2012 IEEE 25th Computer Security Foundations Symposium

Labeled Sequent Calculi for Access Control Logics: Countermodels, Saturation and Abduction

Valerio Genovese*, Deepak Garg†, Daniele Rispoli‡
*University of Luxembourg and University of Torino, Italy
Email: genovese@di.unito.it
†Max Planck Institute for Software Systems, Germany
Email: dg@mpi-sws.org
‡University of Torino, Italy
Email: daniele.rispoli@gmail.com

***Abstract*—We show that Kripke semantics of modal logic, manifest in the syntactic proof formalism of labeled sequent calculi, can be used to solve three central problems in access control: Generating evidence for denial of access (countermodel generation), finding all consequences of a policy (saturation) and determining which additional credentials will allow an access (abduction). At the core of our work is a single, non-trivial, countermodel producing decision procedure for a specific access control logic. The procedure is based on backwards search in a labeled sequent calculus for the logic. Modifications of the calculus yield a procedure for abduction and, surprisingly, for saturation.**

I. Introduction

The role of formal logic in the context of access control is now well-established. Logic has been used to model and reason about access policies starting with the work of Abadi et al. [2]; proof theory has been used to enforce access policies in architectures like proof-carrying authorization [3, 6, 7, 17, 24, 27], and to prove meta-properties of policies [16]; logic programming, both top-down and bottom-up, has been used to efficiently determine consequences of policies [9, 13, 23] and as the basis of privacy analysis of policies [8]; logical abduction has been used to determine credentials needed to authorize a specific access [10]; and, logics embedded in type systems have been used to statically enforce access policies in programming language interfaces [4, 20, 26]. In fact, logic has been so widely used in access control that several specialized logics, called *access control logics*, have been proposed exclusively for representing and reasoning about access policies. Technically, all access control logics are modal logics, containing at least one principal indexed modality A says φ (principal A supports the truth of formula φ), used to represent authenticated statements made by individuals participating in the access control process.

The primary focus of study in the area of access control logics in the past decade has been *proof theory* (symbolic proofs); semantics, when studied, have been second-rate citizens because it is unclear what role they could play in practice. Unlike other applications of logic, where real-world situations correspond to a logic's *models* and the semantics connect logical formulas to their interpretations in the real world, there are no known interesting connections between models of access control logics (which are specializations of the standard Kripke models of modal logic) and actual access control systems.

In this paper we argue that despite the fact that Kripke semantics of access control logics are not useful to formalize real-world access control systems, such semantics *are* useful to solve the following relevant problems in the use of access control logics:

- *Countermodel generation*: Producing evidence of why an access is denied, or why it does not follow from a given policy. (Existence of a sound countermodel producing procedure also implies decidability.)
- *Saturation* or finding all consequences of an access policy.
- *Abduction* or determining which additional credentials suffice to authorize an access.

All three problems are important for enforcement of access policies. Countermodels enable a reference monitor to justify to a principal why it has been denied access: If a policy represented as a formula P does not entail an authorization represented as formula φ, then the reference monitor can provide a countermodel for $P \to \varphi$, thus justifying the denial of authorization φ. Saturation is necessary to pre-compile policies and to cache their consequences. Abduction is useful for finding missing credentials and for justifying authorizations on-the-fly, as in the Grey system [7].

The main contribution of this paper is in showing that all the above problems can be solved using the single foundational formalism of *labeled sequent calculi*, which are symbolic proof systems that directly mimic Kripke semantics of the logic in the inference rules [5]. Working with a specific access control logic, a propositional variant of the logic BL [17], we show how its labeled sequent calculus can be used to obtain an easily implementable decision procedure which produces countermodels when no proof exists, how the generated countermodels can be used to find all consequences of a policy, and how the labeled sequent calculus can be adapted to find additional credentials that suffice to authorize a given access. Throughout the paper, we combine ideas from

DOI 10.1109/CSF.2012.11

Kripke semantics with those from proof theory.

It is well known that proving decidability of multi-modal logics like ours is a challenging problem due to interactions between modalities, which can cause decision procedures to loop (see [21] for examples). Producing countermodels is even harder. Our technical work is complicated further by our decision to use an intuitionistic logic instead of a classical logic. We make this choice because intuitionistic logics are known to be a better fit for modeling access policies than classical logics. However, the choice requires us to introduce and handle an additional preorder to model implication in the Kripke semantics, thus creating another source of interaction in all our algorithms. Our eventual underlying decision procedure is an extension of our prior, general result for modal logics [15]. The extension is non-trivial because our logic BL_{sf} includes the connective A sf B (principal A speaks for principal B) that stipulates relations between accessibility relations in Kripke models. The connective is used to represent unrestricted delegation in access control [2].

Saturation of access control policies to derive all consequences is a well-studied technique used in many policy engines like SecPAL [9]. Unlike the conventional, syntactic approach of using forward chaining to find the consequence-set of a policy, our approach uses a completely novel, and somewhat surprising technique based on sets of countermodels obtained from labeled sequent calculi. Abduction for access control policies written in a small fragment of finite domain, first-order logic, Datalog, has been studied by Becker et al. [10]. Although we do not consider quantifiers directly in this paper, our abduction result is more general because quantifiers over finite domains can be trivially eliminated and we work with an entire logic, not a fragment.

Organization: In Section II we introduce the logic we use, BL_{sf}. After an informal description of the logic, we present the foundations of our work: the Kripke semantics (Section II-A) and the labeled sequent calculus (Section II-B). In Section III, we present our countermodel producing decision procedure, which also forms the basis of saturation and abduction, which are presented in Sections IV and V, respectively. Section VI discusses related work and Section VII concludes the paper with some directions for future work. Proofs of theorems are presented in the appendix. To keep the presentation concise, straightforward inference rules are deferred to an accompanying technical report (TR in the sequel) [19].

II. BL_{sf}: The Access Control Logic

BL_{sf} is propositional intuitionistic logic extended with two connectives, commonly used to model access policies: A says φ (principal A supports formula φ) and A sf B (principal A speaks for principal B)[1]. The syntax of BL_{sf} formulas is shown below. p denotes an atomic formula, drawn from a countable set of symbols, and A, B denote principals drawn from a different, finite set $\mathcal{I}$. The connectives $\top$ (true), $\bot$ (false), $\wedge$ (and), $\vee$ (or) and $\rightarrow$ (implication) have usual meanings.

[1]In existing literature, A sf B is often written $A \Rightarrow B$. We prefer the notation A sf B to prevent confusion with logical implication.

$$\text{Formulas} \quad \varphi, \psi \quad ::= \quad p \mid \top \mid \bot \mid \varphi_1 \wedge \varphi_2 \mid \varphi_1 \vee \varphi_2 \mid \varphi_1 \rightarrow \varphi_2 \mid A \text{ says } \varphi \mid A \text{ sf } B$$

(We do not include first-order quantifiers, but those ranging over a finite domain I of individuals can be defined in the usual way: $\forall x{\in}I.\,\varphi \equiv \bigwedge_{i \in I} \varphi[i/x]$ and $\exists x{\in}I.\,\varphi \equiv \bigvee_{i \in I} \varphi[i/x]$.)

Although we formally define the semantics of BL_{sf} in Section II-A, we present here some admissible axioms with their common names from literature.

$$\frac{\text{(All intuitionistic propositional tautologies)}\quad \vdash \varphi}{\vdash A \text{ says } \varphi} \quad \text{(nec)}$$

$$\vdash (A \text{ says } (\varphi \rightarrow \psi)) \rightarrow ((A \text{ says } \varphi) \rightarrow (A \text{ says } \psi)) \quad \text{(K)}$$

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

$$\vdash (A \text{ sf } B) \rightarrow ((A \text{ says } \varphi) \rightarrow (B \text{ says } \varphi)) \quad \text{(speaksfor)}$$

$$\vdash A \text{ sf } A$$

$$\vdash (A \text{ sf } B) \rightarrow ((B \text{ sf } C) \rightarrow (A \text{ sf } C))$$

Rule (nec) and axiom (K) are standard in modal logic; they are needed to treat A says φ as a normal necessitation modality (with index A). Axiom (I) has been argued by Abadi [1] as one of the weakest axioms needed to correctly model delegation in logic using A says φ. Axiom (speaksfor) characterizes the formula A sf B: If A sf B, then any statement φ that A makes is echoed by B, so the formula A sf B means that A has authority to speak on behalf of B [2].

Example 1. We illustrate our logic using an example from prior work [14]. Consider a simple policy containing the following 3 formulas. Here, file1 is a file, `deletefile1` means that file1 should be deleted and `admin`, `Alice` and `Bob` are principals.

1) (`admin` says `deletefile1`) $\rightarrow$ `deletefile1`
2) `admin` says ((`Bob` says `deletefile1`) $\rightarrow$ `deletefile1`)
3) `Alice` sf `Bob`

The first formula means that if `admin` says that file1 should be deleted, then this should be the case. The second formula says that `admin` trusts `Bob` to decide that file1 should be deleted. The third formula means that `Alice` is trusted to make statements on `Bob`'s behalf. If P is the set of formulas 1–3, then from P and the assumption `Alice` says `deletefile1`, we can derive `deletefile1` in BL_{sf}, as may also be expected intuitively.

A. Kripke Semantics

The meaning of BL_{sf}'s connectives are formally defined through semantics written in the style of Kripke, which is standard for modal logics [12]. In the Kripke style, a model of the logic contains several points called worlds, which represent possible states of knowledge. To interpret modalities, binary accessibility relations on worlds are stipulated, with one relation S_A for every modality (A says $\cdot$). Intuitively, if wS_Aw' then principal A believes that world w' is a potential (knowledge) successor of the world w. Intuitionistic implication is modeled using a binary preorder, $\leq$.

We treat the formula A sf B as an atom in the Kripke semantics and validate axioms related to it, e.g., (speaksfor), through conditions on Kripke frames. This interpretation is very distinct from earlier interpretations of A sf B, e.g., [2, 14], that define A sf B in terms of relations between accessibility relations S_A and S_B.

Definition 2 (Kripke model)**.** A Kripke model or, simply, model, $\mathcal{M}$ is a tuple $(W, \leq, \{S_A\}_{A\in\mathcal{I}}, h, sf)$ where,

- W is a set. Its elements are called worlds.
- $\leq$ is a preorder on W.
- For each principal A, S_A is a binary relation on W, called the accessibility relation of principal A.
- h, called the truth assignment or assignment, is a map from the set of atoms to $\mathcal{P}(W)$. Informally, for any atom p, $h(p)$ is the set of worlds where p holds.
- sf is a map from pairs of principals to $\mathcal{P}(W)$. Informally, for any two principals A and B, $sf(A, B)$ is the set of worlds where A sf B holds.

Let $S_* = \bigcup_{A\in\mathcal{I}} S_A$. We require that in any model, the following properties hold.

