says read\_file1*. To allow for this inference, most authorization logics include the following axiom, or a stronger axiom that implies it (this axiom was proposed by Abadi [1]):

$$A \text{ says } \varphi \rightarrow B \text{ says } (A \text{ says } \varphi) \quad (\text{I-SS})$$

However, this axiom also allows *unwanted* statements to flow from one principal to another. Here is an example. Suppose *Admin* delegates to *Bob* the authority to *read\_file1* through statement (2), under the conception that *Bob* will only allow *read\_file1* under reasonable conditions. However, *Bob*, mistakenly or maliciously, adds the following rule:

$$\text{Bob says } (\text{bad\_condition} \rightarrow \text{read\_file1})$$

where *bad\_condition* means that a certain bad condition (for reading *file1*) holds. Now, using the statements above and (I-SS), *Bob says bad\_condition* implies that *Admin says read\_file1*, which is undesirable.

The problem here is that the logic, so far, does not provide a construct to allow *Admin* to represent in statement (2) that it actually *trusts* the assumption (*Bob* says *read\_file1*). We propose to rectify this situation by including the construct *A* ratified  $\varphi$ , which means that *A* says  $\varphi$  and that this statement is trusted by the principal in the enclosing scope. With this construct, *Admin* can revise its statement to say that:

2a. *Admin* says  $((\text{Bob ratified } \text{read\_file1}) \rightarrow \text{read\_file1})$

If *Bob* merely says *read\_file1*, it will imply *Admin* says *Bob* says *read\_file1*, but not *Admin* says *Bob* ratified *read\_file1*, and not allow for the deduction of *Admin* says *read\_file1*. To allow for the latter, *Admin* must make explicit rules to convert *Bob*'s statements to ratified statements, e.g., it may add the following two rules:

3. *Admin* says  $((\text{Bob says } \text{good\_condition}) \rightarrow (\text{Bob ratified } \text{good\_condition}))$
4. *Admin* says  $((\text{Bob says } (\text{good\_condition} \rightarrow \text{read\_file1})) \rightarrow (\text{Bob ratified } (\text{good\_condition} \rightarrow \text{read\_file1})))$

thus allowing deduction of *Admin* says *read\_file1* from the statements *Bob* says  $(\text{good\_condition} \rightarrow \text{read\_file1})$  and *Bob* says *good\_condition*, but not from *Bob* says  $(\text{bad\_condition} \rightarrow \text{read\_file1})$  and *Bob* says *bad\_condition*. The formal rules that allow these deductions and a more detailed example of the use of ratification are presented in Section 4.

## 4 The New Modalities

In this section we present  $\text{ACL}^+$ , an access control logic with the modalities  $\mathbf{P}_A$ ,  $\mathbf{C}_A$  and *A* ratified  $\bullet$ . To summarize,

1. Permission and control can be represented directly in  $\text{ACL}^+$  using the modalities  $\mathbf{P}_A\varphi$  (principal *A* is authorized (permitted)  $\varphi$ ) and  $\mathbf{C}_A\varphi$  (principal *A* controls  $\varphi$ ).
2.  $\text{ACL}^+$  contains the operator *A* ratified  $\varphi$ , which means that principal *A* states  $\varphi$  and this statement has been ratified (or, is trusted) by the principal in whose context the formula is interpreted.

We introduce  $\text{ACL}^+$  piecewise, starting with a simple access control logic containing the modality says defined by the following rules and axioms:

$$\begin{array}{l}
 \text{all axioms of intuitionistic propositional logic} \\
 \frac{\vdash \varphi \quad \vdash \varphi \rightarrow \psi}{\vdash \psi} \quad (\text{MP}) \\
 \frac{\vdash \varphi}{\vdash A \text{ says } \varphi} \quad (\text{nec-S}) \\
 \vdash (A \text{ says } (\varphi \rightarrow \psi)) \rightarrow (A \text{ says } \varphi) \rightarrow (A \text{ says } \psi) \quad (\text{K-S}) \\
 \vdash A \text{ says } \varphi \rightarrow B \text{ says } (A \text{ says } \varphi) \quad (\text{I-SS})
 \end{array}$$

We note that our logic is intuitionistic (constructive). The use of intuitionistic logic for access control has been motivated in prior work [12]; briefly, constructivism disallows proofs by contradiction, thus eliminating authorization if it is merely not denied. Axioms (MP) and (nec-S) express that says is a normal necessitation modality and are standard in access control literature.

## 4.1 Permission and Control

To this basic logic we add the modalities  $\mathbf{P}_A$  and  $\mathbf{C}_A$ , characterized by the following rules and axioms:

**Definition 1 (Axioms and Rules for  $\mathbf{P}_A$  and  $\mathbf{C}_A$ ).**

$$\begin{array}{l}
\frac{\vdash \varphi}{\vdash \mathbf{C}_A \varphi} \quad (\text{nec-C}) \\
\vdash \mathbf{C}_A(\varphi \rightarrow \psi) \rightarrow (\mathbf{C}_A \varphi \rightarrow \mathbf{C}_A \psi) \quad (\text{C-Deduce}) \\
\vdash \mathbf{C}_A \varphi \rightarrow \mathbf{P}_A \varphi \quad (\text{C2P}) \\
\vdash \mathbf{P}_A(\varphi \vee \psi) \rightarrow \mathbf{P}_A \varphi \vee \mathbf{P}_A \psi \quad (\text{or-P}) \\
\vdash (\mathbf{C}_A \varphi \wedge (A \text{ says } \mathbf{C}_B \varphi)) \rightarrow \mathbf{C}_B \varphi \quad (\text{del-C})
\end{array}$$

Axiom (C-Deduce) expresses that control is closed under logical deduction while rule (nec-C) means that all valid formulas of the logic are controlled by every principal  $A$ . Together, (nec-C) and (C-Deduce) make  $\mathbf{C}_A$  a normal necessitation modality (similar to  $\Box$  in standard modal logics). As motivated in Section 3, we model permission with a *possibility* modality, i.e., it is not closed under logical consequence, but we require it to distribute over disjunction (or-P). Axiom (C2P) relates the notion of control with that of permission and reads: “If principal  $A$  controls  $\varphi$ , then it is authorized (permitted) on  $\varphi$ ”. This implies that control of a formula is stronger than permission on the formula. Axiom (del-C) allows a principal  $A$  in control of  $\varphi$  to delegate that control to another principal  $B$  (see Example 2).

**Definition 2 (Authorization).** *Given a policy  $\Gamma$ , we say that  $A$  is authorized on access  $\varphi$  if and only if  $\Gamma \vdash \mathbf{P}_A \varphi$ .*

*Example 2.* The policy of Example 1 can be re-represented with the new modalities as follows

- (1)  $\mathbf{C}_{Admin}(read\_file1)$
- (2)  $Admin \text{ says } (\mathbf{C}_{Bob}(read\_file1))$

From (del-C), (MP) and (C2P) we can prove that  $Bob$  is authorized to read file1, i.e.,  $(1), (2) \vdash \mathbf{P}_{Bob}(read\_file1)$ .

*Example 3.* A principal can selectively delegate privileges it controls to other principals. Consider a policy in which  $A$  controls the deletion of files 1 and 2.  $A$  can delegate to  $B$  only the authority to delete file 1 by asserting that  $B$  controls it. Formally,

$$\mathbf{C}_A(delete\_file1 \wedge delete\_file2), A \text{ says } (\mathbf{C}_B(delete\_file1)) \vdash \mathbf{C}_B(delete\_file1)$$

*Proof.* From the assumption  $\mathbf{C}_A(delete\_file1 \wedge delete\_file2)$  infer using (nec-C) and (C-deduce) that  $\mathbf{C}_A(delete\_file1)$ .  $\mathbf{C}_B(delete\_file1)$  follows using (del-C) and the assumption  $A \text{ says } (\mathbf{C}_B(delete\_file1))$ .

## 4.2 The Modality ( $A$ ratified $\varphi$ )

Next, we add to our logic the modality  $A$  ratified  $\varphi$ , which means not only that  $A$  says  $\varphi$ , but also that the latter has been checked, ratified, or is trusted by the principal in whose scope it occurs (Section 3)<sup>2</sup>. For instance, the formula  $B$  says ( $A$  ratified  $\varphi$ ) means that: “ $A$  says  $\varphi$  and  $B$  ratified (trusts) this statement”. The resulting logic is called  $ACL^+$ .

Like  $C_A$  and  $A$  says  $\bullet$ , we model  $A$  ratified  $\bullet$  as a normal modality:

$$\frac{\vdash \varphi}{\vdash A \text{ ratified } \varphi} \quad (\text{nec-R})$$

$$\vdash (A \text{ ratified } (\varphi \rightarrow \psi)) \rightarrow (A \text{ ratified } \varphi) \rightarrow (A \text{ ratified } \psi) \quad (\text{K-R})$$

Further, the modality  $A$  ratified  $\varphi$  implies  $A$  says  $\varphi$ , but the converse is not true in general:

$$\vdash (A \text{ ratified } \varphi) \rightarrow (A \text{ says } \varphi) \quad (\text{RS})$$

The axiom (RS) makes  $A$  ratified  $\varphi$  stronger than  $A$  says  $\varphi$ . Statement  $\varphi$  directly signed by a principal can be taken as an evidence of  $A$  says  $\varphi$ , not  $A$  ratified  $\varphi$ .

(I-SS) and (RS) together imply that:

$$\vdash (A \text{ ratified } \varphi) \rightarrow B \text{ says } A \text{ says } \varphi$$

but it is not possible to derive in general that

$$(A \text{ says } \varphi) \rightarrow B \text{ says } A \text{ ratified } \varphi$$

which would be unjustified because if  $A$  says  $\varphi$ , then  $B$  has not necessarily ratified it.

*Example 4.* The purpose of introducing ratified is to allow a principal control over what statements and proofs of another principal it will admit as trusted. Assume that a hospital administrator  $PA$  controls access to sensitive patient records. The main policy is that “a doctor has access to all patient records” and the determination of who constitutes a doctor comes from the principal  $HR$ , representing the human resources database. Let  $C_A(\text{access\_records})$  mean that principal  $A$  has control over the access to patient records and  $isDoctor\_A$  mean that  $A$  is a doctor. The main policy can be encoded as the formula<sup>3</sup>:

$$PA \text{ says } \bigwedge_{A \in \mathcal{P}} [(HR \text{ ratified } isDoctor\_A) \rightarrow (C_A(\text{access\_records}))] \quad (\text{P1})$$

Observe that we are using ( $HR$  ratified  $\dots$ ) inside the policy instead of ( $HR$  says  $\dots$ ) to make sure that consequences of the policy depend only on statements of  $HR$  that have been ratified by  $PA$ .

Now,  $PA$  can choose to trust the policies of  $HR$  selectively. For instance, if  $PA$  trusts all deductions of the form  $isDoctor\_A$  that  $HR$  may make, it can have the policy:

<sup>2</sup> The idea of interpreting formulas in the context of principals goes back to the logics DTL and BL [10].

<sup>3</sup> Because we are using a propositional language, we assume principals to range over a *finite* set  $\mathcal{P}$ . Accordingly,  $\bigwedge_{A \in \mathcal{P}} \varphi$  reads “For all principals  $A$  in  $\mathcal{P}$ ,  $\varphi$  holds”.

$$PA \text{ says } \bigwedge_{A \in \mathcal{P}} [(HR \text{ says } isDoctor\_A) \rightarrow (HR \text{ ratified } isDoctor\_A)] \quad (P2)$$

Then, for any principal  $A$ , we have that

$$(P1), (P2), HR \text{ says } (isDoctor\_A) \vdash PA \text{ says } C_A(access\_records)$$

If, on the other hand,  $PA$  only trusts  $HR$ 's statements about two principals  $Alice$  and  $Bob$ , it can selectively assert (in place of (P2)) that:

$$\begin{aligned} PA \text{ says } ((HR \text{ says } isDoctor\_Alice) \rightarrow (HR \text{ ratified } isDoctor\_Alice)) \\ PA \text{ says } ((HR \text{ says } isDoctor\_Bob) \rightarrow (HR \text{ ratified } isDoctor\_Bob)) \end{aligned}$$

As a last illustration, suppose that the  $HR$  has two policies, one of which states that every administrator is a doctor and the other of which (mistakenly) states that every hospital employee is a doctor:

$$HR \text{ says } \bigwedge_{A \in \mathcal{P}} (isAdmin\_A \rightarrow isDoctor\_A) \quad (P3)$$

$$HR \text{ says } \bigwedge_{A \in \mathcal{P}} (isEmployee\_A \rightarrow isDoctor\_A) \quad (P4)$$

$PA$  can choose to ratify the first of these, but not the second, by asserting in place of (P2) that:

$$PA \text{ says } ((HR \text{ says } \bigwedge_{A \in \mathcal{P}} (isAdmin\_A \rightarrow isDoctor\_A)) \rightarrow (HR \text{ ratified } \bigwedge_{A \in \mathcal{P}} (isAdmin\_A \rightarrow isDoctor\_A))) \quad (P5)$$

$$PA \text{ says } \bigwedge_{A \in \mathcal{P}} ((HR \text{ says } isAdmin\_A) \rightarrow (HR \text{ ratified } isAdmin\_A)) \quad (P6)$$

Suppose that  $HR$  says  $isAdmin\_Alice$ . Then, we can deduce  $PA$  says  $C_{Alice}(access\_records)$  from (P1), (P3), (P5) and (P6) as follows:

1. From (P3) and (I-SS), deduce that

$$PA \text{ says } (HR \text{ says } (\bigwedge_{A \in \mathcal{P}} (isAdmin\_A \rightarrow isDoctor\_A)))$$

2. From (1), (K-S) and (P5) deduce that

$$PA \text{ says } (HR \text{ ratified } (\bigwedge_{A \in \mathcal{P}} (isAdmin\_A \rightarrow isDoctor\_A)))$$

3. From ( $HR$  says  $isAdmin\_Alice$ ) and (I-SS) deduce that ( $PA$  says  $HR$  says  $isAdmin\_Alice$ )
4. From (3), (K-S) and (P6) deduce that ( $PA$  says  $HR$  ratified  $isAdmin\_Alice$ )
5. From (2), (4), (K-S), and (K-R) deduce that ( $PA$  says  $HR$  ratified  $isDoctor\_Alice$ )
6. From (5), (P1), and (K-S) deduce that ( $PA$  says  $C_{Alice}(access\_records)$ )

If we replace the assumption ( $HR$  says  $isAdmin\_Alice$ ) with the assumption ( $HR$  says  $isEmployee\_Alice$ ), then we cannot deduce ( $PA$  says ( $C_{Alice}(access\_records)$ )) because we cannot deduce (5) above. In place of (5), we can deduce only the weaker statement ( $PA$  says ( $HR$  says  $isDoctor\_Alice$ )), which does not imply ( $PA$  says  $C_{Alice}(access\_records)$ ) in our theory.

## 5 Semantics

In this section, we define sound and complete semantics for  $ACL^+$ . Our semantics uses graph-based structures called Kripke models, that are standard in modal logic. Although Kripke semantics are not necessarily intuitive, they lead directly to a proof theory for the logic, a decidability result for it, and an implementation of its decision procedure (Section 6).

**Definition 3.** *An intuitionistic model,  $\mathcal{M}$ , of  $ACL^+$  is a tuple*

$$(W, \leq, \{S_A\}_{A \in \mathcal{P}}, \{C_A\}_{A \in \mathcal{P}}, \{R_A\}_{A \in \mathcal{P}}, \{P_A\}_{A \in \mathcal{P}}, h)$$

where

- $\mathcal{P}$  is a set of principals.
- $(W, \leq)$  is a preorder, where elements of  $W$  are called states or worlds, and  $\leq$  is a binary relation over  $W$  which satisfies the following conditions
  - $\forall x. (x \leq x)$  (refl)
  - $\forall x, y, z. ((x \leq y) \wedge (y \leq z) \rightarrow (x \leq z))$  (trans)
- $S_A, C_A, R_A$  and  $P_A$  are binary relations on  $W$  that satisfy the following conditions:
  - $\forall x, y, z, w. ((x \leq y) \wedge (yS_A z) \wedge (z \leq w)) \rightarrow (xS_A w)$  (mon-S)
  - $\forall x, y, z, w. ((x \leq y) \wedge (yC_A z) \wedge (z \leq w)) \rightarrow (xC_A w)$  (mon-C)
  - $\forall x, y, z, w. ((x \leq y) \wedge (yR_A z) \wedge (z \leq w)) \rightarrow (xR_A w)$  (mon-R)
  - $\forall x, y, z, w. ((x \leq y) \wedge (zP_A y) \wedge (z \leq w)) \rightarrow (wP_A x)$  (mon-P)
- $h$  is an assignment which, for each atom  $q$ , assigns the subset of worlds  $h(q) \subseteq W$  where  $q$  holds. Moreover, we require  $h$  to be monotone w.r.t.  $\leq$ , i.e., if  $x \in h(q)$  and  $x \leq y$  then  $y \in h(q)$ .

Conditions above ensure monotonicity of the logic (Lemma 1), which is a standard property of Kripke semantics for constructive logics. Moreover, to force  $ACL^+$  models to admit the axioms (I-SS), (C2P), (del-C) and (RS) we require the following to hold for any two principals  $A$  and  $B$ .

$$\begin{aligned} \forall x, y, z. ((xS_B y) \wedge (yS_A z)) &\rightarrow (xS_A z) && \text{(s-I-SS)} \\ \forall x \exists y. (xC_A y \wedge xP_A y) &&& \text{(s-C2P)} \\ \forall x, y. ((xC_B y) \rightarrow ((xC_A y) \vee \exists z((xS_A z) \wedge (zC_B y)))) &&& \text{(s-del-C)} \\ \forall x, y. ((xS_A y) \rightarrow (xR_A y)) &&& \text{(s-RS)} \end{aligned}$$

An interpretation for the logic is a pair  $\mathcal{M}, t$  where  $\mathcal{M}$  is a model and  $t$  is a world in  $\mathcal{M}$ .

**Definition 4 (Satisfaction Relation).** *The satisfaction relation “ $\models$ ” between interpretations and formulae of the logic is defined as follows.*

- $\mathcal{M}, t \models q$  iff  $t \in h(q)$
- $\mathcal{M}, t \not\models \perp$
- $\mathcal{M}, t \models \varphi \vee \psi$  iff  $\mathcal{M}, t \models \varphi$  or  $\mathcal{M}, t \models \psi$
- $\mathcal{M}, t \models \varphi \wedge \psi$  iff  $\mathcal{M}, t \models \varphi$  and  $\mathcal{M}, t \models \psi$

- $\mathcal{M}, t \models \varphi \rightarrow \psi$  iff for all  $s, t \leq s$  and  $\mathcal{M}, s \models \varphi$  implies  $\mathcal{M}, s \models \psi$
- $\mathcal{M}, t \models \neg\varphi$  iff for all  $s, t \leq s$  implies  $\mathcal{M}, t \not\models \varphi$
- $\mathcal{M}, t \models A \text{ says } \varphi$  iff for all  $s$  such that  $tS_A s$  we have  $\mathcal{M}, s \models \varphi$
- $\mathcal{M}, t \models \mathbf{C}_A \varphi$  iff for all  $s$  such that  $tC_A s$  we have  $\mathcal{M}, s \models \varphi$
- $\mathcal{M}, t \models A \text{ ratified } \varphi$  iff for all  $s$  such that  $tR_A s$  we have  $\mathcal{M}, s \models \varphi$
- $\mathcal{M}, t \models \mathbf{P}_A \varphi$  iff there exists an  $s, tP_A s$  such that  $\mathcal{M}, s \models \varphi$

**Lemma 1 (Monotonicity).** *For any formula  $\varphi$  and any interpretation  $\mathcal{M}, t$ , if  $\mathcal{M}, t \models \varphi$  and  $t \leq s$  then  $\mathcal{M}, s \models \varphi$ .*

We say that  $\mathcal{M} \models \varphi$  if for all  $t \in \mathcal{M}$ , it is the case that  $\mathcal{M}, t \models \varphi$ . Further,  $\Gamma \models \varphi$  if for every  $\mathcal{M}$  satisfying the above conditions,  $\mathcal{M} \models \Gamma$  implies  $\mathcal{M} \models \varphi$ .

**Theorem 1 (Soundness).** *If  $\Gamma \vdash \varphi$  then  $\Gamma \models \varphi$*

**Theorem 2 (Completeness).** *If  $\Gamma \models \varphi$  then  $\Gamma \vdash \varphi$*

We note that the conditions (s-I-SS), (s-C2P), (s-del-C) and (s-RS) are *canonical* for the axioms (I-SS), (C2P), (del-C) and (RS), respectively, i.e., a logic with any subset of these axioms is sound and complete with respect to models that satisfy the conditions corresponding to the chosen axioms.

## 6 A Semantic-Based Calculus for ACL<sup>+</sup>

In this section we briefly present Seq-ACL<sup>+</sup>, a sound, complete and cut-free sequent calculus for ACL<sup>+</sup>. The calculus is inspired by the work of Negri [19]<sup>4</sup> and follows the so-called labeled approach [4,20], which directly uses the Kripke semantics. The use of labeled sequent calculi for access control is relatively new and has been introduced in [15,16] to define proof theory of a specific says-based access control logic. The sequent calculus directly leads to a decision procedure for the logic ACL<sup>+</sup>.

Seq-ACL<sup>+</sup> manipulates two types of labeled formulas:

1. *World formulas*, denoted by  $x : \varphi$ , where  $x$  is a world and  $\varphi$  is a well formed formula of ACL<sup>+</sup>, intuitively meaning that  $\varphi$  holds in world  $x$ .
2. *Transition formulas* representing semantic accessibility relationships. These formulas have one of the forms  $xS_A y, xC_A y, xR_A y, xP_A y$  and  $x \leq y$ .

A sequent is a tuple  $\langle \Sigma, \mathbb{M}, \Gamma, \Delta \rangle$ , usually written  $\Sigma; \mathbb{M}; \Gamma \Rightarrow \Delta$  where  $\mathbb{M}, \Gamma$  and  $\Delta$  are multisets of labeled formulas and  $\Sigma$  is the set of labels (worlds) appearing in the rest of the sequent. Intuitively, the sequent  $\Sigma; \mathbb{M}; \Gamma \Rightarrow \Delta$  means that “every model which satisfies all labeled formulas of  $\Gamma \cup \mathbb{M}$  satisfies at least one labeled formula in  $\Delta$ ”. This is made precise by the notion of *validity* in the following definition.

**Definition 5 (Sequent validity).** *Given a model*

$$\mathcal{M} = (W, \leq, \{S_A\}_{A \in \mathcal{P}}, \{C_A\}_{A \in \mathcal{P}}, \{R_A\}_{A \in \mathcal{P}}, \{P_A\}_{A \in \mathcal{P}}, h)$$

*and a label alphabet  $\mathcal{A}$ , consider a mapping  $I : \mathcal{A} \rightarrow W$ . Let  $F$  denote a labeled formula. Define  $\mathcal{M} \models_I F$  as follows:*

<sup>4</sup> In particular, proofs of metatheorems about Seq-ACL<sup>+</sup> use methods developed in [19].

- $\mathcal{M} \models_I x : \alpha$  iff  $\mathcal{M}, I(x) \models \alpha$
- $\mathcal{M} \models_I x C_A y$  iff  $I(x) C_A I(y)$  (Similarly for  $S_A, R_A, P_A$  and  $\leq$ ).

We say that  $\Sigma; \mathbb{M}; \Gamma \Rightarrow \Delta$  is valid in  $\mathcal{M}$  if, for every mapping  $I : \mathcal{A} \rightarrow W$ , if  $\mathcal{M} \models_I F$  for every  $F \in \mathbb{M} \cup \Gamma$ , then  $\mathcal{M} \models_I G$  for some  $G \in \Delta$ . We say that  $\Sigma; \mathbb{M}; \Gamma \Rightarrow \Delta$  is valid in  $\text{Seq-ACL}^+$  if it is valid in every  $\mathcal{M}$ .

Figure 1 lists the rules of the calculus  $\text{Seq-ACL}^+$ , divided into four groups.

- *Axiom rules* do not have premises and describe valid sequents.
- *Logical rules* operate on connectives of the logic. For reasons of space, we omit some rules:  $\wedge L, \wedge R, \vee L$  and  $\vee R$ <sup>5</sup> are standard (see, for instance, [19]) while rules for says and ratified have the same structure as those for **C**.
- *Semantic rules* define the properties that hold for relationships  $\leq, S_A, R_A, C_A$  and  $P_A$  in all  $\text{ACL}^+$  models.
- *Access control rules* codify axioms that differentiate  $\text{ACL}^+$  from other constructive normal modal logics, i.e., (I-SS), (C2P), (del-C) and (RS).

Note that semantic and access control rules are in one-to-one correspondence with semantic conditions of Definition 3.

We say that a sequent  $\Sigma; \mathbb{M}; \Gamma \Rightarrow \Delta$  is *derivable* in  $\text{Seq-ACL}^+$  if it admits a *derivation*. A derivation is a tree whose nodes are sequents. A branch is a sequence of nodes  $\Sigma_1; \mathbb{M}_1; \Gamma_1 \Rightarrow \Delta_1, \Sigma_2; \mathbb{M}_2; \Gamma_2 \Rightarrow \Delta_2, \dots, \Sigma_n; \mathbb{M}_n; \Gamma_n \Rightarrow \Delta_n, \dots$ . Each node  $\Sigma_i; \mathbb{M}_i; \Gamma_i \Rightarrow \Delta_i$  is obtained from its immediate successor  $\Sigma_{i-1}; \mathbb{M}_{i-1}; \Gamma_{i-1} \Rightarrow \Delta_{i-1}$  by applying *backward* a rule of  $\text{Seq-ACL}^+$ , having  $\Sigma_{i-1}; \mathbb{M}_{i-1}; \Gamma_{i-1} \Rightarrow \Delta_{i-1}$  as the conclusion and  $\Sigma_i; \mathbb{M}_i; \Gamma_i \Rightarrow \Delta_i$  as one of its premises. A branch is closed if one of its nodes is an instance of axiom rules, otherwise it is open. We say that a tree is closed if all of its branches are closed. A sequent  $\Sigma; \mathbb{M}; \Gamma \Rightarrow \Delta$  has a derivation in  $\text{Seq-ACL}^+$  if there is a closed tree having  $\Sigma; \mathbb{M}; \Gamma \Rightarrow \Delta$  as the root. As an example we show a derivation of the axiom (C2P)

$$\begin{array}{c}
\frac{}{x, y, z; x \leq y, z \leq z, y C_A z, y P_A z; y : \mathbf{C}_{AP}, z : p \Rightarrow y : \mathbf{P}_{AP}, z : p} \text{init} \\
\frac{}{x, y, z; x \leq y, y C_A z, y P_A z; y : \mathbf{C}_{AP}, z : p \Rightarrow y : \mathbf{P}_{AP}, z : p} \text{refl} \\
\frac{}{x, y, z; x \leq y, y C_A z, y P_A z; y : \mathbf{C}_{AP}, z : p \Rightarrow y : \mathbf{P}_{AP}} \text{PR} \\
\frac{}{x, y, z; x \leq y, y C_A z, y P_A z; y : \mathbf{C}_{AP} \Rightarrow y : \mathbf{P}_{AP}} \text{CL} \\
\frac{}{x, y, z; x \leq y, y C_A z, y P_A z; y : \mathbf{C}_{AP} \Rightarrow y : \mathbf{P}_{AP}} \text{s-C2P} \\
\frac{x, y; x \leq y; y : \mathbf{C}_{AP} \Rightarrow y : \mathbf{P}_{AP}}{x; ; \Rightarrow x : \mathbf{C}_{AP} \rightarrow \mathbf{P}_{AP}} \rightarrow \text{R}
\end{array}$$

**Theorem 3 (Admissibility of cut).**  $\Sigma; \mathbb{M}; \Gamma \Rightarrow x : \alpha, \Delta$  and  $\Sigma; \mathbb{M}; \Gamma, x : \alpha \Rightarrow \Delta$  imply  $\Sigma; \mathbb{M}; \Gamma \Rightarrow \Delta$ .