- $\forall x.(x \leq x)$ (refl)
- $\forall x, y, z.(((x \leq y) \wedge (y \leq z)) \rightarrow (x \leq z))$ (trans)
- $\forall x, y, z.(((x \leq y) \wedge (yS_Az)) \rightarrow (xS_Az))$ (mon-S)
- $\forall x, y, z.(((xS_By) \wedge (yS_Az)) \rightarrow (xS_Az))$ (I)
- If $w \in sf(A, B)$, then for all w', wS_Bw' implies wS_Aw'. (basic-sf)
- For all A and w, $w \in sf(A, A)$. (refl-sf)
- If $w \in sf(A, B) \cap sf(B, C)$, then $w \in sf(A, C)$. (trans-sf)
- If $x \in h(p)$ and $x \leq y$, then $y \in h(p)$. (mon)
- If $x(\leq \cup S_*)^* y$ and $x \in sf(A, B)$, then $y \in sf(A, B)$. (mon-sf)

Properties (refl) and (trans) make $\leq$ a preorder. Property (mon-S) validates axiom (K). Other properties corresponding to axiom (K) have also been proposed in literature [25, 28]; our property (mon-S) is a slight simplification of a similar property used by Wolter et al. [28]. Property (I) corresponds to axiom (I). Property (basic-sf) corresponds to axiom (speaksfor). Properties (refl-sf) and (trans-sf) make A sf B reflexive and transitive, respectively. Property (mon) is standard in Kripke models of intuitionistic logics and forces monotonicity of satisfaction (Lemma 5 below). Property (mon-sf) implies that if A sf B holds in a world, then it also holds in all future worlds.

A model without the assignments h and sf, i.e., the tuple $(W, \leq, \{S_A\}_{A\in\mathcal{I}})$ is also called a *frame* and the conditions (refl)–(I) on relations above are called *frame conditions*.

Definition 3 (Satisfaction)**.** Given a model $\mathcal{M} = (W, \leq, \{S_A\}_{A\in\mathcal{I}}, h, sf)$ and a world $w \in W$, we define the satisfaction relation $\mathcal{M} \models w : \alpha$, read "the world w satisfies formula α in model $\mathcal{M}$", by induction on α as follows:

- $\mathcal{M} \models w : p$ iff $w \in h(p)$
- $\mathcal{M} \models w : \top$ (unconditionally)
- $\mathcal{M} \models w : \alpha \wedge \beta$ iff $\mathcal{M} \models w : \alpha$ and $\mathcal{M} \models w : \beta$
- $\mathcal{M} \models w : \alpha \vee \beta$ iff $\mathcal{M} \models w : \alpha$ or $\mathcal{M} \models w : \beta$
- $\mathcal{M} \models w : \alpha \rightarrow \beta$ iff for every w' such that $w \leq w'$ and $\mathcal{M} \models w' : \alpha$, we have $\mathcal{M} \models w' : \beta$.
- $\mathcal{M} \models w : A$ says α iff for every w' such that wS_Aw', we have $\mathcal{M} \models w' : \alpha$.
- $\mathcal{M} \models w : A$ sf B iff $w \in sf(A, B)$.

We say that $\mathcal{M} \not\models w : \alpha$ if it is not the case that $\mathcal{M} \models w : \alpha$. In particular, for every $\mathcal{M}$ and every w, $\mathcal{M} \not\models w : \bot$.

A formula α is true in a model $\mathcal{M}$, written $\mathcal{M} \models \alpha$, if for every world $w \in \mathcal{M}$, $\mathcal{M} \models w : \alpha$. A formula α is *valid* in BL_{sf}, written $\models \alpha$, if $\mathcal{M} \models \alpha$ for every model $\mathcal{M}$.

Example 4. It is easily checked that every axiom presented in Section II is valid in BL_{sf} in the sense of the definition above.

The following is a fundamental property of the Kripke semantics of all intuitionistic modal logics, needed to prove soundness of sequent calculi (Theorem 7).

Lemma 5 (Monotonicity)**.** *If $\mathcal{M} \models w : \alpha$ and $w \leq w' \in \mathcal{M}$, then $\mathcal{M} \models w' : \alpha$.*

Proof: By induction on α. ∎

B. SeqC*: A Labeled Sequent Calculus*

Next, we introduce a labeled sequent calculus for BL_{sf}, which, although a syntactic proof system, derives its inference rules directly from the inductive definition of satisfaction in the Kripke semantics. This labeled sequent calculus, called SeqC, forms the basis of all the remaining work in this paper. Conclusions in SeqC have the form: "Formula φ is true in world w", where w is a symbolic world. Hypotheses are assumptions of the same form, as well as symbolic relations between the worlds. Formally, we introduce a syntactic category of labeled formulas, written $w : \varphi$, to mean that formula φ is true in world w. A sequent in our calculus has the form $\Sigma; \mathbb{M}; \Gamma \Rightarrow \Delta$, where

- Σ is a finite set of world symbols appearing in the rest of the sequent. World symbols are also called *labels*.
- $\mathbb{M}$ is a finite set of relations between labels in Σ. Relations have the forms $x \leq y$ and xS_Ay.
- Γ is a finite set of labeled formulas.
- Δ is a finite set of labeled formulas.

Semantically, $\Sigma; \mathbb{M}; \Gamma \Rightarrow \Delta$ is valid when every model with a world set containing at least Σ, satisfying all relations in $\mathbb{M}$ and all labeled formulas in Γ also satisfies at least one labeled formula in Δ.

Definition 6 (Sequent satisfaction and validity)**.** A model $\mathcal{M}$ and a mapping ρ from elements of Σ to worlds of $\mathcal{M}$ satisfy a (possibly non-provable) sequent $\Sigma; \mathbb{M}; \Gamma \Rightarrow \Delta$, written $\mathcal{M}, \rho \models (\Sigma; \mathbb{M}; \Gamma \Rightarrow \Delta)$, if one of the following holds:

- There is an $xRy \in \mathbb{M}$ with $R \in \{\leq\} \cup \{S_A \mid A \in \mathcal{I}\}$ such that $\rho(x)\ R\ \rho(y) \notin \mathcal{M}$.
- There is an $x : \alpha \in \Gamma$ such that $\mathcal{M} \not\models \rho(x) : \alpha$.
- There is an $x : \alpha \in \Delta$ such that $\mathcal{M} \models \rho(x) : \alpha$.

A model $\mathcal{M}$ satisfies a sequent $\Sigma; \mathbb{M}; \Gamma \Rightarrow \Delta$, written $\mathcal{M} \models (\Sigma; \mathbb{M}; \Gamma \Rightarrow \Delta)$, if for every mapping ρ, we have $\mathcal{M}, \rho \models$

$(\Sigma; \mathbb{M}; \Gamma \Rightarrow \Delta)$. Finally, a sequent $\Sigma; \mathbb{M}; \Gamma \Rightarrow \Delta$ is valid, written $\models (\Sigma; \mathbb{M}; \Gamma \Rightarrow \Delta)$ if for every model $\mathcal{M}$, we have $\mathcal{M} \models (\Sigma; \mathbb{M}; \Gamma \Rightarrow \Delta)$.

Rules of SeqC*:* Selected rules of the labeled sequent calculus for BL_{sf} are shown in Figure 1. (For the remaining rules, see our TR.) Rules for each connective mimic the (Kripke) semantic definition of the connective. For example, in the rule ($\wedge$R), to prove $x : \alpha \wedge \beta$ in the conclusion, we prove $x : \alpha$ and $x : \beta$ in the premises. The conditions (refl)–(mon-sf) in the definition of Kripke models (Definition 2), with the exception of (mon), are modeled by the frame rules in Figure 1. Condition (mon) is implicit in the rule (init). In the rules ($\rightarrow$R) and (saysR), the world y in the premise is fresh. We say that $\vdash (\Sigma; \mathbb{M}; \Gamma \Rightarrow \Delta)$ if $\Sigma; \mathbb{M}; \Gamma \Rightarrow \Delta$ has a proof in the calculus. The sequent calculus is both sound and complete with respect to the semantics.

Theorem 7 (Soundness)**.** *If* $\vdash (\Sigma; \mathbb{M}; \Gamma \Rightarrow \Delta)$*, then* $\models (\Sigma; \mathbb{M}; \Gamma \Rightarrow \Delta)$.

Proof: Fix an $\mathcal{M}$. It is easily proved by induction on the given derivation of $\Sigma; \mathbb{M}; \Gamma \Rightarrow \Delta$ that for every mapping ρ, $\mathcal{M}, \rho \models (\Sigma; \mathbb{M}; \Gamma \Rightarrow \Delta)$. ■

The converse of Theorem 7, completeness, also holds but we do not prove the result here because it is a consequence of the correctness of our countermodel producing decision procedure. The following theorem is central to the proof of termination of our decision procedure.

Theorem 8 (Weak subformula property)**.** *If a formula* φ *appears in any proof tree (possibly infinite) obtained by applying the rules of Figure 1 backwards starting from a concluding sequent* $\Sigma; \mathbb{M}; \Gamma \Rightarrow \Delta$*, then either* φ *has the form* A sf B *where* $A, B \in \mathcal{I}$*, or* φ *is a subformula of some formula in either* Γ *or* Δ.

Proof: By induction on the distance (in the proof tree) of the occurrence of φ from the conclusion $\Sigma; \mathbb{M}; \Gamma \Rightarrow \Delta$. ■

III. Decidability and Countermodel Generation

Our first application of the labeled sequent calculus SeqC is a decision procedure that provides countermodels if a sequent has no proof. Production of countermodels is of practical use in access control because a countermodel can be used as evidence to justify denial of authorization. Note that backwards search in SeqC does not directly yield a decision procedure because the rules ($\rightarrow$R) and (saysR) can be applied indefinitely to produce new worlds. The countermodel producing decision procedure presented here bounds the backwards application of these rules and is based on our prior general result for multi-modal logics [15], which in turn generalizes earlier work on uni-modal tableaux calculi [18]. In the following we present the decision procedure briefly and extend it with the connective A sf B. Readers not interested in understanding how the procedure works may directly skip to Section III-B, which lists the decision procedure as a sequent calculus.

The key idea of our technique is to prevent infinite application of the rules ($\rightarrow$R) and (saysR) in backward search by checking for containment of formulas labeling a world in those labeling another. In its naive form, this check results in incompleteness because of the condition (I) and the connective A sf B. To recover completeness, we check containment not between sets of formulas labeling two worlds, but between the sets obtained by applying a suitably chosen function, called Sfor, on those sets. The selection of an appropriate definition for Sfor is the central idea of our decision procedure. Using this function, we define a sub-class of sequents called *saturated histories*, on which backwards application of any of the rules of Figure 1 is certainly useless. We then use this notion of "uselessness of backwards rule application" to build a decision procedure and use a counting argument based on the weak subformula property (Theorem 8) to show that it terminates. We further show how to extract a countermodel from a saturated history, thus forming the basis of our countermodel extraction.

In the following, we describe the decision procedure, starting with the definition of Sfor and saturated history in Section III-A, followed by the decision procedure itself in Section III-B.

A. Saturated Histories

We use the term *history* for a tuple $\Sigma; \mathbb{M}; \Gamma; \Delta$ or, equivalently, for a sequent $\Sigma; \mathbb{M}; \Gamma \Rightarrow \Delta$. Let $T(\varphi)$ and $F(\varphi)$ be two uninterpreted unary relations. Informally, we read $T(\varphi)$ as "φ should be true" and $F(\varphi)$ as "φ should be false". Given a history $\Sigma; \mathbb{M}; \Gamma; \Delta$ and $x \in \Sigma$, the *signed formulas* of x, written $\text{Sfor}(\Sigma; \mathbb{M}; \Gamma; \Delta, x)$ are defined as follows:

$$\begin{gathered}\text{Sfor}(\Sigma; \mathbb{M}; \Gamma; \Delta, x) = \\ \{T(\varphi) \mid x : \varphi \in \Gamma\} \cup \\ \{F(\varphi) \mid x : \varphi \in \Delta\} \cup \\ \{T(A \text{ says } \varphi) \mid \exists y.\ y (\leq \cup S_*)^* x \in \mathbb{M} \wedge y : A \text{ says } \varphi \in \Gamma\} \cup \\ \{T(\varphi \rightarrow \psi) \mid \exists y.\ y \leq x \in \mathbb{M} \wedge y : \varphi \rightarrow \psi \in \Gamma\} \cup \\ \{T(p) \mid \exists y.\ y \leq x \in \mathbb{M} \wedge y : p \in \Gamma\}\end{gathered}$$

The key component in the definition of Sfor is the third one, which must align with the choice of axioms for the modality A says $\cdot$. Here, the choice corresponds to the axiom (I). When $\Sigma, \mathbb{M}, \Gamma, \Delta$ are clear from context, we abbreviate $\text{Sfor}(\Sigma; \mathbb{M}; \Gamma; \Delta, x)$ to $\text{Sfor}(x)$. We say that $x \preccurlyeq y$ iff $\text{Sfor}(x) \subseteq \text{Sfor}(y)$.

We call a pair $\mathbb{M}; \Gamma$ *closed* if they are closed under backward application of the frame rules of Figure 1. (Note that the frame rules of Figure 1 only add elements to $\mathbb{M}$ and Γ.) We write $\overline{\mathbb{M}; \Gamma}$ for the closure of $\mathbb{M}; \Gamma$ by the frame rules.

We call a frame $\mathbb{M}$ *tree-like* if it can be derived from a finite tree of the relations $\leq$ and S_A and (possibly partial) closure by frame rules. This tree is called the underlying tree of $\mathbb{M}$ and we say that $x \ll y$ (in $\mathbb{M}$) iff there is a directed path from x to y in the tree underlying $\mathbb{M}$.

The key definition in our method is that of a *saturated history*. Intuitively, this definition characterizes those histories $\Sigma; \mathbb{M}; \Gamma; \Delta$ for which we can directly define a countermodel for the sequent $\Sigma; \mathbb{M}; \Gamma \Rightarrow \Delta$. (The definition of this countermodel is given soon after the definition of a saturated history.)

Axiom Rules

$$\frac{}{\Sigma; \mathbb{M}, x \leq y; \Gamma, x : p \Rightarrow y : p, \Delta}\,\text{init} \qquad \frac{}{\Sigma; \mathbb{M}; \Gamma, x : A \;\mathsf{sf}\; B \Rightarrow x : A \;\mathsf{sf}\; B, \Delta}\,\text{sf}$$

Logical Rules

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

$$\frac{\Sigma; \mathbb{M}, x \leq y; \Gamma, x : \alpha \to \beta \Rightarrow y : \alpha, \Delta \qquad \Sigma; \mathbb{M}, x \leq y; \Gamma, x : \alpha \to \beta, y : \beta \Rightarrow \Delta}{\Sigma; \mathbb{M}, x \leq y; \Gamma, x : \alpha \to \beta \Rightarrow \Delta}\,\to\text{L}$$

$$\frac{\Sigma, y; \mathbb{M}, xS_A y; \Gamma \Rightarrow y : \alpha, x : A \;\mathsf{says}\; \alpha, \Delta}{\Sigma; \mathbb{M}; \Gamma \Rightarrow x : A \;\mathsf{says}\; \alpha, \Delta}\,\text{saysR} \qquad \frac{\Sigma; \mathbb{M}, xS_A y; \Gamma, x : A \;\mathsf{says}\; \alpha, y : \alpha \Rightarrow \Delta}{\Sigma; \mathbb{M}, xS_A y; \Gamma, x : A \;\mathsf{says}\; \alpha \Rightarrow \Delta}\,\text{saysL}$$

Frame Rules

$$\frac{\Sigma, x; \mathbb{M}, x \leq x; \Gamma \Rightarrow \Delta}{\Sigma, x; \mathbb{M}; \Gamma \Rightarrow \Delta}\,\text{refl} \qquad \frac{\Sigma; \mathbb{M}, x \leq y, y \leq z, x \leq z; \Gamma \Rightarrow \Delta}{\Sigma; \mathbb{M}, x \leq y, y \leq z; \Gamma \Rightarrow \Delta}\,\text{trans} \qquad \frac{\Sigma; \mathbb{M}, x \leq y, yS_A z, xS_A z; \Gamma \Rightarrow \Delta}{\Sigma; \mathbb{M}, x \leq y, yS_A z; \Gamma \Rightarrow \Delta}\,\text{mon-S}$$

$$\frac{\Sigma; \mathbb{M}, xS_B y, yS_A z, xS_A z; \Gamma \Rightarrow \Delta}{\Sigma; \mathbb{M}, xS_B y, yS_A z; \Gamma \Rightarrow \Delta}\,\text{I} \qquad \frac{\Sigma; \mathbb{M}, xS_B y, xS_A y; \Gamma, x : A \;\mathsf{sf}\; B \Rightarrow \Delta}{\Sigma; \mathbb{M}, xS_B y; \Gamma, x : A \;\mathsf{sf}\; B \Rightarrow \Delta}\,\text{basic-sf} \qquad \frac{\Sigma, x; \mathbb{M}; \Gamma, x : A \;\mathsf{sf}\; A \Rightarrow \Delta}{\Sigma, x; \mathbb{M}; \Gamma \Rightarrow \Delta}\,\text{refl-sf}$$

$$\frac{\Sigma; \mathbb{M}; \Gamma, x : A \;\mathsf{sf}\; B, x : B \;\mathsf{sf}\; C, x : A \;\mathsf{sf}\; C \Rightarrow \Delta}{\Sigma; \mathbb{M}; \Gamma, x : A \;\mathsf{sf}\; B, x : B \;\mathsf{sf}\; C \Rightarrow \Delta}\,\text{trans-sf} \qquad \frac{\Sigma; \mathbb{M}, x \leq y; \Gamma, x : A \;\mathsf{sf}\; B, y : A \;\mathsf{sf}\; B \Rightarrow \Delta}{\Sigma; \mathbb{M}, x \leq y; \Gamma, x : A \;\mathsf{sf}\; B \Rightarrow \Delta}\,\text{mon1-sf}$$

$$\frac{\Sigma; \mathbb{M}, xS_C y; \Gamma, x : A \;\mathsf{sf}\; B, y : A \;\mathsf{sf}\; B \Rightarrow \Delta}{\Sigma; \mathbb{M}, xS_C y; \Gamma, x : A \;\mathsf{sf}\; B \Rightarrow \Delta}\,\text{mon2-sf}$$

Fig. 1. SeqC: A labeled sequent calculus for $\mathrm{BL}_{\mathrm{sf}}$, selected rules

Definition 9 (Saturated history)**.** A history $\Sigma; \mathbb{M}; \Gamma; \Delta$ is called saturated if the following hold:

1) $\mathbb{M}$ is tree-like and $\mathbb{M}; \Gamma$ is closed. (In particular, because $\mathbb{M}$ is tree-like, it has a relation $\ll$ defined on it.)
2) If $x : p \in \Gamma$, then there is no y such that $x \leq y \in \mathbb{M}$ and $y : p \in \Delta$.
3) There is no x such that $x : \top \in \Delta$.
4) There is no x such that $x : \bot \in \Gamma$.
5) If $x : \alpha \wedge \beta \in \Gamma$, then $x : \alpha \in \Gamma$ and $x : \beta \in \Gamma$.
6) If $x : \alpha \wedge \beta \in \Delta$, then either $x : \alpha \in \Delta$ or $x : \beta \in \Delta$.
7) If $x : \alpha \vee \beta \in \Gamma$, then either $x : \alpha \in \Gamma$ or $x : \beta \in \Gamma$.
8) If $x : \alpha \vee \beta \in \Delta$, then $x : \alpha \in \Delta$ and $x : \beta \in \Delta$.
9) If $x : \alpha \to \beta \in \Gamma$ and $x \leq y \in \mathbb{M}$, then either $y : \alpha \in \Delta$ or $y : \beta \in \Gamma$.
10) If $x : \alpha \to \beta \in \Delta$, then either:
    a) There is a y such that $x \leq y \in \mathbb{M}$, $y : \alpha \in \Gamma$ and $y : \beta \in \Delta$ or
    b) There is a y such that $y \neq x$, $y \ll x$ and $x \preccurlyeq y$.
11) If $x : A \;\mathsf{says}\; \alpha \in \Gamma$ and $xS_A y \in \mathbb{M}$, then $y : \alpha \in \Gamma$.
12) If $x : A \;\mathsf{says}\; \alpha \in \Delta$, then either:
    a) There is a y such that $xS_A y \in \mathbb{M}$ and $y : \alpha \in \Delta$ or
    b) There is a y such that $y \neq x$, $y \ll x$ and $x \preccurlyeq y$.
13) There are no x, A, B such that $x : A \;\mathsf{sf}\; B \in \Gamma$ and $x : A \;\mathsf{sf}\; B \in \Delta$.

Definition 10 (Countermodel of a saturated history)**.** For a saturated history $\Sigma; \mathbb{M}; \Gamma; \Delta$, the *countermodel* of the history, $\mathbf{CM}(\Sigma; \mathbb{M}; \Gamma; \Delta)$ is defined as follows. Let $C = \{x \leq y \mid x \preccurlyeq y\}$ and let $\mathbb{M}'; \Gamma' = \overline{(\mathbb{M} \cup C); \Gamma}$.

- The worlds of $\mathbf{CM}(\Sigma; \mathbb{M}; \Gamma; \Delta)$ are those in Σ.
- The relations of $\mathbf{CM}(\Sigma; \mathbb{M}; \Gamma; \Delta)$ are those in $\mathbb{M}'$.
- $h(p) = \{x \mid \exists y.\ (y \leq x \in \mathbb{M}) \wedge (y : p \in \Gamma)\}$.
- $sf(A, B) = \{x \mid x : A \;\mathsf{sf}\; B \in \Gamma\}$.