**Theorem 4 (Soundness of  $\text{Seq-ACL}^+$ ).** If a sequent  $\Sigma; \mathbb{M}; \Gamma \Rightarrow \Delta$  is derivable then it is valid in the sense of Definition 5.

**Theorem 5 (Completeness of  $\text{Seq-ACL}^+$ ).** If a formula  $\alpha$  is valid in  $\text{ACL}^+$  (i.e.,  $\models \alpha$ ), then  $x; ; \Rightarrow x : \alpha$  is derivable in  $\text{Seq-ACL}^+$ .

<sup>5</sup> We do not have specific rules for negation because, in constructive logics,  $\neg\varphi$  is equivalent to  $\varphi \rightarrow \perp$ .

### Axiom Rules

$$\frac{}{\Sigma; \mathbb{M}, x \leq y; \Gamma, x : p \Rightarrow y : p, \Delta} \text{init} \quad \frac{}{\Sigma; \mathbb{M}; \Gamma, x : \perp \Rightarrow \Delta} \perp\text{L} \quad \frac{}{\Sigma; \mathbb{M}; \Gamma \Rightarrow x : \top, \Delta} \top\text{R}$$

### Logical Rules

$$\frac{\Sigma; \mathbb{M}, x \leq y; \Gamma, x : \alpha \rightarrow \beta \Rightarrow_{\mathcal{T}} y : \alpha, \Delta \quad \Sigma; \mathbb{M}, x \leq y; \Gamma, x : \alpha \rightarrow \beta, y : \beta \Rightarrow_{\mathcal{T}} \Delta}{\Sigma; \mathbb{M}, x \leq y; \Gamma, x : \alpha \rightarrow \beta \Rightarrow \Delta} \rightarrow\text{L}$$

$$\frac{\Sigma, y; \mathbb{M}, x \leq y; \Gamma, y : \alpha \Rightarrow y : \beta, \Delta}{\Sigma; \mathbb{M}; \Gamma \Rightarrow x : \alpha \rightarrow \beta, \Delta} \rightarrow\text{R}_{y \text{ new}}$$

$$\frac{\Sigma; \mathbb{M}, x C_{Ay}; \Gamma, x : C_A \alpha, y : \alpha \Rightarrow \Delta}{\Sigma; \mathbb{M}, x C_{Ay}; \Gamma, x : C_A \alpha \Rightarrow \Delta} \text{CL}$$

$$\frac{\Sigma, y; \mathbb{M}, x C_{Ay}; \Gamma \Rightarrow y : \alpha, \Delta}{\Sigma; \mathbb{M}; \Gamma \Rightarrow x : C_A \alpha, \Delta} \text{CR}_{y \text{ new}}$$

$$\frac{\Sigma; \mathbb{M}, x P_{Ay}; \Gamma \Rightarrow x : P_A \alpha, y : \alpha, \Delta}{\Sigma; \mathbb{M}, x P_{Ay}; \Gamma \Rightarrow x : P_A \alpha, \Delta} \text{PR}$$

$$\frac{\Sigma, y; \mathbb{M}, x P_{Ay}; \Gamma, y : \alpha \Rightarrow \Delta}{\Sigma; \mathbb{M}; \Gamma, x : P_A \alpha \Rightarrow \Delta} \text{PL}_{y \text{ new}}$$

### Semantical Rules

$$\frac{\Sigma; \mathbb{M}, x \leq y, y S_{Az}, z \leq w, x S_{Aw}; \Gamma \Rightarrow \Delta}{\Sigma; \mathbb{M}, x \leq y, y S_{Az}, z \leq w; \Gamma \Rightarrow \Delta} \text{mon-S} \quad \frac{\Sigma; \mathbb{M}, x \leq y, y C_{Az}, z \leq w, x C_{Aw}; \Gamma \Rightarrow \Delta}{\Sigma; \mathbb{M}, x \leq y, y C_{Az}, z \leq w; \Gamma \Rightarrow \Delta} \text{mon-C}$$

$$\frac{\Sigma; \mathbb{M}, x \leq y, y R_{Az}, z \leq w, x R_{Aw}; \Gamma \Rightarrow \Delta}{\Sigma; \mathbb{M}, x \leq y, y R_{Az}, z \leq w; \Gamma \Rightarrow \Delta} \text{mon-R} \quad \frac{\Sigma; \mathbb{M}, x \leq y, z P_{Ay}, z \leq w, w P_{Ax}; \Gamma \Rightarrow \Delta}{\Sigma; \mathbb{M}, x \leq y, z P_{Ay}, z \leq w; \Gamma \Rightarrow \Delta} \text{mon-P}$$

$$\frac{\Sigma; \mathbb{M}, x \leq x; \Gamma \Rightarrow \Delta}{\Sigma; \mathbb{M}; \Gamma \Rightarrow \Delta} \text{refl}_{x \in \Sigma}$$

$$\frac{\Sigma; \mathbb{M}, x \leq y, y \leq z, x \leq z; \Gamma \Rightarrow \Delta}{\Sigma; \mathbb{M}, x \leq y, y \leq z; \Gamma \Rightarrow \Delta} \text{trans}$$

### Access Control Rules

$$\frac{\Sigma; \mathbb{M}, x S_{By}, y S_{Az}, x S_{Az}; \Gamma \Rightarrow \Delta}{\Sigma; \mathbb{M}, x S_{By}, y S_{Az}; \Gamma \Rightarrow \Delta} \text{s-I-SS}$$

$$\frac{\Sigma, y; \mathbb{M}, x C_{Ay}, x P_{Ay}; \Gamma \Rightarrow \Delta}{\Sigma; \mathbb{M}; \Gamma \Rightarrow \Delta} \text{s-C2P}_{y \text{ new}}$$

$$\frac{\Sigma; \mathbb{M}, x C_{By}, x C_{Ay}; \Gamma \Rightarrow \Delta \quad \Sigma, z; \mathbb{M}, x C_{By}, x S_{Az}, z C_{By}; \Gamma \Rightarrow \Delta}{\Sigma; \mathbb{M}, x C_{By}; \Gamma \Rightarrow \Delta} \text{s-del-C}_{z \text{ new}}$$

$$\frac{\Sigma; \mathbb{M}, x S_{Ay}, x R_{Ay}; \Gamma \Rightarrow \Delta}{\Sigma; \mathbb{M}, x S_{Ay}; \Gamma \Rightarrow \Delta} \text{s-RS}$$

**Fig. 1.** Seq-ACL<sup>+</sup> Rules

## 6.1 Termination

Next, we use the sequent calculus Seq-ACL<sup>+</sup> to prove that the logic ACL<sup>+</sup> is decidable. Note that admissibility of cut (Theorem 3) alone does not ensure the termination of backward proof search in the sequent calculus because access control rules and the rules saysL, ratifiedL, CL, and PR may increase the complexity of sequents in a backward proof search. Accordingly, we prove that these “critical” rules can be applied in a controlled way. For instance, the following Lemma states the use of CL, PR, and access control rules can be limited. (Without loss of generality we assume that the root of each proof has the form  $x; ; \Rightarrow x : \varphi$ ).

**Lemma 2 (Controlled use of rules).** *In each branch of a backward proof search, it is useless to: (1) apply CL on the same transition relation  $x C_A y \in \mathbb{M}$  more than once, (2) apply PR on the same transition relation  $x P_A y \in \mathbb{M}$  more than once, (3) apply rule  $\chi$  for  $\chi \in \{\text{mon-S, mon-R, mon-C, mon-P, sym, trans, s-I-SS, s-del-C, s-C2P, s-RS}\}$  on the same transition formula (or label as in s-RS) more than once.*

However, even the above Lemma is not sufficient to ensure termination of backward proof search. In particular, there are two issues:

1. Interaction of the rule (trans) with  $\rightarrow L$  adds new accessible worlds, and we can build chains of accessible worlds on which  $\rightarrow L$  can be applied *ad infinitum*.
2. Application of rules (s-del-C) and (s-C2P) generates transition relations with new labels that can be used for repeated application of the same rules.

We bound the number of such interactions using a counting argument. Let  $\text{depth}(F)$  be the height of the parse tree of formula  $F$ .

**Definition 6 (Label distance).** *Given a sequent  $\Sigma, \mathbb{M}, \Gamma \Rightarrow \Delta$  and two labels  $x$  and  $y$  such that  $x \leq y \in \mathbb{M}$ , we define the distance  $d(x, y)$  between two labels as 0 when  $x = y$  and  $n$  when  $x \neq y$ , where  $n$  is the length of the longest sequence of transitions in  $\mathbb{M}$  “connecting” the two labels, i.e.,  $x \overset{\sim}{\circ} x_1, x_1 \overset{\sim}{\circ} x_2, \dots, x_{n-1} \overset{\sim}{\circ} y$  where  $\overset{\sim}{\circ} \in \{S_A, C_A, R_A, P_A, \leq\}$  (for any principal  $A$ ). As an example if  $\{x \leq y, y C_A z, z P_A k, x S_A k\} \in \mathbb{M}$  we have  $d(x, k) = 3$ .*

**Lemma 3 (Bounded application of rules).** *Let  $x, x_1$  be labels and  $F$  a formula such that  $d(x, x_1) > \text{depth}(F)$ . Then, in each branch of a backwards proof search starting with  $x; ; \Rightarrow x : F$ , it is useless to: (1) apply  $\rightarrow L$  on a transition formula  $x_1 \leq x_2$ , (2) apply s-C2P on a label  $x_1$ , (3) apply s-del-C on a transition formula  $x_1 C_B x_2$ .*

Using this lemma, we obtain decidability for ACL<sup>+</sup>.

**Theorem 6 (Decidability).** *The logic ACL<sup>+</sup> is decidable.*

Our proof of decidability directly leads to a decision procedure for ACL<sup>+</sup>. A Prolog implementation of the procedure is available from the authors’ webpages.

$$\begin{array}{c}
\frac{\Sigma; \mathbb{M}, xS_{Ay}, xS_{By}; \Gamma \Rightarrow \Delta}{\Sigma; \mathbb{M}, xS_{By}; \Gamma \Rightarrow \Delta} \text{s-sub-S}_B^A \\
\frac{\Sigma; \mathbb{M}, xP_{Ay}, xP_{By}; \Gamma \Rightarrow \Delta}{\Sigma; \mathbb{M}, xP_{Ay}; \Gamma \Rightarrow \Delta} \text{s-sub-P}_B^A \\
\frac{\Sigma; \mathbb{M}, xR_{Ay}, xR_{By}; \Gamma \Rightarrow \Delta}{\Sigma; \mathbb{M}, xR_{By}; \Gamma \Rightarrow \Delta} \text{s-sub-R}_B^A \\
\frac{\Sigma; \mathbb{M}, xC_{By}, xC_{Ay}; \Gamma \Rightarrow \Delta}{\Sigma; \mathbb{M}, xC_{By}; \Gamma \Rightarrow \Delta} \text{s-sub-C}_B^A
\end{array}$$

**Fig. 2.** Access Control Rules for Subordination

## 7 Extending Seq-ACL<sup>+</sup> with Constructs for Subordination

The correspondence between semantic conditions and axioms allows us to modularly extend ACL<sup>+</sup> with new axioms, and new (corresponding) sequent calculus rules. The difficult aspect in any such extension is to prove decidability. As a specific case, we show here how we may extend the logic with new *subordination axioms* of any of the following forms, and obtain decidability again. (In these axioms  $A$  and  $B$  are specific principals, not metavariables, but  $\varphi$  is a metavariable standing for all formulas.)

$$\begin{array}{ll}
\vdash A \text{ says } \varphi \rightarrow B \text{ says } \varphi & (\text{sub-S})_B^A \\
\vdash A \text{ ratified } \varphi \rightarrow B \text{ ratified } \varphi & (\text{sub-R})_B^A \\
\vdash \mathbf{P}_A \varphi \rightarrow \mathbf{P}_B \varphi & (\text{sub-P})_B^A \\
\vdash \mathbf{C}_A \varphi \rightarrow \mathbf{C}_B \varphi & (\text{sub-C})_B^A
\end{array}$$

We call these axioms subordination axioms because each axiom suggests that one of the two principals  $A$  and  $B$  is subordinate to the other. The first (second) axiom means that statements (ratifications) of  $A$  are echoed by  $B$ , so  $B$  is, in a sense, subordinate to  $A$ . The third (fourth) axiom means that if  $A$  has a permission (ability to control), then so does  $B$ , so  $B$  is more powerful than  $A$ .

**Definition 7.** *The semantic conditions on models corresponding to the axioms above are, respectively:*

$$\begin{array}{ll}
\forall x, y. (xS_{By} \rightarrow xS_{Ay}) & (s\text{-sub-S})_B^A \\
\forall x, y. (xR_{By} \rightarrow xR_{Ay}) & (s\text{-sub-R})_B^A \\
\forall x, y. (xP_{Ay} \rightarrow xP_{By}) & (s\text{-sub-P})_B^A \\
\forall x, y. (xC_{By} \rightarrow xC_{Ay}) & (s\text{-sub-C})_B^A
\end{array}$$

Corresponding access control rules for the sequent calculus are shown in Figure 2.