It is not obvious that $\mathbf{CM}(\Sigma; \mathbb{M}; \Gamma; \Delta)$ is a model, because it may not satisfy the monotonicity condition, (mon), for h. It trivially satisfies all other conditions in the definition of a model. Lemma 11 states that the monotonicity condition (mon) must also always hold for $\mathbf{CM}(\Sigma; \mathbb{M}; \Gamma; \Delta)$.

Lemma 11. *If $\Sigma; \mathbb{M}; \Gamma; \Delta$ is a saturated history, then $\mathbf{CM}(\Sigma; \mathbb{M}; \Gamma; \Delta)$ has a monotonic valuation h, i.e., $x \in h(p)$ and $x \leq y \in \mathbf{CM}(\Sigma; \mathbb{M}; \Gamma; \Delta)$ imply $y \in h(p)$.*

Proof: See Appendix A, Lemma 23. ∎

The next Lemma states the central property of our method. In particular, the Lemma immediately implies that if $\Sigma; \mathbb{M}; \Gamma; \Delta$ is a saturated history, then $\mathbf{CM}(\Sigma; \mathbb{M}; \Gamma; \Delta)$ is a

countermodel to the sequent $\Sigma; \mathbb{M}; \Gamma \Rightarrow \Delta$.

Lemma 12. *The following hold for any saturated history* $\Sigma; \mathbb{M}; \Gamma; \Delta$*:*

A. *If* $T(\varphi) \in$ *Sfor*$(\Sigma; \mathbb{M}; \Gamma; \Delta, x)$*, then* *CM*$(\Sigma; \mathbb{M}; \Gamma; \Delta) \models x : \varphi$
B. *If* $F(\varphi) \in$ *Sfor*$(\Sigma; \mathbb{M}; \Gamma; \Delta, x)$*, then* *CM*$(\Sigma; \mathbb{M}; \Gamma; \Delta) \not\models x : \varphi$

Proof: See Appendix A, Lemma 24. ∎

Corollary 13 (Existence of countermodel)**.** *If* $\Sigma; \mathbb{M}; \Gamma; \Delta$ *is a saturated history, then* *CM*$(\Sigma; \mathbb{M}; \Gamma; \Delta) \not\models (\Sigma; \mathbb{M}; \Gamma \Rightarrow \Delta)$.

Proof: Lemma 12 immediately implies that $\text{CM}(\Sigma; \mathbb{M}; \Gamma; \Delta), \rho \not\models (\Sigma; \mathbb{M}; \Gamma \Rightarrow \Delta)$, where $\rho : \Sigma \to \Sigma$ is the identity substitution. ∎

B. SeqC_T*: Countermodel Producing Decision Procedure*

We synthesize a countermodel producing decision procedure for BL_sf using the idea of saturated histories and the definition of the countermodel $\text{CM}(\Sigma; \mathbb{M}; \Gamma; \Delta)$. We present the decision procedure as a sequent calculus, SeqC_T, with judgments of the form $\Sigma; \mathbb{M}; \Gamma \Rightarrow_\text{T} \Delta \searrow S$, where S is a possibly empty, finite set of (counter)models. Reading the rules backwards, the calculus is an algorithm with inputs Σ, $\mathbb{M}$, Γ and Δ and output S. The correctness properties of the algorithm are that: (1) Given any Σ, $\mathbb{M}$, Γ and Δ with tree-like $\mathbb{M}$, the algorithm terminates and produces some S. (2) If $S = \{\}$, then $\Sigma; \mathbb{M}; \Gamma \Rightarrow \Delta$ has a proof in SeqC and if $S \neq \{\}$, then every model $\mathcal{M} \in S$ satisfies $\mathcal{M} \not\models (\Sigma; \mathbb{M}; \Gamma \Rightarrow \Delta)$. The requirement that $\mathbb{M}$ be tree-like is needed to complete the proofs. In practice, we start from an empty $\mathbb{M}$, which is trivially tree-like.

Selected rules of the calculus SeqC_T are shown in Figure 2. With the exception of the new rule (CM), each rule in the calculus corresponds to a rule of the same name in SeqC (Figure 1). The difference between the calculi is that there are additional conditions on each rule in SeqC_T, which are written in boxes in the figure. These are called *applicability conditions*. There are two key points to observe here. First, by design, if the applicability conditions of all rules in the figure fail, i.e., no rule (except CM) applies, then the tuple $\Sigma; \mathbb{M}; \Gamma; \Delta$ in the conclusion of the rule is a saturated history. Therefore, by Corollary 13, $\Sigma; \mathbb{M}; \Gamma \Rightarrow \Delta$ has a countermodel, which is output into S using the rule (CM). Second, all rules of the calculus except (CM) simply aggregate the countermodels from their premises into a single set in the conclusion. This is sound because all rules of the Figure 1 are invertible, so any countermodel of any of the premises is necessarily a countermodel of the conclusion. The following lemmas and theorems state termination and partial correctness of SeqC_T.

Theorem 14 (Termination)**.** *The following hold:*

1) *Any backwards derivation in* SeqC_T *starting from a sequent* $\Sigma; \mathbb{M}; \Gamma \Rightarrow_T \Delta$ *with* $\mathbb{M}$ *tree-like terminates.*
2) *For any* $\Sigma; \mathbb{M}; \Gamma; \Delta$ *with* $\mathbb{M}$ *tree-like, there is an* S *such that* $\vdash (\Sigma; \mathbb{M}; \Gamma \Rightarrow_T \Delta \searrow S)$ *and such an* S *can be finitely computed.*

Proof: By a counting argument using Theorem 8. See Appendix A, Theorem 29 for details. ∎

Note that Theorem 14(2) does not stipulate that the computed S be unique. Indeed, depending on the order in which the rules of the calculus $\Rightarrow_\text{T}$ are applied to a given sequent, S may be different. However, the fact that at least one such S exists and can be computed is enough to get decidability for BL_sf.

Theorem 15 (Correctness)**.** *For a tree-like* $\mathbb{M}$*, suppose that* S *is such that* $\vdash (\Sigma; \mathbb{M}; \Gamma \Rightarrow_T \Delta \searrow S)$ *(such an* S *must exist and can be computed using Theorem 14). Then:*

1) *If* $S = \{\}$*, then* $\models (\Sigma; \mathbb{M}; \Gamma \Rightarrow \Delta)$.
2) *If* $S \neq \{\}$*, then every model* $\mathcal{M}$ *in* S *is a countermodel to the sequent, i.e.,* $\mathcal{M} \not\models (\Sigma; \mathbb{M}; \Gamma \Rightarrow \Delta)$.

Proof: The proof of this theorem uses an intermediate calculus. See Appendix C, Theorem 31 for details. ∎

Corollary 16 (Decidability and finite model property)**.** BL_sf *is decidable, has the finite model property and has a constructive decision procedure.*

Proof: Immediate from Theorem 15. ∎

Example 17. Consider the policy P containing the facts 1–3 from Example 1. These facts *do not* entail `deletefile1`. When we run the sequent $x; \cdot; x : P \Rightarrow_\text{T} x :$ `deletefile1` $\searrow \ldots$ through the procedure of Figure 2, all branches except one close. That one branch produces a countermodel with three worlds x, y, z, relations $xS_{\texttt{admin}}y, yS_{\texttt{Bob}}z, yS_{\texttt{Alice}}z, xS_{\texttt{Bob}}z, xS_{\texttt{Alice}}z, z \leq y, x \leq x, y \leq y, z \leq z$, and the assignments $h(\texttt{deletefile1}) = \{\}$ and $sf(\texttt{Alice}, \texttt{Bob}) = \{x, y, z\}$. It is easily verified that this countermodel satisfies $x : P$, but does not satisfy $x :$ `deletefile1`.

IV. Policy Saturation

Our second application of the labeled sequent calculus SeqC is policy saturation, the problem of generating all possible atomic consequences of a given policy. This is useful, e.g., to pre-compile a policy to access control lists. The usual approach to policy saturation is based in bottom-up logic programming engines like Datalog, used in the context of access control in systems like SecPAL [9]. We show that, surprisingly, our construction of countermodels from Section III-B directly yields a completely different algorithm to find all atomic consequences of a policy.

Our algorithm works as follows. Suppose we wish to find all atomic consequences of the policy $\varphi_1, \ldots, \varphi_n$. We choose a symbolic world x and run the decision procedure of Section III-B with $\Sigma = x$, $\mathbb{M} = \cdot$, $\Gamma = x : \varphi_1, \ldots, x : \varphi_n$ and $\Delta = \cdot$. If the algorithm ends with $S = \{\}$, then the policy is (clearly) inconsistent and it proves any atomic formula. If, on the other hand, the algorithm ends with $S \neq \{\}$, then as the following theorem states, $x : p$ is provable from Γ iff $x \in h(p)$ in every model $\mathcal{M}$ in S. Thus, by running

Axiom Rules

$$\frac{\text{No other rule applies}}{\Sigma; \mathbb{M}; \Gamma \Rightarrow_{\mathrm{T}} \Delta \searrow \{\mathsf{CM}(\Sigma; \mathbb{M}; \Gamma; \Delta)\}}\,\text{CM} \qquad \frac{}{\Sigma; \mathbb{M}, x \leq y; \Gamma, x : p \Rightarrow_{\mathrm{T}} y : p, \Delta \searrow \{\}}\,\text{init}$$

$$\frac{}{\Sigma; \mathbb{M}; \Gamma, x : A \mathsf{\ sf\ } B \Rightarrow_{\mathrm{T}} x : A \mathsf{\ sf\ } B, \Delta \searrow \{\}}\,\text{sf}$$

Logical Rules

$$\frac{\boxed{x : \alpha \notin \Delta \text{ and } x : \beta \notin \Delta} \qquad \Sigma; \mathbb{M}; \Gamma \Rightarrow_{\mathrm{T}} x : \alpha, x : \alpha \wedge \beta, \Delta \searrow S_1 \qquad \Sigma; \mathbb{M}; \Gamma \Rightarrow_{\mathrm{T}} x : \beta, x : \alpha \wedge \beta, \Delta \searrow S_2}{\Sigma; \mathbb{M}; \Gamma \Rightarrow_{\mathrm{T}} x : \alpha \wedge \beta, \Delta \searrow S_1 \cup S_2}\,\wedge\text{R}$$

$$\frac{\boxed{\forall y \in \Sigma.(x \leq y \in \mathbb{M}) \Rightarrow (y : \alpha \notin \Gamma \text{ or } y : \beta \notin \Delta)} \quad \boxed{\forall y \in \Sigma.(y \ll x) \Rightarrow (x = y \text{ or } x \not\preccurlyeq y)} \qquad \Sigma, y; \mathbb{M}, x \leq y; \Gamma, y : \alpha \Rightarrow_{\mathrm{T}} y : \beta, x : \alpha \to \beta, \Delta \searrow S}{\Sigma; \mathbb{M}; \Gamma \Rightarrow_{\mathrm{T}} x : \alpha \to \beta, \Delta \searrow S}\,\to\text{R}$$

$$\frac{\boxed{y : \alpha \notin \Delta \text{ and } y : \beta \notin \Gamma} \qquad \Sigma; \mathbb{M}, x \leq y; \Gamma, x : \alpha \to \beta \Rightarrow_{\mathrm{T}} y : \alpha, \Delta \searrow S_1 \qquad \Sigma; \mathbb{M}, x \leq y; \Gamma, x : \alpha \to \beta, y : \beta \Rightarrow_{\mathrm{T}} \Delta \searrow S_2}{\Sigma; \mathbb{M}, x \leq y; \Gamma, x : \alpha \to \beta \Rightarrow_{\mathrm{T}} \Delta \searrow S_1 \cup S_2}\,\to\text{L}$$

$$\frac{\boxed{\forall y \in \Sigma.(xS_Ay \in \mathbb{M}) \Rightarrow y : \alpha \notin \Delta} \quad \boxed{\forall y \in \Sigma.(y \ll x) \Rightarrow (x = y \text{ or } x \not\preccurlyeq y)} \qquad \Sigma, y; \mathbb{M}, xS_Ay; \Gamma \Rightarrow_{\mathrm{T}} y : \alpha, x : A \mathsf{\ says\ } \alpha, \Delta \searrow S}{\Sigma; \mathbb{M}; \Gamma \Rightarrow_{\mathrm{T}} x : A \mathsf{\ says\ } \alpha, \Delta \searrow S}\,\text{saysR}$$

$$\frac{\boxed{y : \alpha \notin \Gamma} \qquad \Sigma; \mathbb{M}, xS_Ay; \Gamma, x : A \mathsf{\ says\ } \alpha, y : \alpha \Rightarrow_{\mathrm{T}} \Delta \searrow S}{\Sigma; \mathbb{M}, xS_Ay; \Gamma, x : A \mathsf{\ says\ } \alpha \Rightarrow_{\mathrm{T}} \Delta \searrow S}\,\text{saysL}$$

Frame Rules

$$\frac{\boxed{xS_Az \notin \mathbb{M}} \qquad \Sigma; \mathbb{M}, x \leq y, yS_Az, xS_Az; \Gamma \Rightarrow_{\mathrm{T}} \Delta \searrow S}{\Sigma; \mathbb{M}, x \leq y, yS_Az; \Gamma \Rightarrow_{\mathrm{T}} \Delta \searrow S}\,\text{mon-S}$$

$$\frac{\boxed{xS_Az \notin \mathbb{M}} \qquad \Sigma; \mathbb{M}, xS_By, yS_Az, xS_Az; \Gamma \Rightarrow_{\mathrm{T}} \Delta \searrow S}{\Sigma; \mathbb{M}, xS_By, yS_Az; \Gamma \Rightarrow_{\mathrm{T}} \Delta \searrow S}\,\text{I}$$

$$\frac{\boxed{xS_Ay \notin \mathbb{M}} \qquad \Sigma; \mathbb{M}, xS_By, xS_Ay; \Gamma, x : A \mathsf{\ sf\ } B \Rightarrow_{\mathrm{T}} \Delta \searrow S}{\Sigma; \mathbb{M}, xS_By; \Gamma, x : A \mathsf{\ sf\ } B \Rightarrow_{\mathrm{T}} \Delta \searrow S}\,\text{basic-sf}$$

Fig. 2. $\mathrm{SeqC_T}$: Terminating, countermodel producing sequent calculus for $\mathrm{BL_{sf}}$, selected rules. Applicability conditions are written in boxes. Wherever mentioned, the relation $\preccurlyeq$ is the equivalence relation of the contexts $\Sigma; \mathbb{M}; \Gamma; \Delta$ in the conclusion of the rule. Similarly, $\ll$ is the order of the underlying tree of $\mathbb{M}$.

our decision procedure on the policy with an empty goal and *intersecting* the valuation of the initial worlds in the ensuing countermodels, we obtain exactly the set of all provable atoms. We call this property comprehensiveness.

Theorem 18 (Comprehensiveness)**.** *Suppose* $\mathbb{M}$ *is tree-like and* $\vdash (\Sigma; \mathbb{M}; \Gamma \Rightarrow_T \Delta \searrow S)$*. Then* $\vdash (\Sigma; \mathbb{M}; \Gamma \Rightarrow x : p, \Delta)$ *iff* $\forall \mathcal{M} \in S.\ \mathcal{M} \models x : p$*.*

Proof: See Appendix D, Theorem 34. ∎

Example 19. Let P be the set of formulas 1–3 from Example 1 and let $P' = P$, `Alice says deletefile1`. We intuitively expect that the only atomic consequence of P' is `deletefile1`. Using the saturation procedure described above, we confirm this intuition. When we run the sequent $x; \cdot; x : P' \Rightarrow_{\mathrm{T}} \cdot \searrow \ldots$ through the procedure of Figure 2, it produces exactly one countermodel with one world x, the relations $x \leq x$, and the assignments $h(\texttt{deletefile1}) = \{x\}$ and $sf(A, B) = \{x\}$. Using Theorem 18, we conclude that

the only atomic consequence of the policy is `deletefile1`, which is also what we expected intuitively.

V. Policy Abduction

Next, we adapt the labeled sequent calculus SeqC to a procedure for abduction over access policies written in $\mathrm{BL_{sf}}$. Abduction is the problem of finding credentials that together with a given policy Γ prove a given goal φ. These missing credentials, the output of abduction, are represented by a formula, often called the abducible. For example, if Γ entails φ then no additional credentials are required and the abducible is $\top$. Similarly, for $\Gamma = q \to p, (r \wedge s) \to p$ and $\varphi = p$, the abducible is $p \vee q \vee (r \wedge s)$. In practice, abducibles are restricted to formulas of specific forms that can be easily justified a priori (without assumptions).

In the following, we adapt the terminating calculus $\mathrm{SeqC_T}$ of Section III-B to obtain a general abduction method for $\mathrm{BL_{sf}}$. Our abducibles are simple formulas containing the connectives $\wedge$, $\vee$ and formulas $\top$, $\bot$, p and A says p at the leaves, as formalized in the following definition.

$$\text{Abducible} \quad \Theta \quad ::= \quad p \mid A \text{ says } p \mid \top \mid \bot \mid \Theta_1 \wedge \Theta_2 \mid \Theta_1 \vee \Theta_2$$

We do not allow formulas of the forms $\varphi \to \psi$ and A sf B in abducibles because we want that abducibles be easy to justify a priori; this is true for formulas of the above restricted forms, but is not the case for arbitrary formulas.

The abduction procedure is presented as a calculus $\mathrm{SeqC_A}$, whose selected rules are shown in Figure 3. The calculus is an adaptation of the terminating calculus $\mathrm{SeqC_T}$ of Figure 2, obtained by replacing the output countermodels with abducibles. Its sequents have the form $\Sigma; \mathbb{M}; \Gamma \Rightarrow_{\mathrm{A}} \Delta \searrow \Theta$. The applicability conditions are the same, so backwards search in the calculus terminates as it does for $\mathrm{SeqC_T}$. The main rule is AB, which is a replacement of the earlier rule CM. In this rule, the input contexts $\Sigma; \mathbb{M}; \Gamma; \Delta$ are a saturated history, so the output is an abducible, $\mathrm{AB}(\Sigma; \mathbb{M}; \Gamma; \Delta)$, which is defined below. Here, $\mathrm{root}(\mathbb{M})$ is the root of the underlying tree of $\mathbb{M}$.

$$\begin{gathered}\mathrm{AB}(\Sigma; \mathbb{M}; \Gamma; \Delta) \;= \\ (\bigvee\{p \mid y : p \in \Delta \text{ and } (\mathrm{root}(\mathbb{M})) \leq y \in \mathbb{M}\}) \vee \\ (\bigvee\{A \text{ says } p \mid y : p \in \Delta \text{ and } (\mathrm{root}(\mathbb{M}))S_A y \in \mathbb{M}\})\end{gathered}$$

Intuitively, for every labeled atom $y : p \in \Delta$, we look at the path between the root of the underlying tree of $\mathbb{M}$ and y. Because the saturated history is closed under backward application of rules (I), (mon-S) and (trans), either $(\mathrm{root}(\mathbb{M})) \leq y \in \mathbb{M}$ or $(\mathrm{root}(\mathbb{M}))S_A y \in \mathbb{M}$ for some $A \in \mathcal{I}$. In the former case, it suffices to add the credential p to complete the proof and in the latter case it suffices to add the credential A says p to complete the proof. If both sets in the definition of $\mathrm{AB}(\Sigma; \mathbb{M}; \Gamma; \Delta)$ are empty, then $\mathrm{AB}(\Sigma; \mathbb{M}; \Gamma; \Delta) = \bot$. This can happen only if we start from a sequent that contains $\bot$ in positive positions (i.e., as subgoals).

An abducible Θ is *satisfied* by extending the current policy Γ with a set $F \subseteq \{p, A \text{ says } p \mid A \in \mathcal{I}\}$. Given such a set, we define the satisfaction relation $F \models \Theta$ in the obvious way:

- $F \models \top$ (always)
- $F \models p$ iff $p \in F$
- $F \models A$ says p iff $(A \text{ says } p) \in F$
- $F \models \Theta_1 \wedge \Theta_2$ iff $F \models \Theta_1$ and $F \models \Theta_2$
- $F \models \Theta_1 \vee \Theta_2$ iff $F \models \Theta_1$ or $F \models \Theta_2$

The following theorem states that our abduction procedure is sound in the sense that if the abducible of a sequent is satisfied by F, then extending the hypotheses with F results in a provable sequent.

Theorem 20 (Soundness)**.** *If* $\vdash (\Sigma; \mathbb{M}; \Gamma \Rightarrow_A \Delta \searrow \Theta)$ *and* $F \models \Theta$*, then* $\vdash (\Sigma; \mathbb{M}; \Gamma, \mathit{root}(\mathbb{M}) : F \Rightarrow \Delta)$.

Proof: See Appendix E, Theorem 35. ∎

Example 21. Let P be the set of formulas 1–3 from Example 1. These facts do not entail `deletefile1`, so we can try to run our abduction algorithm. When we run the sequent $x; \cdot; x : P \Rightarrow_{\mathrm{A}} x : \texttt{deletefile1} \searrow \ldots$ through the procedure of Figure 3, all branches except one close. That one branch ends in a saturated history with three worlds x, y, z, relations $xS_{\texttt{admin}}y, yS_{\texttt{Bob}}z, yS_{\texttt{Alice}}z, xS_{\texttt{Bob}}z, xS_{\texttt{Alice}}z, x \leq x, y \leq y, z \leq z$, and a Δ containing x : `deletefile1`, y : `deletefile1` and z : `deletefile1`. Consequently, the abducible is the formula `deletefile1` $\vee$ (`admin` says `deletefile1`) $\vee$ (`Bob` says `deletefile1`) $\vee$ (`Alice` says `deletefile1`), i.e., our goal `deletefile1` can be proved if any of `admin`, `Bob`, `Alice` assert it. This is exactly what we expect from an informal analysis of the policy.