**Lemma 4.** *The extension of Seq-ACL<sup>+</sup> with any subset of the rules in Figure 2 is sound and complete w.r.t. models that satisfy corresponding conditions from Definition 7. Further, the extended calculus admits cut and is decidable.*

## 8 Related Work

The study of formal properties of says and other constructs in modal logic is a relatively new research trend. Prior work by the second author [10] adopts a modified version of constructive modal logic S4 called DTL<sub>0</sub> and shows how existing access control logics can be embedded (via translation) into DTL<sub>0</sub>. Other work [11] translates 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  $\varphi$ . The first author has developed conditional logics as a general framework for modular sequent calculi for standard access control logics with the says connective [15,16]. Dinesh et al. [9] present an access control logic based on says and extended with obligation and permissions, but their treatment of permissions is different from ours and is closely tied to says. The use of canonical properties for access control axioms was first considered in [8] where standard access control axioms (e.g. (unit) and (hand-off)) are characterized in terms of first-order conditions on Kripke models.

## 9 Conclusion

We have presented  $\text{ACL}^+$ , a constructive multi-modal logic for access control that introduces three new modalities  $\mathbf{P}_A$  (permission),  $\mathbf{C}_A$  (control), and ratified (trusted statement) to fix some practical problems in reasoning with policies. The connectives of the logic are defined by a sound and complete Kripke semantics for  $\text{ACL}^+$  together with a correspondence between conditions on models and the logic’s axioms. The semantics lead to  $\text{Seq-ACL}^+$ , a sound, complete, cut-free and terminating calculus for  $\text{ACL}^+$ . Finally,  $\text{ACL}^+$  can be extended with new axioms, as illustrated by examples of axioms for specific kinds of subordination among principals.

*Acknowledgments* Valerio Genovese was supported by the National Research Fund, Luxembourg. Deepak Garg was supported by the U.S. Army Research Office contract “Perpetually Available and Secure Information Systems” (DAAD19-02-1-0389) to Carnegie Mellon CyLab and the AFOSR MURI “Collaborative Policies and Assured Information Sharing”.

## References

1. Abadi, M.: Logic in access control. In: Proceedings of the 18th Annual IEEE Symposium on Logic in Computer Science (LICS). pp. 228–233 (2003)
2. Abadi, M.: Variations in access control logic. In: Proceedings of the 9th International Conference on Deontic Logic in Computer Science (DEON). pp. 96–109 (2008)
3. Abadi, M.: Logic in access control (tutorial notes). In: Proceedings of the 9th International School on Foundations of Security Analysis and Design (FOSAD). pp. 145–165 (2009)
4. Basin, D., D’Agostino, M., Gabbay, D.M., Matthews, S., Viganó, L.: Labelled Deduction. Springer (2000)
5. Bauer, L.: Access Control for the Web via Proof-Carrying Authorization. Ph.D. thesis, Princeton University (2003)
6. Bauer, L., Garriss, S., McCune, J.M., Reiter, M.K., Rouse, J., Rutenbar, P.: Device-enabled authorization in the Grey system. In: Proceedings of the 8th International Conference on Information Security (ISC). pp. 431–445 (2005)
7. Becker, M.Y., Fournet, C., Gordon, A.D.: SecPAL: Design and semantics of a decentralized authorization language. Journal of Computer Security 18(4), 619–665 (2010)
8. Boella, G., Gabbay, D.M., Genovese, V., van der Torre, L.: Fibred security language. Studia Logica 92(3), 395–436 (2009)

9. Dinesh, N., Joshi, A.K., Lee, I., Sokolsky, O.: Permission to speak: A logic for access control and conformance. *Journal of Logic and Algebraic Programming* 80(1), 50–74 (2011)
10. Garg, D.: Principal centric reasoning in constructive authorization logic. In: *Informal Proceedings of Intuitionistic Modal Logic and Application (IMLA)* (2008), Full version available as Carnegie Mellon Technical Report CMU-CS-09-120
11. Garg, D., Abadi, M.: A modal deconstruction of access control logics. In: *Proceedings of the 11th International Conference on Foundations of Software Science and Computational Structures (FoSSaCS)*. pp. 216–230 (2008)
12. Garg, D., Pfenning, F.: Non-interference in constructive authorization logic. In: *Proceedings of the 19th IEEE Computer Security Foundations Workshop (CSFW)*. pp. 283–293 (2006)
13. Garg, D., Pfenning, F.: A proof-carrying file system. In: *Proceedings of the 31st IEEE Symposium on Security and Privacy (Oakland)*. pp. 349–364 (2010)
14. Genovese, V., Giordano, L., Gliozzi, V., Pozzato, G.L.: A constructive conditional logic for access control: a preliminary report. In: *Proceedings of the 19th European Conference on Artificial Intelligence (ECAI)*. pp. 1073–1074 (2010)
15. Genovese, V., Giordano, L., Gliozzi, V., Pozzato, G.L.: Logics for access control: A conditional approach. In: *Informal Proceedings of the 1st Workshop on Logic in Security (LIS)*. pp. 78–92 (2010)
16. Genovese, V., Giordano, L., Gliozzi, V., Pozzato, G.L.: A conditional constructive logic for access control and its sequent calculus. In: *Proceedings of the 20th International Conference on Automated Reasoning with Analytic Tableaux and Related Methods (TABLEAUX)* (2011), to appear
17. Gurevich, Y., Neeman, I.: Logic of infons: The propositional case. *ACM Transactions on Computational Logic* 12(2) (2011)
18. Lampson, B.W., Abadi, M., Burrows, M., Wobber, E.: Authentication in distributed systems: Theory and practice. *ACM Transactions on Computer Systems* 10(4), 265–310 (1992)
19. Negri, S.: Proof analysis in modal logic. *Journal of Philosophical Logic* 34, 507–544 (2005)
20. Negri, S., von Plato, J.: *Proof Analysis*. Cambridge University Press (2011)
21. Schneider, F.B., Walsh, K., Sireer, E.G.: Nexus Authorization Logic (NAL): Design rationale and applications. Tech. rep., Cornell University (2009), online at <http://ecommons.library.cornell.edu/handle/1813/13679>
22. Wobber, E., Abadi, M., Burrows, M.: Authentication in the taos operating system. *ACM Transactions on Computer Systems* 12(1), 3–32 (1994)

## 10 Appendix A: ACL<sup>+</sup> Soundness and Completeness Proof

To prove completeness, we construct a canonical model. We use  $\Gamma$  to denote a finite or infinite set of formulas. Such a set is also called a *theory*.

**Definition 8 (Maximal theory).** A theory  $\Gamma$  is called maximal if:

- (Closure)  $\Gamma \vdash \varphi$  implies  $\varphi \in \Gamma$
- (Primality1)  $\varphi \vee \psi \in \Gamma$  implies  $\varphi \in \Gamma$  or  $\psi \in \Gamma$
- (Primality2)  $\perp \notin \Gamma$

**Lemma 5 (Saturated Extensions).** Suppose  $\Gamma \not\vdash \varphi$ , there is a saturated extension  $\Gamma^*$  such that  $\Gamma^* \not\vdash \varphi$ .

*Proof.* This is proved by standard Lindenbaum construction.

**Definition 9 (Canonical model).** We define the canonical model  $M^c$  as follows:

- Worlds of the canonical model are maximal theories  $\Gamma$
- $\Gamma \leq \Gamma'$  iff  $\Gamma \subseteq \Gamma'$
- $\Gamma S_A \Gamma'$  iff  $\{\varphi \mid A \text{ says } \varphi \in \Gamma\} \subseteq \Gamma'$
- $\Gamma R_A \Gamma'$  iff  $\{\varphi \mid A \text{ ratified } \varphi \in \Gamma\} \subseteq \Gamma'$
- $\Gamma C_A \Gamma'$  iff  $\{\varphi \mid A \text{ controls } \varphi \in \Gamma\} \subseteq \Gamma'$
- $\Gamma P_A \Gamma'$  iff  $\{\mathbf{P}_A \varphi \mid \varphi \in \Gamma'\} \subseteq \Gamma$
- $P \in \rho(\Gamma)$  iff  $P \in \Gamma$

**Lemma 6 (Existence Lemma).** For any state  $\Gamma_1 \in S^c$ , if  $\mathbf{P}_A \varphi \in \Gamma_1$ , then there is a state  $\Gamma_2 \in S^c$  such that  $\Gamma_1 P_A \Gamma_2$  and  $\varphi \in \Gamma_2$ .

*Proof.* Suppose  $\mathbf{P}_A \varphi \in \Gamma_1$ . We will construct a state  $\Gamma_2$  such that  $\Gamma_1 P_A \Gamma_2$  and  $\varphi \in \Gamma_2$ . Take  $\{\varphi\}$ , this set is consistent due to (Primality2) and  $\nVdash P_A \perp$ . Now, thanks to Lemma 5 let  $\Gamma_2$  be the saturated extension of  $\{\varphi\}$  such that  $\{P_A \psi \mid \psi \in \Gamma_2\} \subseteq \Gamma_1$ <sup>6</sup>. But then we get  $\Gamma_1 P_A \Gamma_2$ .

**Lemma 7.** Let  $\Gamma$  be a set of formulas and let  $\Delta = \{\varphi : A \text{ says } \varphi \in \Gamma\}$ . If  $\Delta \vdash \varphi$ , then  $\Gamma \vdash A \text{ says } \varphi$ .

*Proof.* Suppose that there is a derivation of  $\psi$  from  $\Delta$ . Then, there must be a finite set of formulas  $\{\varphi_1, \dots, \varphi_n\} \subseteq \Delta$  such that  $\{\varphi_1, \dots, \varphi_n\} \vdash \psi$ . By Theorem ??,  $\vdash \varphi_1 \wedge \dots \wedge \varphi_n \rightarrow \psi$ . By (nec-S) and (K-S),  $\vdash A \text{ says } \varphi_1 \wedge \dots \wedge A \text{ says } \varphi_n \rightarrow A \text{ says } \psi$ . As  $A \text{ says } \varphi_i \in \Gamma$  for all  $i = 1, \dots, n$ , by modus ponens,  $\Gamma \vdash A \text{ says } \beta$ .

**Lemma 8 (Canonical Model).** The canonical model  $M^c$  of Definition 7 is indeed a model of the logic.

*Proof.* First we notice that  $\leq$  is a preorder because  $\subseteq$  is. Then, we directly verify that  $M^c$  satisfies the semantic conditions reported in Definition 5.

(mon-S) Suppose  $\Gamma_1 \leq \Gamma_2$ ,  $\Gamma_2 S_A \Gamma_3$  and  $\Gamma_3 \leq \Gamma_4$ . We need to show that  $\Gamma_1 S_A \Gamma_4$ . Expanding definitions of  $S_A$  and  $\leq$  in  $\Gamma_1 \leq \Gamma_2$  and  $\Gamma_2 S_A \Gamma_3$  we get  $\{\varphi \mid A \text{ says } \varphi \in \Gamma_1 \subseteq \Gamma_3$ . Then, from  $\Gamma_3 \leq \Gamma_4$  we infer  $\Gamma_1 S_A \Gamma_4$ .

(mon-C) and (mon-R) cases are similar to (mon-S)

(s-I-SS) Suppose  $\Gamma_1 S_B \Gamma_2$  and  $\Gamma_2 S_A \Gamma_3$ . We need to show  $\Gamma_1 S_A \Gamma_3$ , i.e.,  $\{\varphi \mid A \text{ says } \varphi \in \Gamma_1\} \subseteq \Gamma_3$ . Now, pick any  $A \text{ says } \varphi \in \Gamma_1$ , we prove that  $\varphi \in \Gamma_3$ . Since  $A \text{ says } \varphi \in \Gamma_1$ , by axiom (I-SS) and condition (Closure) on  $\Gamma_1$ , we must also have  $B \text{ says } A \text{ says } \varphi \in \Gamma_1$ . Now, due that  $\Gamma_1 S_B \Gamma_2$ , we must have  $A \text{ says } \varphi \in \Gamma_2$  and thanks to  $\Gamma_2 S_A \Gamma_3$  we finally get  $\varphi \in \Gamma_3$ .

(s-C2P) Take any  $\Gamma_1 \in S^c$ , we show that there exists a  $\Gamma_2$  such that  $\Gamma_1 C_A \Gamma_2$  and  $\Gamma_1 P_A \Gamma_2$ . Due that  $\Gamma_1$  is maximal we have that it contains all substitutional instances

<sup>6</sup> Notice that it is always possible to construct  $\Gamma_2$  such that  $\{P_A \psi \mid \psi \in \Gamma_2\} \subseteq \Gamma_1$ , the proof is by induction of  $\psi$ .

of axiom (C2P)  $\mathbf{C}_A\varphi \rightarrow \mathbf{P}_A\varphi$ , in particular  $\mathbf{C}_A\top \rightarrow \mathbf{P}_A\top \in \Gamma_1$ . Moreover, as  $\top$  belongs to all maximal states, by generalization  $\Box\top$  does too, so  $\mathbf{C}_A\top \in \Gamma_1$ , but then  $\mathbf{P}_A\top \in \Gamma_1$ . Hence, by the Existence Lemma,  $\Gamma_1$  has a successor  $\Gamma_2$ .