VI. Related Work

We discuss closely related work on decision procedures, saturation and abduction for access control logics.

A procedure to generate countermodels in the context of access control is new to our work, but the importance of this idea has been anticipated before. Regarding decision procedures, there are some decidability results for access control logics, e.g., for the logic ICL [14] and the logic programming language SecPAL [9], but for the logic presented in this paper, the decidability result is also new. Our specific countermodel producing decision procedure is based on our prior work on multi-modal logics [15], which in turn is inspired by work for uni-modal logics, notably that of Gasquet et al. [18] and Negri [21, 22]. In terms of presentation, our labeled sequent calculus is presented is similar to that of Negri [21].

The idea of saturation for access policies has been investigated several times, notably in access control languages like SecPAL and Binder whose implementations or semantics are defined by translation into Datalog [9, 13]. Our technique of saturating policies using a comprehensive set of countermodels is novel. Saturation by translation to Datalog is likely more efficient than our method, but our method is more general because it covers all connectives of the logic.

Abduction for access policies has been investigated formally by Becker et al. [10, 11] in the context of SecPAL. Their procedure is based on an adaptation of a tabled logic programming engine. Our algorithm is more general because it handles all

Axiom Rules

$$\frac{\text{No other rule applies}}{\Sigma; \mathbb{M}; \Gamma \Rightarrow_{\mathrm{A}} \Delta \searrow \mathrm{AB}(\Sigma; \mathbb{M}; \Gamma; \Delta)}\,\mathrm{AB} \qquad \frac{}{\Sigma; \mathbb{M}, x \leq y; \Gamma, x : p \Rightarrow_{\mathrm{A}} y : p, \Delta \searrow \top}\,\mathrm{init}$$

$$\frac{}{\Sigma; \mathbb{M}; \Gamma, x : A \;\mathsf{sf}\; B \Rightarrow_{\mathrm{A}} x : A \;\mathsf{sf}\; B, \Delta \searrow \top}\,\mathrm{sf}$$

Logical Rules

$$\frac{\boxed{x : \alpha \notin \Delta \text{ and } x : \beta \notin \Delta} \qquad \Sigma; \mathbb{M}; \Gamma \Rightarrow_{\mathrm{A}} x : \alpha, x : \alpha \wedge \beta, \Delta \searrow \Theta_1 \qquad \Sigma; \mathbb{M}; \Gamma \Rightarrow_{\mathrm{A}} x : \beta, x : \alpha \wedge \beta, \Delta \searrow \Theta_2}{\Sigma; \mathbb{M}; \Gamma \Rightarrow_{\mathrm{A}} x : \alpha \wedge \beta, \Delta \searrow \Theta_1 \wedge \Theta_2}\,\wedge\mathrm{R}$$

$$\frac{\boxed{\forall y \in \Sigma.(x \leq y \in \mathbb{M}) \Rightarrow (y : \alpha \notin \Gamma \text{ or } y : \beta \notin \Delta)} \quad \boxed{\forall y \in \Sigma.(y \ll x) \Rightarrow (x = y \text{ or } x \not\ll y)} \qquad \Sigma, y; \mathbb{M}, x \leq y; \Gamma, y : \alpha \Rightarrow_{\mathrm{A}} y : \beta, x : \alpha \to \beta, \Delta \searrow \Theta}{\Sigma; \mathbb{M}; \Gamma \Rightarrow_{\mathrm{A}} x : \alpha \to \beta, \Delta \searrow \Theta}\,\to\mathrm{R}$$

$$\frac{\boxed{y : \alpha \notin \Delta \text{ and } y : \beta \notin \Gamma} \qquad \Sigma; \mathbb{M}, x \leq y; \Gamma, x : \alpha \to \beta \Rightarrow_{\mathrm{A}} y : \alpha, \Delta \searrow \Theta_1 \qquad \Sigma; \mathbb{M}, x \leq y; \Gamma, x : \alpha \to \beta, y : \beta \Rightarrow_{\mathrm{A}} \Delta \searrow \Theta_2}{\Sigma; \mathbb{M}, x \leq y; \Gamma, x : \alpha \to \beta \Rightarrow_{\mathrm{A}} \Delta \searrow \Theta_1 \wedge \Theta_2}\,\to\mathrm{L}$$

$$\frac{\boxed{\forall y \in \Sigma.(xS_Ay \in \mathbb{M}) \Rightarrow y : \alpha \notin \Delta} \quad \boxed{\forall y \in \Sigma.(y \ll x) \Rightarrow (x = y \text{ or } x \not\ll y)} \qquad \Sigma, y; \mathbb{M}, xS_Ay; \Gamma \Rightarrow_{\mathrm{A}} y : \alpha, x : A \;\mathsf{says}\; \alpha, \Delta \searrow \Theta}{\Sigma; \mathbb{M}; \Gamma \Rightarrow_{\mathrm{A}} x : A \;\mathsf{says}\; \alpha, \Delta \searrow \Theta}\,\mathrm{saysR}$$

$$\frac{\boxed{y : \alpha \notin \Gamma} \qquad \Sigma; \mathbb{M}, xS_Ay; \Gamma, x : A \;\mathsf{says}\; \alpha, y : \alpha \Rightarrow_{\mathrm{A}} \Delta \searrow \Theta}{\Sigma; \mathbb{M}, xS_Ay; \Gamma, x : A \;\mathsf{says}\; \alpha \Rightarrow_{\mathrm{A}} \Delta \searrow \Theta}\,\mathrm{saysL}$$

Frame Rules

$$\frac{\boxed{xS_Az \notin \mathbb{M}} \qquad \Sigma; \mathbb{M}, x \leq y, yS_Az, xS_Az; \Gamma \Rightarrow_{\mathrm{A}} \Delta \searrow \Theta}{\Sigma; \mathbb{M}, x \leq y, yS_Az; \Gamma \Rightarrow_{\mathrm{A}} \Delta \searrow \Theta}\,\text{mon-S}$$

$$\frac{\boxed{xS_Az \notin \mathbb{M}} \qquad \Sigma; \mathbb{M}, xS_By, yS_Az, xS_Az; \Gamma \Rightarrow_{\mathrm{A}} \Delta \searrow \Theta}{\Sigma; \mathbb{M}, xS_By, yS_Az; \Gamma \Rightarrow_{\mathrm{A}} \Delta \searrow \Theta}\,\mathrm{I}$$

$$\frac{\boxed{xS_Ay \notin \mathbb{M}} \qquad \Sigma; \mathbb{M}, xS_By, xS_Ay; \Gamma, x : A \;\mathsf{sf}\; B \Rightarrow_{\mathrm{A}} \Delta \searrow \Theta}{\Sigma; \mathbb{M}, xS_By; \Gamma, x : A \;\mathsf{sf}\; B \Rightarrow_{\mathrm{A}} \Delta \searrow \Theta}\,\text{basic-sf}$$

Fig. 3. $\mathrm{SeqC_A}$: Abduction calculus calculus for $\mathrm{BL_{sf}}$, selected rules.

connectives of the logic, but may be less efficient. Abductive credential gathering for access policies has been implemented several times using heuristics, e.g., in the Grey system [7].

VII. Conclusion

Using a specific access control logic $\mathrm{BL_{sf}}$, we have argued that Kripke semantics, manifest in the symbolic framework of labeled sequent calculi, can be used to solve three practical access control problems: Countermodel generation, policy saturation, and policy abduction. The foundational underpinning of our work is a non-trivial, countermodel producing decision procedure for the logic $\mathrm{BL_{sf}}$. The same decision procedure yields algorithms for policy saturation and abduction.

In future work, we plan to implement our algorithms and evaluate them on realistic access policies. The main challenge we anticipate is that our algorithms, as presented in this paper, have significant computational complexity, and may be inefficient in practice. To alleviate this problem, we plan to investigate adaptations of our techniques to goal-directed (backchaining) search, which is usually very efficient in practice. The adaptation is likely to be non-trivial because, unlike the rules of the sequent calculus of Figure 1, rules

of goal-directed search are non-invertible, which may make construction of countermodels very difficult.

References

[1] M. Abadi, "Logic in access control," in *Proceedings of the 18th Annual IEEE Symposium on Logic in Computer Science (LICS)*, 2003, pp. 228–233.

[2] M. Abadi, M. Burrows, B. Lampson, and G. Plotkin, "A calculus for access control in distributed systems," *ACM TOPLAS*, vol. 15, no. 4, pp. 706–734, 1993.

[3] A. W. Appel and E. W. Felten, "Proof-carrying authentication," in *6th ACM Conference on Computer and Communications Security (CCS)*, 1999, pp. 52–62.

[4] K. Avijit, A. Datta, and R. Harper, "Distributed programming with distributed authorization," in *Proceedings of the Fifth ACM Workshop on Types in Language Design and Implementation (TLDI)*, 2010, pp. 27–38.

[5] D. Basin, S. Matthews, and L. Vigano, "Labelled Propositional Modal Logics: Theory and Practice," *Journal of Logic and Computation*, vol. 7, no. 6, pp. 685–717, 1997.

[6] L. Bauer, "Access control for the web via proof-carrying authorization," Ph.D. dissertation, Princeton University, 2003.

[7] L. Bauer, S. Garriss, J. M. McCune, M. K. Reiter, J. Rouse, and P. Rutenbar, "Device-enabled authorization in the Grey system," in *Proceedings of the 8th International Conference on Information Security (ISC)*, 2005, pp. 431–445.

[8] M. Y. Becker, "Information flow in credential systems," in *Proceedings of the 23rd IEEE Symposium on Computer Security Foundations (CSF)*, 2010, pp. 171–185.

[9] M. Y. Becker, C. Fournet, and A. D. Gordon, "SecPAL: Design and semantics of a decentralized authorization language," *Journal of Computer Security*, vol. 18, no. 4, pp. 619–665, 2010.

[10] M. Y. Becker, J. F. Mackay, and B. Dillaway, "Abductive authorization credential gathering," in *IEEE International Symposium on Policies for Distributed Systems and Networks (POLICY)*, 2009, pp. 1–8.

[11] M. Y. Becker and S. Nanz, "The role of abduction in declarative authorization policies," in *Proceedings of the 10th International Symposium on Practical Aspects of Declarative Languages (PADL)*, 2008, pp. 84–99.

[12] P. Blackburn, M. de Rijke, and Y. Venema, *Modal Logic*. Cambridge University Press, 2001, no. 53.

[13] J. DeTreville, "Binder, a logic-based security language," in *IEEE Symposium on Security and Privacy*, 2002, pp. 105–113.

[14] D. Garg and M. Abadi, "A modal deconstruction of access control logics," in *Proceedings of the 11th International Conference on Foundations of Software Science and Computational Structures (FoSSaCS)*, 2008, pp. 216–230.

[15] D. Garg, V. Genovese, and S. Negri, "Countermodels from sequent calculi in multi-modal logics," in *Proceedings of the 27th Annual IEEE/ACM Symposium on Logic in Computer Science (LICS)*, 2012, to appear. Available online at http://www.mpi-sws.org/ dg/.

[16] D. Garg and F. Pfenning, "Non-interference in constructive authorization logic," in *Proceedings of the 19th IEEE Computer Security Foundations Workshop (CSFW)*, 2006, pp. 283–293.

[17] ——, "A proof-carrying file system," in *Proceedings of the 31st IEEE Symposium on Security and Privacy (Oakland)*, 2010, pp. 349–364.

[18] O. Gasquet, A. Herzig, and M. Sahade, "Terminating modal tableaux with simple completeness proof," in *Advances in Modal Logic*, 2006, pp. 167–186.

[19] V. Genovese, D. Garg, and D. Rispoli, "Labeled sequent calculi for access control logics: Countermodels, saturation and abduction," 2012, technical report. Available online at http://www.mpi-sws.org/ dg/.

[20] L. Jia, J. A. Vaughan, K. Mazurak, J. Zhao, L. Zarko, J. Schorr, and S. Zdancewic, "Aura: A programming language for authorization and audit," in *Proceedings of the International Conference on Functional Programming (ICFP)*, 2008, pp. 27–38.

[21] S. Negri, "Proof analysis in modal logic," *Journal of Philosophical Logic*, vol. 34, pp. 507–544, 2005.

[22] ——, "Kripke completeness revisited," in *Acts of Knowledge – History, Philosophy and Logic*, G. Primiero and S. Rahman, Eds. College Publications, 2009.

[23] A. Pimlott and O. Kiselyov, "Soutei, a logic-based trust-management system," in *Proceedings of the Eighth International Symposium on Functional and Logic Programming (FLOPS 2006)*, 2006, pp. 130–145.

[24] F. B. Schneider, K. Walsh, and E. G. Sirer, "Nexus Authorization Logic (NAL): Design rationale and applications," *ACM Transactions on Information Systems Security*, vol. 14, no. 1, pp. 1–28, 2011.

[25] A. K. Simpson, "The proof theory and semantics of intuitionistic modal logic," Ph.D. dissertation, University of Edinburgh, 1994.

[26] N. Swamy, J. Chen, C. Fournet, P.-Y. Strub, K. Bhargavan, and J. Yang, "Secure distributed programming with value-dependent types," in *Proceedings of the 16th ACM SIGPLAN International Conference on Functional Programming (ICFP)*, 2011, pp. 266–278.

[27] E. Wobber, M. Abadi, and M. Burrows, "Authentication in the Taos operating system," *ACM Transactions on Computer Systems*, vol. 12, no. 1, pp. 3–32, 1994.

[28] F. Wolter and M. Zakharyaschev, "Intuitionistic modal logics," in *Logic and Foundations of Mathematics*. Kulwer Academic, 1999, pp. 227–238.

Appendix

A. Proofs from Section III

Lemma 22. *Let* $\Sigma; \mathbb{M}; \Gamma; \Delta$ *be a saturated history,* $C \subseteq \{x \leq y \mid x \preccurlyeq y\}$ *and* $\mathbb{M}'; \Gamma' = \overline{(\mathbb{M} \cup C); \Gamma}$. *Then:*

1) *If* $x \leq y \in \mathbb{M}'$, *then* $x(\leq \cup\, C)^* y \in \mathbb{M}$
2) *If* $x S_A y \in \mathbb{M}'$, *then* $x((\leq \cup\, S_* \cup C)^* \circ S_A) y \in \mathbb{M}$.

Proof: By induction on iteration of frame rules that leads to the closure $\overline{(\mathbb{M} \cup C); \Gamma}$. (1) is straightforward. For (2), we need some Lemmas. First, we prove that for any intermediate result $\mathbb{M}_n; \Gamma_n$ in the iteration that defines $\overline{(\mathbb{M} \cup C); \Gamma}$, if $x(\leq \cup N_*)y \in \mathbb{M}_n$, then $x(\leq \cup C \cup N_*)^* y \in \mathbb{M}$. Using this we prove that if $x : A \mathsf{\ sf\ } B \in \Gamma_n$, then $x : A \mathsf{\ sf\ } B \in \Gamma$. The critical rules are (mon1-sf) and (mon2-sf). Finally, we prove the required statement. The critical rule is (basic-sf). ■

Lemma 23 (Lemma 11)**.** *If $\Sigma; \mathbb{M}; \Gamma; \Delta$ is a saturated history, then CM$(\Sigma; \mathbb{M}; \Gamma; \Delta)$ has a monotonic valuation h, i.e., $x \in h(p)$ and $x \leq y \in$ CM$(\Sigma; \mathbb{M}; \Gamma; \Delta)$ imply $y \in h(p)$.*

Proof: Suppose that $x \leq y \in \text{CM}(\Sigma; \mathbb{M}; \Gamma; \Delta)$, i.e., $x \leq y \in \mathbb{M}'$ and $x \in h(p)$. From the latter, there is a z such that $z \leq x \in \mathbb{M}$ and $z : p \in \Gamma$. From Lemma 22(1) it follows that $x(\leq \cup C)^* y$, where all the relations $\leq$ are in $\mathbb{M}$. Hence, we have a chain $x = x_0(\leq \cup C)x_1 \ldots (\leq \cup C)x_n = y$ where all relations $\leq$ are in $\mathbb{M}$. We induct on i to show that $T(p) \in \text{Sfor}(x_i)$.

- For $i = 0$, $x_0 = x$ and we know that $z : p \in \Gamma$ and $z \leq x \in \mathbb{M}$. It follows from definition of Sfor that $T(p) \in \text{Sfor}(x)$, as required.
- For the induction step, assume that $T(p) \in \text{Sfor}(x_i)$. We prove that $T(p) \in \text{Sfor}(x_{i+1})$. We consider two possible cases on the relation $x_i(\leq \cup C)x_{i+1}$.
  - $x_i \leq x_{i+1} \in \mathbb{M}$. Because $T(p) \in \text{Sfor}(x_i)$, there is a z' such that $z' \leq x_i \in \mathbb{M}$ and $z' : p \in \Gamma$. Hence, also $z' \leq x_{i+1} \in \mathbb{M}$. So $T(p) \in \text{Sfor}(x_{i+1})$.
  - $(x_i, x_{i+1}) \in C$. Because of the definition of C, $\text{Sfor}(x_i) \subseteq \text{Sfor}(x_{i+1})$, so $T(p) \in \text{Sfor}(x_i)$ immediately implies $T(p) \in \text{Sfor}(x_{i+1})$.

This completes the inductive proof that $T(p) \in \text{Sfor}(x_i)$. In particular, $T(p) \in \text{Sfor}(x_n)$. By definition of Sfor, there is a z' such that $z' \leq x_n \in \mathbb{M}$ and $z' : p \in \Gamma$. This immediately implies $x_n \in h(p)$, i.e., $y \in h(p)$, as required. ■

Lemma 24 (Lemma 12)**.** *The following hold for any saturated history $\Sigma; \mathbb{M}; \Gamma; \Delta$:*

A. *If $T(\varphi) \in$ Sfor$(\Sigma; \mathbb{M}; \Gamma; \Delta, x)$, then CM$(\Sigma; \mathbb{M}; \Gamma; \Delta) \models x : \varphi$*
B. *If $F(\varphi) \in$ Sfor$(\Sigma; \mathbb{M}; \Gamma; \Delta, x)$, then CM$(\Sigma; \mathbb{M}; \Gamma; \Delta) \not\models x : \varphi$*

Proof: We prove both properties simultaneously by *lexicographic* induction, first on φ, and then on the partial (tree-like) order $\ll$ of $\mathbb{M}$. (Note that we cannot induct on either $\mathbb{M}$ or the relation in CM$(\Sigma; \mathbb{M}; \Gamma; \Delta)$, because both of these may potentially be cyclic.) Since the context $\Sigma; \mathbb{M}; \Gamma; \Delta$ is fixed here, we abbreviate Sfor$(\Sigma; \mathbb{M}; \Gamma; \Delta, x)$ to Sfor(x). Let C be the set $\{(x, y) \mid x \preccurlyeq y\}$.

Proof of A.

Case. $\varphi = p$. We are given that $T(p) \in \text{Sfor}(x)$ and want to prove that CM$(\Sigma; \mathbb{M}; \Gamma; \Delta) \models x : p$. Since $T(p) \in \text{Sfor}(x)$, we know from definition of the function Sfor that there is a y with $y \leq x \in \mathbb{M}$ and $y : p \in \Gamma$. Since $y \leq x \in \mathbb{M}$, we know from definition of CM$(\Sigma; \mathbb{M}; \Gamma; \Delta)$ that $x \in h(p)$. Hence, by definition of $\models$, we have CM$(\Sigma; \mathbb{M}; \Gamma; \Delta) \models x : p$.

Case. $\varphi = \top$. Here, CM$(\Sigma; \mathbb{M}; \Gamma; \Delta) \models x : \top$ is trivial by the definition of $\models$.

Case. $\varphi = \bot$. Then the pre-condition $T(\bot) \in \text{Sfor}(x)$ or, equivalently, $x : \bot \in \Delta$ is impossible by clause (3) of the definition of saturated history. So this case is vacuous.

Case. $\varphi = \alpha \wedge \beta$. We are given that $T(\alpha \wedge \beta) \in \text{Sfor}(x)$ or, equivalently, that $x : \alpha \wedge \beta \in \Gamma$. By clause (5) of the definition of saturated history, $x : \alpha \in \Gamma$ and $x : \beta \in \Gamma$. Hence, $T(\alpha) \in \text{Sfor}(x)$ and $T(\beta) \in \text{Sfor}(x)$. By the i.h., CM$(\Sigma; \mathbb{M}; \Gamma; \Delta) \models x : \alpha$ and CM$(\Sigma; \mathbb{M}; \Gamma; \Delta) \models x : \beta$. Hence, CM$(\Sigma; \mathbb{M}; \Gamma; \Delta) \models x : \alpha \wedge \beta$, as required.