(s-del-C) Suppose  $\Gamma_1\mathbf{C}_B\Gamma_2$  we need to show that, for any principal  $A$  then either (1)  $\Gamma_1\mathbf{C}_A\Gamma_2$  or (2) there exists a  $\Gamma_3$  s.t.  $\Gamma_1\mathbf{C}_A\Gamma_2$  and  $\Gamma_3\mathbf{C}_B\Gamma_2$ . The proof goes by contradiction, suppose that  $\neg\Gamma_1\mathbf{C}_A\Gamma_2$ , i.e., there exists a  $\psi_1$  s.t.  $\mathbf{C}_A\psi_1 \in \Gamma_1$  but  $\psi_1 \notin \Gamma_2$ . We now show that there exists a  $\Gamma_3$  such that  $\Gamma_1\mathbf{S}_A\Gamma_3$  and  $\Gamma_3\mathbf{C}_B\Gamma_2$ . Take the following consistent set  $\Theta = \{\varphi \mid A \text{ says } \varphi \in \Gamma_1\}$ , and let  $\Theta^*$  be it's saturated extension. By definition, we have that  $\Gamma_1\mathbf{S}_A\Theta^*$ , we claim that also  $\Theta^*\mathbf{C}_B\Gamma_2$ . Suppose, by contradiction that  $\{\varphi \mid \mathbf{C}_B\varphi \in \Theta^*\} \not\subseteq \Gamma_2$  then, by Lemma 7, we have that there exists a  $\psi_2$  s.t.  $A$  says  $\mathbf{C}_B\psi_2 \in \Gamma_1$ ,  $\mathbf{C}_B\psi_2 \in \Theta^*$  and  $\psi_2 \notin \Gamma_2$ . Now, by Definition 8, we get  $\mathbf{C}_A(\psi_1 \vee \psi_2) \in \Gamma_1$  and  $A$  says  $\mathbf{C}_B(\psi_2 \vee \psi_1) \in \Gamma_1$ , but then, via axiom (del-C) we get  $\mathbf{C}_B(\psi_2 \vee \psi_1)$ , which by hypothesis implies that  $\psi_2 \vee \psi_1 \in \Gamma_2$ , which is a contradiction. Therefore,  $\Theta^* = \Gamma_3$ .

(s-RS) Suppose  $\Gamma_1\mathbf{S}_A\Gamma_2$ , we need to show that  $\Gamma_1\mathbf{R}_A\Gamma_2$ . From the hypothesis we get that  $\{\varphi \mid A \text{ says } \varphi \in \Gamma_1\} \subseteq \Gamma_2$ . Thanks to axiom (RS) and (Closure) condition we have that  $\{\varphi \mid B \text{ ratified } \varphi \in \Gamma_1\} \subseteq \Gamma_2$ , i.e.,  $\Gamma_1\mathbf{R}_A\Gamma_2$ .

**Theorem 7 (Strong Completeness for ACL<sup>+</sup>).** If  $\Gamma \models \varphi$  then  $\Gamma \vdash \varphi$

*Proof.* Suppose  $\not\vdash \varphi$ , and let  $\Gamma_0$  be a saturated extension of  $\Gamma$ ,  $\varphi \notin \Gamma_0$ ; construct a canonical model  $\mathcal{M}^*$  as in Definition , then  $\mathcal{M}^*, \Gamma_0 \not\models \varphi$ . This yields completeness.

## 11 Appendix B: Proofs of Seq-ACL<sup>+</sup>

In order to prove that Seq-ACL<sup>+</sup> is sound and complete w.r.t. the semantics, we introduce some structural properties.

**Definition 10 (Complexity of a labelled formula).** We define the complexity of a labelled formula  $F$  as follows:

- $cp(x : \varphi) = 2 \times |\varphi|$
- $cp(x\mathbf{S}_A y) = cp(x\mathbf{C}_A y) = cp(x\mathbf{R}_A y) = cp(x\mathbf{P}_A y) = 3$
- $cp(x \leq y) = 2$

where  $|\varphi|$  is the number of symbols occurring in the string representing the formula  $\varphi$ .

**Lemma 9.**  $\Sigma; \mathbb{M}; \Gamma, F \Rightarrow \Delta, F$  is derivable in the calculus.

*Proof.* By induction on the complexity of the formula  $F$ .

**Lemma 10 (Height-preserving label substitution).** If a sequent  $\Sigma; \mathbb{M}; \Gamma \Rightarrow \Delta$  has a derivation of height  $h$ , then  $(\Sigma; \mathbb{M}; \Gamma)[x/z] \Rightarrow (\Delta)[x/z]$  has a derivation of height  $\leq h$ , where  $(\Sigma; \mathbb{M}; \Gamma)[x/z] \Rightarrow (\Delta)[x/z]$  is the sequent obtained from  $\Sigma; \mathbb{M}; \Gamma \Rightarrow \Delta$  by replacing a label  $x$  by a label  $z$  wherever it occurs.

### Axiom Rules

$$\frac{}{\Sigma; \mathbb{M}; x \leq y; \Gamma, x : p \Rightarrow y : p, \Delta} \text{init} \quad \frac{}{\Sigma; \mathbb{M}; \Gamma, x : \perp \Rightarrow \Delta} \perp\text{L} \quad \frac{}{\Sigma; \mathbb{M}; \Gamma \Rightarrow x : \top, \Delta} \top\text{R}$$

### Logical Rules

$$\frac{\Sigma; \mathbb{M}; \Gamma \Rightarrow_{\mathcal{T}} x : \alpha, \Delta \quad \Sigma; \mathbb{M}; \Gamma \Rightarrow_{\mathcal{T}} x : \beta, \Delta}{\Sigma; \mathbb{M}; \Gamma \Rightarrow_{\mathcal{T}} x : \alpha \wedge \beta, \Delta} \wedge\text{R} \quad \frac{\Sigma; \mathbb{M}; \Gamma, x : \alpha, x : \beta \Rightarrow_{\mathcal{T}} \Delta}{\Sigma; \mathbb{M}; \Gamma, x : \alpha \wedge \beta \Rightarrow_{\mathcal{T}} \Delta} \wedge\text{L}$$

$$\frac{\Sigma; \mathbb{M}; \Gamma \Rightarrow_{\mathcal{T}} x : \alpha, x : \beta, \Delta}{\Sigma; \mathbb{M}; \Gamma \Rightarrow_{\mathcal{T}} x : \alpha \vee \beta, \Delta} \vee\text{R} \quad \frac{\Sigma; \mathbb{M}; \Gamma, x : \alpha \Rightarrow_{\mathcal{T}} \Delta \quad \Sigma; \mathbb{M}; \Gamma, x : \beta \Rightarrow_{\mathcal{T}} \Delta}{\Sigma; \mathbb{M}; \Gamma, x : \alpha \vee \beta \Rightarrow_{\mathcal{T}} \Delta} \vee\text{L}$$

$$\frac{\Sigma; \mathbb{M}, x \leq y; \Gamma, x : \alpha \rightarrow \beta \Rightarrow_{\mathcal{T}} y : \alpha, \Delta \quad \Sigma; \mathbb{M}, x \leq y; \Gamma, x : \alpha \rightarrow \beta, y : \beta \Rightarrow_{\mathcal{T}} \Delta}{\Sigma; \mathbb{M}, x \leq y; \Gamma, x : \alpha \rightarrow \beta \Rightarrow \Delta} \rightarrow\text{L}$$

$$\frac{\Sigma, y; \mathbb{M}, x \leq y; \Gamma, y : \alpha \Rightarrow y : \beta, \Delta}{\Sigma; \mathbb{M}; \Gamma \Rightarrow x : \alpha \rightarrow \beta, \Delta} \rightarrow\text{R}_{y \text{ new}}$$

$$\frac{\Sigma; \mathbb{M}, xS_{Ay}; \Gamma, x : A \text{ says } \alpha, y : \alpha \Rightarrow \Delta}{\Sigma; \mathbb{M}, xS_{Ay}; \Gamma, x : A \text{ says } \alpha \Rightarrow \Delta} \text{says L} \quad \frac{\Sigma, y; \mathbb{M}, xS_{Ay}; \Gamma \Rightarrow_{\mathcal{T}} y : \alpha, \Delta}{\Sigma; \mathbb{M}; \Gamma \Rightarrow_{\mathcal{T}} x : A \text{ says } \alpha, \Delta} \text{says R}_{y \text{ new}}$$

$$\frac{\Sigma; \mathbb{M}, xC_{Ay}; \Gamma, x : \mathbf{C}_A \alpha, y : \alpha \Rightarrow \Delta}{\Sigma; \mathbb{M}, xC_{Ay}; \Gamma, x : \mathbf{C}_A \alpha \Rightarrow \Delta} \text{CL} \quad \frac{\Sigma, y; \mathbb{M}, xC_{Ay}; \Gamma \Rightarrow y : \alpha, \Delta}{\Sigma; \mathbb{M}; \Gamma \Rightarrow x : \mathbf{C}_A \alpha, \Delta} \text{CR}_{y \text{ new}}$$

$$\frac{\Sigma; \mathbb{M}, xR_{Ay}; \Gamma, x : A \text{ ratified } \alpha, y : \alpha \Rightarrow \Delta}{\Sigma; \mathbb{M}, xR_{Ay}; \Gamma, x : A \text{ ratified } \alpha \Rightarrow \Delta} \text{ratified L} \quad \frac{\Sigma, y; \mathbb{M}, xR_{Ay}; \Gamma \Rightarrow y : \alpha, \Delta}{\Sigma; \mathbb{M}; \Gamma \Rightarrow x : A \text{ ratified } \alpha, \Delta} \text{ratified R}_{y \text{ new}}$$

$$\frac{\Sigma; \mathbb{M}, xP_{Ay}; \Gamma \Rightarrow x : \mathbf{P}_A \alpha, y : \alpha, \Delta}{\Sigma; \mathbb{M}, xP_{Ay}; \Gamma \Rightarrow x : \mathbf{P}_A \alpha, \Delta} \text{PR} \quad \frac{\Sigma, y; \mathbb{M}, xP_{Ay}; \Gamma, y : \alpha \Rightarrow \Delta}{\Sigma; \mathbb{M}; \Gamma, x : \mathbf{P}_A \alpha \Rightarrow \Delta} \text{PL}_{y \text{ new}}$$

### Semantical Rules

$$\frac{\Sigma; \mathbb{M}, x \leq y, yS_{Az}, z \leq w, xS_{Aw}; \Gamma \Rightarrow \Delta}{\Sigma; \mathbb{M}, x \leq y, yS_{Az}, z \leq w; \Gamma \Rightarrow \Delta} \text{mon-S} \quad \frac{\Sigma; \mathbb{M}, x \leq y, yC_{Az}, z \leq w, xC_{Aw}; \Gamma \Rightarrow \Delta}{\Sigma; \mathbb{M}, x \leq y, yC_{Az}, z \leq w; \Gamma \Rightarrow \Delta} \text{mon-C}$$

$$\frac{\Sigma; \mathbb{M}, x \leq y, yR_{Az}, z \leq w, xR_{Aw}; \Gamma \Rightarrow \Delta}{\Sigma; \mathbb{M}, x \leq y, yR_{Az}, z \leq w; \Gamma \Rightarrow \Delta} \text{mon-R} \quad \frac{\Sigma; \mathbb{M}, x \leq y, zP_{Ay}, z \leq w, wP_{Ax}; \Gamma \Rightarrow \Delta}{\Sigma; \mathbb{M}, x \leq y, zP_{Ay}, z \leq w; \Gamma \Rightarrow \Delta} \text{mon-P}$$

$$\frac{\Sigma; \mathbb{M}, x \leq x; \Gamma \Rightarrow \Delta}{\Sigma; \mathbb{M}; \Gamma \Rightarrow \Delta} \text{refl}_{x \in \Sigma} \quad \frac{\Sigma; \mathbb{M}, x \leq y, y \leq z, x \leq z; \Gamma \Rightarrow \Delta}{\Sigma; \mathbb{M}, x \leq y, y \leq z; \Gamma \Rightarrow \Delta} \text{trans}$$

### Access Control Rules

$$\frac{\Sigma; \mathbb{M}, xS_{By}, yS_{Az}, xS_{Az}; \Gamma \Rightarrow \Delta}{\Sigma; \mathbb{M}, xS_{By}, yS_{Az}; \Gamma \Rightarrow \Delta} \text{s-I-SS} \quad \frac{\Sigma, y; \mathbb{M}, xC_{Ay}, xP_{Ay}; \Gamma \Rightarrow \Delta}{\Sigma; \mathbb{M}; \Gamma \Rightarrow \Delta} \text{s-C2P}_{y \text{ new}}$$

$$\frac{\Sigma; \mathbb{M}, xC_{By}, xC_{Ay}; \Gamma \Rightarrow \Delta \quad \Sigma, z; \mathbb{M}, xC_{By}, xS_{Az}, zC_{By}; \Gamma \Rightarrow \Delta}{\Sigma; \mathbb{M}, xC_{By}; \Gamma \Rightarrow \Delta} \text{s-del-C}_{z \text{ new}}$$

$$\frac{\Sigma; \mathbb{M}, xS_{Ay}, xR_{Ay}; \Gamma \Rightarrow \Delta}{\Sigma; \mathbb{M}, xS_{Ay}; \Gamma \Rightarrow \Delta} \text{s-RS}$$

**Fig. 3.** Seq-ACL<sup>+</sup> Rules

*Proof.* By induction of the height of a derivation of  $\Sigma; \mathbb{M}; \Gamma \Rightarrow \Delta$ . We show only some cases,

- Suppose that *init* is applied to  $\Sigma; \mathbb{M}; \Gamma \Rightarrow \Delta$  with a derivation of height 1:

$$\frac{}{\Sigma; \mathbb{M}', x \leq y; \Gamma, x : p \Rightarrow y : p, \Delta} \text{init}$$

Our goal is to find a proof of height  $\leq 1$  of

$$(\Sigma; \mathbb{M}', x \leq y; \Gamma', x : p)[x/z] \Rightarrow y : p, \Delta[x/z]$$

for every  $z$ . The case of  $z \neq y$  is trivial, in case of  $z = y$  we have

$$\Sigma; \mathbb{M}', y \leq y; \Gamma', y : p \Rightarrow y : p, \Delta[x/y]$$

which is an axiom and therefore has a proof of height 1.

- Suppose that  $\top R$  is applied to  $\Sigma; \mathbb{M}; \Gamma \Rightarrow \Delta$  with a derivation of height 1:

$$\frac{}{\Sigma; \mathbb{M}; \Gamma \Rightarrow x : \top, \Delta'} \top R$$

Then also  $(\Sigma; \mathbb{M}; \Gamma)[x/z] \Rightarrow (x : \top, \Delta')[x/z]$  has a proof of height 1, for every  $z$ .

- Suppose that  $\perp L$  is applied to  $\Sigma; \mathbb{M}; \Gamma \Rightarrow \Delta$  with a derivation of height 1:

$$\frac{}{\Sigma; \mathbb{M}; \Gamma', x : \perp \Rightarrow \Delta} \perp L$$

Then also  $(\Sigma; \mathbb{M}; \Gamma', x : \perp)[x/z] \Rightarrow \Delta[x/z]$  has a proof of height 1, for every  $z$ .

- Suppose that  $\wedge R$  is applied to  $\Sigma; \mathbb{M}; \Gamma \Rightarrow \Delta$  with a derivation of height  $h$ :

$$\frac{(1)\Sigma; \mathbb{M}; \Gamma \Rightarrow x : \alpha, \Delta' \quad (2)\Sigma; \mathbb{M}; \Gamma \Rightarrow x : \beta, \Delta'}{\Sigma; \mathbb{M}; \Gamma \Rightarrow x : \alpha \wedge \beta, \Delta'} \wedge R$$

Our goal is to find a proof of height  $\leq h$  of  $(\Sigma; \mathbb{M}; \Gamma)[x/z] \Rightarrow z : \alpha \wedge \beta, \Delta'[x/z]$ . Applying the inductive hypothesis to (1) and (2) we have proofs of height  $\leq h - 1$  of the sequents:

(3)  $(\Sigma; \mathbb{M}; \Gamma)[x/z] \Rightarrow z : \alpha, \Delta'[x/z]$  and

(4)  $(\Sigma; \mathbb{M}; \Gamma)[x/z] \Rightarrow z : \beta, \Delta'[x/z]$

But from (3) and (4), applying  $\wedge R$ , we get (5)  $(\Sigma; \mathbb{M}; \Gamma)[x/z] \Rightarrow z : \alpha \wedge \beta, \Delta'[x/z]$

- Suppose that  $\rightarrow R$  is applied to  $\Sigma; \mathbb{M}; \Gamma \Rightarrow \Delta$  with a derivation of height  $h$ :

$$\frac{(1)\Sigma, y; \mathbb{M}, x \leq y; \Gamma, y : \alpha \Rightarrow y : \beta, \Delta'}{\Sigma; \mathbb{M}; \Gamma \Rightarrow x : \alpha \rightarrow \beta, \Delta'} \rightarrow R$$

Our goal is to find a proof of height  $\leq h$  of  $(\Sigma; \mathbb{M}; \Gamma)[x/z] \Rightarrow z : \alpha \rightarrow \beta, \Delta'[x/z]$ . Without loss of generality we can suppose  $z \neq y$  due that the label  $y$  in the above derivation is a new label, not occurring in the conclusion of  $\rightarrow R$ . Applying the inductive hypothesis on the premise of  $\rightarrow R$ , we obtain a proof of

$$(\Sigma, y; \mathbb{M}, z \leq y; \Gamma, y : \alpha)[x/z] \Rightarrow y : \beta, \Delta'[x/z]$$

of height no greater than  $h - 1$ . We conclude by an application of  $\rightarrow R$ , obtaining a proof (height  $\leq h$ ) of  $(\Sigma; \mathbb{M}; \Gamma)[x/z] \Rightarrow z : \alpha \rightarrow \beta, \Delta'[x/z]$ .

**Theorem 8 (Height-preserving admissibility of weakening).** *If a sequent  $\Sigma; \mathbb{M}; \Gamma \Rightarrow \Delta$  has a derivation of height  $h$ , then  $\Sigma; \mathbb{M}; \Gamma \Rightarrow \Delta, F$ , and  $(\Sigma; \mathbb{M}; \Gamma), F \Rightarrow \Delta$  have a derivation of height  $\leq h$ . Where  $F$  can be either a world or a transition formula <sup>7</sup>.*

*Proof.* By induction on the height of a derivation of  $\Sigma; \mathbb{M}; \Gamma \Rightarrow \Delta$ .

**Theorem 9 (Height-preserving invertibility of rules).** *Let  $\Sigma; \mathbb{M}; \Gamma \Rightarrow \Delta$  be the conclusion of an application of one of the rules of the calculus, say  $R$ . If  $\Sigma; \mathbb{M}; \Gamma \Rightarrow \Delta$  is derivable, then the premise(s) of  $R$  is (are) derivable with a derivation of (at most) the same height, i.e., rules of the calculus are height-preserving invertible.*

*Proof.* We consider each of the rules.

saysL, CL, ratified L, PR and all semantic and access control rules of Figure 11: these rules are height-preserving invertible, since their premise(s) is (are) obtained by weakening from the conclusion, and weakening is height-preserving admissible (Theorem 8).

Take ( $\rightarrow R$ ), we proceed by an inductive argument on the height of a proof of its conclusions: for any  $y$ , if  $\Sigma; \mathbb{M}; \Gamma, x : \alpha \rightarrow \beta \Rightarrow \Delta$  is an axiom, then  $\Sigma, y; \mathbb{M}, x \leq y; \Gamma, y : \alpha \Rightarrow y : \beta, \Delta$  is an axiom too, since axioms are restricted to atomic formulas. If  $h > 0$  and the proof of  $\Sigma; \mathbb{M}; \Gamma, x : \alpha \rightarrow \beta \Rightarrow \Delta$  is concluded (looking forward) by any rule other than  $\rightarrow R$ , we apply the inductive hypothesis to the premise(s), then we conclude by applying the same rule. If the derivation of  $\Sigma; \mathbb{M}; \Gamma, x : \alpha \rightarrow \beta \Rightarrow \Delta$  is ended by  $\rightarrow R$  we have the following subcases:

- $x : \alpha \rightarrow \beta$  is the principal formula of  $\rightarrow R$ , the proof is ended as follows:

$$\frac{\Sigma, y; \mathbb{M}, x \leq y; \Gamma, y : \alpha \Rightarrow y : \beta, \Delta}{\Sigma; \mathbb{M}; \Gamma \Rightarrow x : \alpha \rightarrow \beta, \Delta} \rightarrow R$$

We have a proof of  $\Sigma, y; \mathbb{M}, x \leq y; \Gamma, y : \alpha \Rightarrow y : \beta, \Delta$  of height  $h - 1$  and the proof is over;

- $x : \alpha \rightarrow \beta$  is not the principal formula of  $\rightarrow R$ ; the proof is ended as follows:

$$\frac{\Sigma, z; \mathbb{M}, w \leq z; \Gamma, z : \alpha \Rightarrow z : \beta, x : \alpha \rightarrow \beta, \Delta}{\Sigma; \mathbb{M}; \Gamma \Rightarrow x : \alpha \rightarrow \beta, w : \alpha' \rightarrow \beta', \Delta} \rightarrow R$$

where  $z$  is a “new” label and then, without loss of generality, we can assume that  $z$  is not  $y$ , since we can apply the height-preserving label substitution. By inductive hypothesis on the premise we obtain a derivation of

$$\Sigma, y, z; \mathbb{M}, w \leq z, x \leq y; \Gamma, z : \alpha', y : \alpha \Rightarrow z : \beta', y : \beta, \Delta$$

from which we can conclude as follows:

$$\frac{\Sigma, z, y; \mathbb{M}, w \leq z, x \leq y; \Gamma, z : \alpha', y : \alpha \Rightarrow z : \beta', y : \beta, \Delta}{\Sigma, y; \mathbb{M}, x \leq y; \Gamma, y : \alpha \Rightarrow y : \beta, w : \alpha' \rightarrow \beta'} \rightarrow R$$

<sup>7</sup> If  $F$  is a world formula then  $(\Sigma; \mathbb{M}; \Gamma), F = \Sigma; \mathbb{M}; \Gamma, F$ . Otherwise, if  $F$  is a transition formula then  $(\Sigma; \mathbb{M}; \Gamma), F = \Sigma; \mathbb{M}, F; \Gamma$ .

Take **CR** we proceed by an inductive argument on the height of a proof of their conclusions: In case of  $\Sigma; \mathbb{M}; \Gamma \Rightarrow x : \mathbf{C}_A \alpha, \Delta$  being an axiom the proof is trivial. If  $h > 0$  and the proof of  $\Sigma; \mathbb{M}; \Gamma \Rightarrow x : \mathbf{C}_A \alpha, \Delta$  is concluded (looking forward) by any rule other than (**CR**), we apply the inductive hypothesis to the premise(s), then we conclude by applying the same rule. If the derivation is ended by (**CR**) we have the following subcases:

- $x : \mathbf{C}_A \alpha$  is the principal formula of (**CR**): the proof is ended as follows

$$\frac{\Sigma, y; \mathbb{M}, x \mathbf{C}_A y; \Gamma \Rightarrow y : \alpha, \Delta}{\Sigma; \mathbb{M}; \Gamma \Rightarrow x : \mathbf{C}_A \alpha, \Delta} \mathbf{CR}$$

We have a proof of  $\Sigma, y; \mathbb{M}, x \mathbf{C}_A y; \Gamma \Rightarrow y : \alpha, \Delta$  of height  $h - 1$  and the proof is over;

- $x : \mathbf{C}_A \alpha$  is not the principal formula of **CR**: the proof is ended as follows

$$\frac{\Sigma, z; \mathbb{M}, w \mathbf{C}_A z; \Gamma \Rightarrow z : \alpha', \Delta}{\Sigma; \mathbb{M}; \Gamma \Rightarrow x : \mathbf{C}_A \alpha, w : \mathbf{C}_A \alpha' \Delta} \mathbf{CR}$$

where  $z$  is “new” label and therefore, without loss of generality, we can assume that  $z$  is not  $y$ , since we can apply the height-preserving label substitution. By inductive hypothesis on the premise we obtain a derivation of

$$\Sigma, z, y; \mathbb{M}, w \mathbf{C}_A z, x \mathbf{C}_A y; \Gamma \Rightarrow z : \alpha', y : \alpha, \Delta$$

from which we conclude as follows:

$$\frac{\Sigma, z, y; \mathbb{M}, w \mathbf{C}_A z, x \mathbf{C}_A y; \Gamma \Rightarrow z : \alpha', y : \alpha, \Delta}{\Sigma, y; \mathbb{M}, x \mathbf{C}_A y; \Gamma \Rightarrow y : \alpha, w : \mathbf{C}_A \alpha' \Delta}$$

The cases for remaining rules proceed similarly.

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  $\Sigma_1; \mathbb{M}_1; \Gamma_1 \Rightarrow \Delta_1$  is derivable by Theorem 9 since it is the premise of a backward application of an invertible rule **R** to  $\Sigma_2; \mathbb{M}_2; \Gamma_2 \Rightarrow \Delta_2$ , then it has a derivation containing *the same rule applications* of the proof of  $\Sigma_2; \mathbb{M}_2; \Gamma_2 \Rightarrow \Delta_2$ . This fact will be used systematically in the remaining 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.

**Theorem 10 (Height-preserving admissibility of contraction).** *The rules of contraction are height-preserving admissible in our calculus, i.e., if a sequent  $\Sigma; \mathbb{M}; \Gamma \Rightarrow \Delta, F, F$  is derivable in the calculus, then there is a derivation of a no greater height of  $\Sigma; \mathbb{M}; \Gamma \Rightarrow F, \Delta$ , and if a sequent  $(\Sigma; \mathbb{M}; \Gamma), F, F \Rightarrow \Delta$  is derivable in the calculus, then there is a derivation of no greater height of  $(\Sigma; \mathbb{M}; \Gamma), F \Rightarrow \Delta$ . Moreover, the proof of the contracted sequent does not add any rule application to the initial proof. In this case we say that the contractions are rule-preserving admissible.*

*Proof.* By simultaneous induction on the height of derivation fro left and right contraction. If  $h = 0$ , i.e.,  $\Sigma; \mathbb{M}; \Gamma \Rightarrow \Delta, F, F$  is an axiom, then we have to consider the following subcases:

- $w : \perp \in \Gamma$ : in this case, obviously  $\Sigma; \mathbb{M}; \Gamma \Rightarrow \Delta, F$  is an axiom too;
- an atom  $x : p \in \Gamma \cap \Delta$ : the proof is over, since  $\Sigma; \mathbb{M}; \Gamma \Rightarrow \Delta, F$  is an axiom too;
- $F$  is an atom and  $x : p \in \Gamma$ : the proof is over, observing that  $\Sigma; \mathbb{M}; \Gamma \Rightarrow \Delta, F$  is an axiom too.

The proof of the case where  $(\Sigma; \mathbb{M}; \Gamma), F, F \Rightarrow \Delta$  is an axiom is symmetric.

If  $h > 0$ , consider the last rule applied (looking forward) to derive the premise of contraction. We distinguish two cases:

- the contracted formula  $F$  is not principal in it: 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).
- the contracted formula  $F$  is principal in it, we consider all the rules:
  - $\wedge R$ : the proof is ended as follows,

$$\frac{(1)\Sigma; \mathbb{M}; \Gamma \Rightarrow x : \alpha, x : \alpha \wedge \beta, \Delta \quad (2)\Sigma; \mathbb{M}; \Gamma \Rightarrow x : \beta, x : \alpha \wedge \beta \Delta}{\Sigma; \mathbb{M}; \Gamma \Rightarrow x : \alpha \wedge \beta, x : \alpha \wedge \beta \Delta} \wedge R$$

Since  $\wedge R$  is height-preserving invertible (see Theorem 9), there is a derivation of no greater height than (1) of  $(1a)\Sigma; \mathbb{M}; \Gamma \Rightarrow x : \alpha, x : \alpha, \Delta$  and a derivation of no greater height than (2) of  $(2a)\Sigma; \mathbb{M}; \Gamma \Rightarrow x : \beta, x : \beta, \Delta$ . Applying the inductive hypothesis on (1a) and (2a) and applying  $(\wedge R)$  to the contracted sequents, we obtain a derivation of no greater height ending with (be  $(1a')$   $(2a')$  the contracted sequents):

$$\frac{(1a')\Sigma; \mathbb{M}; \Gamma \Rightarrow x : \alpha, \Delta \quad (2a')\Sigma; \mathbb{M}; \Gamma \Rightarrow x : \beta \Delta}{\Sigma; \mathbb{M}; \Gamma \Rightarrow x : \alpha \wedge \beta \Delta} \wedge R$$

- For  $(\wedge L), (\vee R), (\vee L), (\rightarrow R), (\rightarrow L)$  we proceed as in the previous case, since all the rules are height preserving.
- **CR**: the proof is ended by:

$$\frac{\Sigma, y; \mathbb{M}, x C_A y; \Gamma \Rightarrow y : \alpha, x : C_A \alpha, \Delta}{\Sigma; \mathbb{M}; \Gamma \Rightarrow x : C_A \alpha, x : C_A \alpha, \Delta} \mathbf{CR}$$

Applying the height-preserving invertibility of **CR**, we have a proof of

$$(1)\Sigma, y, z; \mathbb{M}, x C_A y, x \tilde{N}_i z; \Gamma \Rightarrow y : \alpha, z : \alpha, \Delta$$

Applying the height-preserving label substitution (Lemma 10), replacing  $z$  with  $y$ , we obtain a derivation of sequent

$$(2)\Sigma, y; \mathbb{M}, x C_A y, x C_A y; \Gamma \Rightarrow y : \alpha, y : \alpha, \Delta$$

since  $y$  and  $z$  are new labels not occurring in  $\Gamma, \Delta$ . We can then apply the inductive hypothesis on (2), obtaining a proof of (3)  $\Sigma, y; \mathbb{M}, x C_A y; \Gamma \Rightarrow y : \alpha, \Delta$ , from which we conclude by an application of **CR**:

$$\frac{(3)\Sigma, y; \mathbb{M}, x C_A y; \Gamma \Rightarrow y : \alpha, \Delta}{\Sigma; \mathbb{M}; \Gamma \Rightarrow x : C_A \alpha, \Delta} \mathbf{CR}$$

- **CL** we have a proof ending with:

$$\frac{\Sigma; \mathbb{M}, x C_A y; \Gamma, x : C_A \alpha, x : C_A \alpha, y : \alpha \Rightarrow \Delta}{\Sigma; \mathbb{M}; \Gamma, x : C_A \alpha \Rightarrow \Delta} \mathbf{CL}$$

The cases for the remaining rules proceed similarly.

We now prove the admissibility of cut:

**Theorem 11 (Admissibility of cut).**  $\Sigma; \mathbb{M}; \Gamma \Rightarrow x : \alpha, \Delta$  and  $\Sigma; \mathbb{M}; \Gamma, x : \alpha \Rightarrow \Delta$  imply  $\Sigma; \mathbb{M}; \Gamma \Rightarrow \Delta$ .

*Proof.* As usual, the proof proceeds by a double induction over the complexity of the cut formula 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. We have several cases: (i) one of the two premises is an axiom, (ii) the last step of one of the two premises is obtained by a rule in which  $F$  is not the principal formula, (iii)  $F$  is the principal formula in the last step of both derivations.

- (i) If one of the two premises is an axiom then either  $\Sigma; \mathbb{M}; \Gamma \Rightarrow \Delta$  is an axiom, or the premise which is not an axiom contains two copies of  $x : \alpha$  and  $\Sigma; \mathbb{M}; \Gamma \Rightarrow \Delta$  can be obtained by contraction, which is admissible.
  - (ii) If the last step of one of the two premises is obtained by a rule, say (R), in which  $x : \alpha$  is not the principal formula we proceed as follows: we cut the premise(s) of (R) and then we apply (R) to the result of the cut.
  - (iii) If  $x : \alpha$  is the principal formula in both the inferences steps leading to the two cut premises there are ... subcases:  $x : \alpha$  is introduced by (a)  $\wedge L, \wedge R$ ; (b) by  $\vee L, \vee R$ ; (c) by  $\rightarrow L, \rightarrow R$ ; (d) **CL, CR**, says L, says R, ratified L, ratified R and (e) **PL, PR**
- (a), (b) The proof is easy and left to the reader
- (c) We have to prove that (1)  $\Sigma; \mathbb{M}, x \leq y; \Gamma, x : \alpha \rightarrow \beta \Rightarrow \Delta$  and (2)  $\Sigma; \mathbb{M}, x \leq y; \Gamma \Rightarrow x : \alpha \rightarrow \beta, \Delta$  imply (3)  $\Sigma; \mathbb{M}, x \leq y; \Gamma \Rightarrow \Delta$ <sup>8</sup>.
- \* The premises of rule  $\rightarrow L$  applied over (1) are

$$(4) \Sigma; \mathbb{M}, x \leq y; \Gamma, x : \alpha \rightarrow \beta; \Rightarrow y : \alpha, \Delta$$

$$(5) \Sigma; \mathbb{M}, x \leq y; \Gamma, x : \alpha \rightarrow \beta, y : \beta; \Rightarrow \Delta$$

- \* The premise of rule  $\rightarrow R$  applied over (2) is

$$(6) \Sigma, z; \mathbb{M}, x \leq y, x \leq z; \Gamma, z : \alpha \Rightarrow z : \beta, \Delta$$

<sup>8</sup> Notice that both meta contexts  $\mathbb{M}$  in (1) and (2) have  $x \leq y \in \mathbb{M}$  because it is a condition for the applicability of rule  $\rightarrow L$ .

Now, by inductive hypothesis, we apply the cut rule as follows:

- \* We cut (2) and (4) on the height of the proof to obtain

$$(7) \Sigma; \mathbb{M}, x \leq y; \Gamma \Rightarrow y : \alpha, \Delta$$

- \* We cut (2) and (5) on the height of the proof to obtain

$$(8) \Sigma; \mathbb{M}, x \leq y; \Gamma, y : \beta \Rightarrow \Delta$$

- \* By height-preserving label substitution and contraction, we obtain a proof of no greater height than (6) of

$$(9) \Sigma; \mathbb{M}, x \leq y; \Gamma, y : \alpha \Rightarrow y : \beta, \Delta$$

- \* We cut (9) and (7) on the complexity of the formula (i.e.  $y : \alpha$ ) to obtain

$$(10) \Sigma; \mathbb{M}, x \leq y; \Gamma \Rightarrow y : \beta, \Delta$$

- \* Finally, we cut (10) and (8) on the complexity of the formula (i.e.,  $y : \beta$ ) to obtain

$$(11) \Sigma; \mathbb{M}, x \leq y; \Gamma \Rightarrow \Delta$$

- (d) We have to prove that (1)  $\Sigma; \mathbb{M}, x C_A y; \Gamma, x : \mathbf{C}_A \alpha \Rightarrow \Delta$  and (2)  $\Sigma; \mathbb{M}, x C_A y; \Gamma \Rightarrow x : \mathbf{C}_A \alpha, \Delta$  imply (3)  $\Sigma; \mathbb{M}, x C_A y; \Gamma \Rightarrow \Delta$

- \* The premise of the rule **CL** applied over (1) is

$$(4) \Sigma; \mathbb{M}, x C_A y; \Gamma, x : \mathbf{C}_A \alpha, y : \alpha \Rightarrow \Delta$$

- \* The premise of the rule **CR** applied over (2) is

$$(5) \Sigma, z; \mathbb{M}, x C_A y, x C_A z; \Gamma \Rightarrow z : \alpha, \Delta$$

Now, by inductive hypothesis, we apply the cut rule as follows:

- \* We cut (2) and (4) on the height of the proof to obtain

$$(6) \Sigma; \mathbb{M}, x C_A y; \Gamma, y : \alpha \Rightarrow \Delta$$

- \* By height-preserving label substitution and contraction, we obtain a proof of no greater height than (5) of

$$(7) \Sigma; \mathbb{M}, x C_A y; \Gamma \Rightarrow y : \alpha, \Delta$$

- \* Finally, we cut (7) and (6) on the complexity of the formula (i.e.,  $y : \alpha$ ) to obtain

$$(8) \Sigma; \mathbb{M}, x C_A y, \Gamma \Rightarrow \Delta$$

The cases for says and ratified proceed similarly.

- (e) We have to show that (1)  $\Sigma; \mathbb{M}, x P_A y; \Gamma, x : \mathbf{P}_A \alpha \Rightarrow \Delta$  and (2)  $\Sigma; \mathbb{M}, x P_A y; \Gamma \Rightarrow \mathbf{P}_A \alpha, \Delta$  imply (3)  $\Sigma; \mathbb{M}, x P_A y; \Gamma \Rightarrow \Delta$  Now, by inductive hypothesis, we apply the cut rule as follows:

\* The premise of the rule **PL** applied over (1) is

$$(4) \Sigma, z; \mathbb{M}, xP_Ay, xP_Az; \Gamma, z : \alpha \Rightarrow \Delta$$

\* The premise of the rule **PR** applied over (2) is

$$(5) \Sigma; \mathbb{M}, xP_Ay; \Gamma \Rightarrow x : \mathbf{P}_A\alpha, y : \alpha, \Delta$$

Now, by inductive hypothesis, we apply the cut rule as follows:

\* First, by height-preserving label substitution and contraction, we obtain a proof of no greater height than (4) of

$$(6) \Sigma; \mathbb{M}, xP_Ay; \Gamma, y : \alpha \Rightarrow \Delta$$

\* We then cut (1) and (5) on the height of the proof to obtain

$$(7) \Sigma; \mathbb{M}, xP_Az; \Gamma \Rightarrow y : \alpha, \Delta$$

\* Finally, we cut (7) and (6) on the complexity of the formula (i.e.,  $y : \alpha$ ) to obtain

$$(8) \Sigma; \mathbb{M}, xP_Ay; \Gamma \Rightarrow \Delta$$

**Theorem 12 (Soundness of Seq-ACL<sup>+</sup>).** *If a sequent  $\Sigma; \mathbb{M}; \Gamma \Rightarrow \Delta$  is derivable then,  $\Sigma; \mathbb{M}; \Gamma \Rightarrow \Delta$  it is valid in the sense of Definition 5*

*Proof.* By induction on the height of the derivation of  $\Sigma; \mathbb{M}; \Gamma \Rightarrow \Delta$ . We only present the inductive step for some of the rules:

(s-I-SS) Suppose that the derivation of  $\Sigma; \mathbb{M}', xS_By, yS_Az; \Gamma \Rightarrow \Delta$  ends by an application of s-I-SS: by inductive hypothesis, the premise  $\Sigma; \mathbb{M}', xS_By, yS_Az, xS_Az; \Gamma \Rightarrow \Delta$  is a valid sequent. By contradiction, 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  $F \in \mathbb{M}' \cup \Gamma$ ,  $\mathcal{M} \models_I xS_By$  and  $\mathcal{M} \models_I yS_Az$ , whereas  $\mathcal{M} \not\models_I G$  for any  $G \in \Delta$ . By (s-I-SS) of Definition 5, we have that, since  $I(x)S_B I(y)$  and  $I(y)S_A I(z)$ , then also  $I(x)S_A I(z)$ , then  $\mathcal{M} \models_I xS_Az$  and therefore it the premise  $\Sigma; \mathbb{M}', xS_By, yS_Az, xS_Az; \Gamma \Rightarrow \Delta$  is valid, then also the conclusion has to be valid, which is a contradiction. The proof is similar for all semantic and access control rules in Figure 11.

(saysR) Suppose that the derivation of  $\Sigma; \mathbb{M}; \Gamma \Rightarrow A \text{ says } \alpha, \Delta'$  ends by an application of saysR. By inductive hypothesis, the premise  $\Sigma, y; \mathbb{M}, xS_Ay; \Gamma \Rightarrow y : \alpha, \Delta'$  is a valid sequent. By contradiction, 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  $F \in \mathbb{M} \cup \Gamma$ , whereas  $\mathcal{M} \not\models_I G$  for any  $G \in \Delta$  and  $\mathcal{M} \not\models_I x : A \text{ says } \alpha$ , which means that there exists a label  $z$  such that  $I(x)S_A I(z)$  and  $\mathcal{M}, I(z) \not\models \alpha$ . We can define an interpretation  $I'(k) = I(k)$  for  $k \neq y$  and  $I'(y) = z$ . Since  $y$  in the premiss does not occur in  $\Sigma \cup \mathbb{M} \cup \Gamma \cup \Delta'$  and it is different from  $x$ , we have that  $\mathcal{M} \models_{I'} F$  for every  $F \in \mathbb{M} \cup \Gamma$ ,  $\mathcal{M} \not\models_{I'} G$  for any  $G \in \Delta$ ,  $\mathcal{M} \not\models_{I'} y : \alpha$  but  $\mathcal{M} \models_{I'} xS_Ay$ , against the validity of  $\Sigma, y; \mathbb{M}, xS_Ay; \Gamma \Rightarrow y : \alpha, \Delta'$ .

**Theorem 13 (Completeness of Seq-ACL<sup>+</sup>).** *If a formula  $\alpha$  is valid in ACL<sup>+</sup>, then  $x; \emptyset; \emptyset \Rightarrow x : \alpha$  is derivable in Seq-ACL<sup>+</sup>.*

*Proof.* If  $\alpha$  is valid in ACL<sup>+</sup> then, thanks to Theorem 7,  $\alpha$  is a theorem in the corresponding axiomatization (i.e.,  $\vdash \alpha$ ). We show that if  $\vdash \alpha$ , then  $x; \emptyset; \emptyset \Rightarrow x : \alpha$  is derivable. In order to do this, we must show that the axioms are derivable and that the set of derivable formulas is closed under rules (MP), (nec-S), (nec-C) and (nec-R). We left derivation of axioms to the reader and we focus on showing the admissibility of rules (MP) and (nec-R)

(MP) Suppose that  $x; \emptyset; \emptyset \Rightarrow x : \alpha \rightarrow \beta$  and  $x; \emptyset; \emptyset \Rightarrow x : \alpha$  are derivable. We easily have that  $x; \emptyset; x : \alpha \rightarrow \beta, x : \alpha \Rightarrow x : \beta$  is derivable too. Since cut is admissible (see Theorem 11), by two cuts we obtain  $x; \emptyset; \emptyset \vdash x : \beta$ , as follows

$$\frac{\frac{x; \emptyset; x : \alpha \rightarrow \beta, x : \alpha \Rightarrow x : \beta \quad x; \emptyset; \emptyset \Rightarrow x : \alpha \rightarrow \beta}{x; \emptyset; x : \alpha \Rightarrow x : \beta} \text{ (cut)} \quad x; \emptyset; \emptyset \Rightarrow x : \alpha}{x; \emptyset; \emptyset \Rightarrow x : \beta} \text{ (cut)}$$

(nec-R) Suppose that  $x; \emptyset; \emptyset \Rightarrow x : \alpha$  is derivable, we need to show that  $x; \emptyset; \emptyset \Rightarrow x : A \text{ ratified } \alpha$  is. First we notice that, by height preserving label substitution,  $y; \emptyset; \emptyset \Rightarrow y : \alpha$  is derivable and, by height preserving admissibility of weakening,  $x, y; xR_A y; \emptyset \Rightarrow y : \alpha$  is derivable too. But then, we can prove  $x; \emptyset; \emptyset \Rightarrow x : A \text{ ratified } \alpha$  as follows

$$\frac{x, y; xR_A y; \emptyset \Rightarrow y : \alpha}{x; \emptyset; \emptyset \Rightarrow x : A \text{ ratified } \alpha} \text{ ratified } R$$

## 11.1 Termination

In general, cut-freeness alone does not ensure termination of proof search in a sequent calculus; the presence of labels and of rules saysL, ratifiedL, CL, PR, and semantic and access control rules in Figure 11 which increase the complexity of the sequent in a backward proof search, are potential causes of a nonterminating proof search.

First we give some definitions that will be useful in the rest of the Section.

**Definition 11 (Formula Depth).** *Given a formula  $\varphi$  we define  $\text{dept}(\varphi)$  inductively on the structure of  $\varphi$  as follows:*

- $\text{dept}(p) = 0$ , with  $p$  propositional variable.
- $\text{dept}(\alpha \circ \beta) = \max\{\text{dept}(\alpha), \text{dept}(\beta)\}$ , with  $\circ \in \{\wedge, \vee, \rightarrow\}$ .
- $\text{dept}(\bigcirc \alpha) = \text{dept}(\alpha) + 1$ , with  $\bigcirc \in \{A \text{ says}, \mathbf{C}_A, A \text{ ratified}, \mathbf{P}_A\}$

**Definition 12 (Label distance).** *Given a sequent  $\Sigma, \mathbb{M}, \Gamma \Rightarrow \Delta$  and two labels  $x$  and  $y$  such that  $x \leq y \in \Gamma$ , we define the distance  $d(x, y)$  between two labels as:*

(case  $y = x$ )  $d(x, y) = 0$

(case  $y \neq x$ )  $d(x, y) = n$  where  $n$  is the length of the longest sequence of transitions in  $\mathbb{M}$  “connecting” the two labels, i.e.,  $x \overset{\sim}{\circ} x_1, x_1 \overset{\sim}{\circ} x_2, \dots, x_{n-1} \overset{\sim}{\circ} y$  where  $\overset{\sim}{\circ} \in$

$\{A \text{ says, } \mathbf{C}_A, A \text{ ratified, } \mathbf{P}_A, \leq\}$ <sup>9</sup>. As an example if  $\{x \leq y, yC_Az, zP_Ak, xS_Ak\} \in \mathbb{M}$  we have  $d(x, k) = 3$ .

We first show that both **CL**, *A says*, *A ratified*,  $\mathbf{P}_iR$  and rules in Figures ??, ?? can be applied in a controlled way.

**Lemma 11 (Controlled use of CL).** *It is useless to apply CL on the same transition  $xC_Ay \in \mathbb{M}$  more than once in a backward proof search in each branch of a derivation*

*Proof.* Consider a proof where **CL** is applied more than once on the same transition in a derivation and consider the two highest applications: since **CL** is invertible, we can consider, without loss of generality, that the two applications of  $\mathbf{C}_A L$  are consecutive, as follows:

$$\frac{\frac{(1)\Sigma; \mathbb{M}, xC_Ay; \Gamma, x : \mathbf{C}_A\alpha, x : \mathbf{C}_A\alpha, y : \alpha, y : \alpha \Rightarrow \Delta}{\Sigma; \mathbb{M}, xC_Ay; \Gamma, x : \mathbf{C}_A\alpha, x : \mathbf{C}_A\alpha, y : \alpha \Rightarrow \Delta} (\mathbf{C}L)}{\Sigma; \mathbb{M}; \Gamma, x : \mathbf{C}_A\alpha \Rightarrow \Delta} (\mathbf{C}L)$$

From (1) we can find a derivation of  $(1')\Sigma; \mathbb{M}; \Gamma, x : \mathbf{C}_A\alpha, x : \mathbf{C}_A\alpha, y : \alpha \Rightarrow \Delta$  by contraction and this derivation does not have any application of **CL** having  $xC_Ay$  as a principal formula (remember that contraction is rule-preserving admissible). Thus, we can remove one application of **CL** as follows:

$$\frac{(1')\Sigma; \mathbb{M}, xC_Ay; \Gamma, x : \mathbf{C}_A\alpha, x : \mathbf{C}_A\alpha, y : \alpha \Rightarrow \Delta}{\Sigma; \mathbb{M}, xC_Ay; \Gamma, x : \mathbf{C}_A\alpha \Rightarrow \Delta} \mathbf{C}L$$

**Lemma 12 (Controlled use of PR).** *It is useless to apply PR on the same transition  $xP_Ay \in \mathbb{M}$  more than once in a backward proof search in each branch of a derivation*

*Proof.* Consider a proof where **PR** is applied more than once on the same transition in a derivation and consider the two highest applications: since **PR** is invertible, we can consider, without loss of generality, that the two applications of  $\mathbf{P}R$  are consecutive, as follows:

$$\frac{\frac{(1)\Sigma; \mathbb{M}, xP_Ay; \Gamma \Rightarrow x : \mathbf{P}_A\alpha, y : \alpha, y : \alpha, \Delta}{\Sigma; \mathbb{M}, xP_Ay; \Gamma \Rightarrow x : \mathbf{P}_A\alpha, y : \alpha, \Delta} (\mathbf{P}R)}{\Sigma; \mathbb{M}, xP_Ay; \Gamma \Rightarrow x : \mathbf{P}_A\alpha, \Delta} (\mathbf{P}R)$$

From (1) we can find a derivation of  $(1')\Sigma; \mathbb{M}, xP_Ay; \Gamma \Rightarrow x : \mathbf{P}_A\alpha, y : \alpha, \Delta$  by contraction and this derivation does not have any application of **PR** having  $xP_Ay$  as a principal formula (remember that contraction is rule-preserving admissible). Thus, we can remove one application of **PR** as follows:

$$\frac{(1')\Sigma; \mathbb{M}, xP_Ay; \Gamma \Rightarrow x : \mathbf{P}_A\alpha, y : \alpha, \Delta}{\Sigma; \mathbb{M}, xP_Ay; \Gamma \Rightarrow x : \mathbf{P}_A\alpha, \Delta} (\mathbf{P}R)$$

<sup>9</sup> For any principal  $A$ .

**Lemma 13 (Controlled use of  $\chi$ ).** *It is useless to apply  $\chi$  (with  $\chi \in \{\text{mon-S, mon-R, mon-C, mon-P, sym, trans, s-I-SS, s-del-C, s-C2P, s-RS}\}$ ) on the same transition formula (or label as in  $s\text{-RS}$ ) more than once in a backward proof search in each branch of a derivation.*

*Proof.* The proof proceeds similarly to those of previous lemmas.

However, the above lemmas are not sufficient to ensure termination of the proof search. In particular, there are two issues:

1. The interaction of rule (trans) with  $\rightarrow L$  brings in new accessible worlds, we can build chains of accessible worlds on which  $\rightarrow L$  can be applied *ad infinitum*.
2. The application of rules (s-del-C) and (s-C2P) generates transition formulas that contains new labels that can be used for new applications of the same rules.

Concerning point (1), suppose we attempt to find a proof for the sequent

$$\{x\}, \emptyset, \emptyset \Rightarrow x : ((p \rightarrow q) \rightarrow r) \rightarrow \perp$$

we can build an infinite proof tree as follows<sup>10</sup>

$$\begin{array}{c} \vdots \\ \hline \{x, y, z, k\}, x \leq y, y \leq z, z \leq k, y \leq k, k : p, z : p, y : (p \rightarrow q) \rightarrow r \Rightarrow k : q, z : q, y : \perp \quad (\rightarrow L) \\ \hline \{x, y, z, k\}, x \leq y, y \leq z, z \leq k, k : p, z : p, y : (p \rightarrow q) \rightarrow r \Rightarrow k : q, z : q, y : \perp \quad \text{trans} \\ \hline \{x, y, z\}, x \leq y, y \leq z, z : p, y : (p \rightarrow q) \rightarrow r \Rightarrow z : p \rightarrow q, z : q, y : \perp \quad (\rightarrow R) \\ \hline \{x, y, z\}, x \leq y, y \leq z, z : p, y : (p \rightarrow q) \rightarrow r \Rightarrow z : q, y : \perp \quad (\rightarrow L) \\ \hline \{x, y, z\}, x \leq y, y \leq z, z : p, y : (p \rightarrow q) \rightarrow r \Rightarrow z : q, y : \perp \quad (\rightarrow R) \\ \hline \{x, y\}, x \leq y, y : (p \rightarrow q) \rightarrow r \Rightarrow y : (p \rightarrow q), y : \perp \quad (\rightarrow L) \\ \hline \{x, y\}, x \leq y, y : (p \rightarrow q) \rightarrow r \Rightarrow y : \perp \quad (\rightarrow L) \\ \hline \{x\}, \emptyset, \emptyset \Rightarrow x : ((p \rightarrow q) \rightarrow r) \rightarrow \perp \quad (\rightarrow R) \end{array}$$

This behavior can be avoided by putting a bound on the applications of  $\rightarrow R$ , in particular the following Lemma holds

**Lemma 14 (Bounded application of  $\rightarrow L$ ).** *Given a derivation starting with  $\Rightarrow x : F$ , it is useless to apply  $\rightarrow L$  on a transition formula  $x_1 \leq x_2$  such that  $d(x, x_1) > \text{depth}(F)$ .*

*Proof. (sketch)* Suppose, in the proof search of  $\Rightarrow x : F$ , to have a sequent  $\Sigma_1, \mathbb{M}_1, \Gamma_1 \Rightarrow \Delta_1$  and to apply  $\rightarrow L$  on  $(y_1 : \varphi_1 \rightarrow \varphi_2) \in \Gamma_1$  and  $y_1 \leq y_2 \in \mathbb{M}_1$  with  $d(x, y_1) > \text{depth}(F)$ . Suppose that the resulting sequent of such application is  $\Sigma_2, \mathbb{M}_2, \Gamma_2 \Rightarrow \Delta_2$ , for any  $y_1 : \varphi$  introduced by the last application of  $\rightarrow L$  we have that,

- (a)  $\varphi$  is a subformula of  $F$  and,
- (b) For all labels  $k$ , s.t.,  $d(x, k) \leq \text{depth}(F)$ , it must be possible to introduce  $k : \varphi$  by applying  $\rightarrow L$  on it.

<sup>10</sup> For compactness we only consider left branches generated by applications of  $\rightarrow L$ .

Point (a) follows from the fact that we are proving a regular sequent  $\Rightarrow x : F$  and from the definition of Logical Rules. Point (b) says that after such application of  $\rightarrow L$  all the formulas  $\varphi$  that can be associated to label  $y_1$ , can also be associated to labels that have a depth smaller or equal to  $\text{depth}(F)$ . Therefore, if a branch in the proof tree is closed with an axiom rule in which  $y_1$  is the label of the principal formula, then there must be an equivalent branch closed by an axiom rule in which some other label  $k$  with  $d(x, k) \leq \text{depth}(F)$  is principal.

Take label  $y$  such that  $d(x, y) > m\text{depth}(F)$ , for every formula  $\varphi$  such that  $y : \varphi$ , it is

Concerning point (2), due to the fact that rules (s-C2P) and (s-del-C) generate new labels they can be, in principle, applied infinitely often. For instance, (s-C2P) could be applied *ad infinitum* as follows

$$\frac{\frac{\frac{\vdots}{\Sigma, y, z, w; \mathbb{M}, xCAy, xPAy, yCAz, yPAz, zCAw, zPAw; \Gamma \Rightarrow \Delta} \text{(s-C2P)}}{\Sigma, y, z; \mathbb{M}, xCAy, xPAy, yCAz, yPAz; \Gamma \Rightarrow \Delta} \text{(s-C2P)}}{\Sigma, y; \mathbb{M}, xCAy, xPAy; \Gamma \Rightarrow \Delta} \text{(s-C2P)}}{\Sigma; \mathbb{M}; \Gamma \Rightarrow \Delta} \text{(s-C2P)}$$

A similar case can be shown for s-del-C. This behavior can be avoided by putting a bound on the application of rules s-C2P, s-del-C, as the following Lemmas show.

**Lemma 15 (Bounded application of s-C2P).** *Given a derivation starting with  $\Rightarrow x : F$ , it is useless to apply s-C2P on a label  $x_1$  such that  $d(x, x_1) > \text{depth}(F)$ .*

*Proof.* The argument proceeds similarly to proof of Lemma 14. Intuitively, if a sequent is provable, then there must be a proof in which s-C2P is never applied to a label  $k$  such that  $d(x, k) > \text{depth}(F)$ .

**Lemma 16 (Bounded application of s-del-C).** *Given a derivation starting with  $\Rightarrow x : F$ , it is useless to apply s-del-C on a transition formula  $x_1 C_B x_2$  such that  $d(x, x_1) > \text{depth}(F)$ .*

*Proof.* The argument proceeds similarly to proof of Lemma 14.