Case. $\varphi = \alpha \vee \beta$. We are given that $T(\alpha \vee \beta) \in \text{Sfor}(x)$ or, equivalently, that $x : \alpha \vee \beta \in \Gamma$. By clause (7) of the definition of saturated history, either $x : \alpha \in \Gamma$ or $x : \beta \in \Gamma$. Hence, either $T(\alpha) \in \text{Sfor}(x)$ or $T(\beta) \in \text{Sfor}(x)$. By the i.h., either CM$(\Sigma; \mathbb{M}; \Gamma; \Delta) \models x : \alpha$ or CM$(\Sigma; \mathbb{M}; \Gamma; \Delta) \models x : \beta$. In either case, CM$(\Sigma; \mathbb{M}; \Gamma; \Delta) \models x : \alpha \wedge \beta$, as required.

Case. $\varphi = \alpha \to \beta$. We are given that $T(\alpha \to \beta) \in \text{Sfor}(x)$. We need to show that for any y such that $x \leq y$ in the model and CM$(\Sigma; \mathbb{M}; \Gamma; \Delta) \models y : \alpha$, we have CM$(\Sigma; \mathbb{M}; \Gamma; \Delta) \models y : \beta$. Pick any y such that $x \leq y$ in the model and CM$(\Sigma; \mathbb{M}; \Gamma; \Delta) \models y : \alpha$. From Lemma 22(1), it follows that $x(\leq \cup C)^* y$, where the $\leq$ relations are in $\mathbb{M}$. Hence, there is a chain $x = x_0(\leq \cup C)x_1 \ldots (\leq \cup C)x_n = y$, where the $\leq$ relations are in $\mathbb{M}$. We induct on i to prove that $T(\alpha \to \beta) \in \text{Sfor}(x_i)$ for each i.

- For $i = 0$, $x_0 = x$ and we are given that $T(\alpha \to \beta) \in \text{Sfor}(x)$, so we are done.
- For the inductive case, assume that $T(\alpha \to \beta) \in \text{Sfor}(x_i)$ for some i. We show that $T(\alpha \to \beta) \in \text{Sfor}(x_{i+1})$. We consider two possible cases on the relation $x_i(\leq \cup C)x_{i+1}$:
  - $x_i \leq x_{i+1} \in \mathbb{M}$: From the i.h., we know that $T(\alpha \to \beta) \in \text{Sfor}(x_i)$. Hence, there is a z' such that $z' \leq x_i \in \mathbb{M}$ and $z' : \alpha \to \beta \in \Gamma$. Clearly, $z' \leq x_{i+1} \in \mathbb{M}$, so $T(\alpha \to \beta) \in \text{Sfor}(x_{i+1})$.
  - $(x_i, x_{i+1}) \in C$: Because of the definition of C, $\text{Sfor}(x_i) \subseteq \text{Sfor}(x_{i+1})$, so $T(\alpha \to \beta) \in \text{Sfor}(x_i)$ immediately implies $T(\alpha \to \beta) \in \text{Sfor}(x_{i+1})$.

This completes the inductive proof. It follows, in particular, that $T(\alpha \to \beta) \in \text{Sfor}(x_n)$. Consequently, there is some z' such that $z' \leq x_n = y \in \mathbb{M}$ and $z' : \alpha \to \beta \in \Gamma$. Hence, by clause (9) of the definition of saturated history, we must have either $y : \alpha \in \Delta$ or $y : \beta \in \Gamma$. The former implies, by the i.h., that CM$(\Sigma; \mathbb{M}; \Gamma; \Delta) \not\models y : \alpha$, which contradicts our assumption that CM$(\Sigma; \mathbb{M}; \Gamma; \Delta) \models y : \alpha$. So, we must have $y : \beta \in \Gamma$. This implies $T(\beta) \in \text{Sfor}(y)$ and hence, by the

i.h., that $\text{CM}(\Sigma; \mathbb{M}; \Gamma; \Delta) \models y : \beta$.

Case. $\varphi = A$ says α. We are given that $T(A \text{ says } \alpha) \in \text{Sfor}(x)$. We need to show that $\text{CM}(\Sigma; \mathbb{M}; \Gamma; \Delta) \models x : A$ says α, i.e., for any y such that xS_Ay in the model, we have $\text{CM}(\Sigma; \mathbb{M}; \Gamma; \Delta) \models y : \alpha$. Pick any y such that xS_Ay in the model. By Lemma 22(2), we have $x((\leq \cup S_* \cup C)^* \circ S_A)y$, where the relations $\leq$ and S_A are in $\mathbb{M}$. So there are $x_0, \ldots, x_n$ such that $x = x_0(\leq \cup S_* \cup C)x_1 \ldots (\leq \cup S_* \cup C)x_nS_Ay$. We now prove, by induction on i, that $T(A \text{ says } \alpha) \in \text{Sfor}(x_i)$ for each i.

- For $i = 0$, $x_0 = x$ and we are given that $T(A \text{ says } \alpha) \in \text{Sfor}(x)$.
- For the inductive case, assume that $T(A \text{ says } \alpha) \in \text{Sfor}(x_i)$ for some i. We show that $T(A \text{ says } \alpha) \in \text{Sfor}(x_{i+1})$ by case analyzing the relation $x_i(\leq \cup S_* \cup C)x_{i+1}$.
  - $x_i(\leq \cup S_*)x_{i+1} \in \mathbb{M}$: By the i.h., $T(A \text{ says } \alpha) \in \text{Sfor}(x_i)$ so there is some z such that $z(\leq \cup S_*)^*x_i \in \mathbb{M}$ and $z : A \text{ says } \alpha \in \Gamma$. Clearly, we have $z(\leq \cup S_*)^*x_{i+1} \in \mathbb{M}$, so $T(A \text{ says } \alpha) \in \text{Sfor}(x_{i+1})$.
  - $(x_i, x_{i+1}) \in C$: Because of the definition of C, $\text{Sfor}(x_{i+1}) \supseteq \text{Sfor}(x_i)$. Thus, $T(A \text{ says } \alpha) \in \text{Sfor}(x_i)$ immediately implies $T(A \text{ says } \alpha) \in \text{Sfor}(x_{i+1})$.

Since we just proved that $T(A \text{ says } \alpha) \in \text{Sfor}(x_i)$, it follows, in particular, that $T(A \text{ says } \alpha) \in \text{Sfor}(x_n)$. Consequently, there is some z' such that $z'(\leq \cup S_*)^*x_n \in \mathbb{M}$ and $z' : A \text{ says } \alpha \in \Gamma$. Then, we also have (within $\mathbb{M}$) that: $z'(\leq \cup S_*)^*x'_nS_Ay$. So, due to conditions (I) and (mon-S), $z'S_Ay \in \mathbb{M}$. Hence, by clause (11) of the definition of saturated history, we must have $y : \alpha \in \Gamma$. Therefore, $T(\alpha) \in \text{Sfor}(y)$ and by the i.h., $\text{CM}(\Sigma; \mathbb{M}; \Gamma; \Delta) \models y : \alpha$.

Case. $\varphi = A$ sf B. We are given that $T(A \text{ sf } B) \in \text{Sfor}(x)$ and want to show that $\text{CM}(\Sigma; \mathbb{M}; \Gamma; \Delta) \models x : A \text{ sf } B$. From the assumption $T(A \text{ sf } B) \in \text{Sfor}(x)$ we know that $x : A \text{ sf } B \in \Gamma$, so by the definition of $\text{CM}(\Sigma; \mathbb{M}; \Gamma; \Delta)$, we have $x \in sf(A, B)$. Hence, by definition of $\models$, we get that $\text{CM}(\Sigma; \mathbb{M}; \Gamma; \Delta) \models x : A \text{ sf } B$.

Proof of B.

Case. $\varphi = p$. We are given that $F(p) \in \text{Sfor}(x)$ or, equivalently, that $x : p \in \Delta$. Suppose, for the sake of contradiction, that $\text{CM}(\Sigma; \mathbb{M}; \Gamma; \Delta) \models x : p$. Then, $x \in h(p)$ and hence, from the construction of the countermodel, there is a z such that $z \leq x \in \mathbb{M}$ and $z : p \in \Gamma$. This immediately contradicts clause (2) of the definition of saturated history because we have $z \leq x \in \mathbb{M}$, $z : p \in \Gamma$ and $x : p \in \Delta$. Hence we must have $\text{CM}(\Sigma; \mathbb{M}; \Gamma; \Delta) \not\models x : p$.

Case. $\varphi = \top$. Then the pre-condition $F(\top) \in \text{Sfor}(x)$ or, equivalently, $x : \top \in \Delta$ is impossible by clause (3) of the definition of saturated history. So this case is vacuous.

Case. $\varphi = \bot$. Here, $\text{CM}(\Sigma; \mathbb{M}; \Gamma; \Delta) \not\models x : \bot$ is trivial by the definition of $\models$.

Case. $\varphi = \alpha \wedge \beta$. Suppose $F(\alpha \wedge \beta) \in \text{Sfor}(x)$. Then, $x : \alpha \wedge \beta \in \Delta$. Hence, by clause (6) of the definition of saturated history, either $x : \alpha \in \Delta$ or $x : \beta \in \Delta$. Therefore, either $F(\alpha) \in \text{Sfor}(x)$ or $F(\beta) \in \text{Sfor}(x)$. By i.h., either $\text{CM}(\Sigma; \mathbb{M}; \Gamma; \Delta) \not\models x : \alpha$ or $\text{CM}(\Sigma; \mathbb{M}; \Gamma; \Delta) \not\models x : \beta$. In either case, $\text{CM}(\Sigma; \mathbb{M}; \Gamma; \Delta) \not\models x : \alpha \wedge \beta$.

Case. $\varphi = \alpha \vee \beta$. Suppose $F(\alpha \vee \beta) \in \text{Sfor}(x)$. Then, $x : \alpha \vee \beta \in \Delta$. Hence, by clause (8) of the definition of saturated history, $x : \alpha \in \Delta$ and $x : \beta \in \Delta$. Therefore, $F(\alpha) \in \text{Sfor}(x)$ and $F(\beta) \in \text{Sfor}(x)$. By i.h., $\text{CM}(\Sigma; \mathbb{M}; \Gamma; \Delta) \not\models x : \alpha$ and $\text{CM}(\Sigma; \mathbb{M}; \Gamma; \Delta) \not\models x : \beta$. By definition of $\models$, we have $\text{CM}(\Sigma; \mathbb{M}; \Gamma; \Delta) \not\models x : \alpha \vee \beta$.

Case. $\varphi = \alpha \to \beta$. Suppose $F(\alpha \to \beta) \in \text{Sfor}(x)$. This implies, by definition of Sfor, that $x : \alpha \to \beta \in \Delta$. By clause (10) of the definition of saturated history, we have that either:

1) There is a y such that $x \leq y \in \mathbb{M}$, $y : \alpha \in \Gamma$ and $y : \beta \in \Delta$ or
2) There is a y such that $y \neq x$, $y \ll x$ and $x \preccurlyeq y$.

If (a) holds, then by the i.h., $\text{CM}(\Sigma; \mathbb{M}; \Gamma; \Delta) \models y : \alpha$ and $\text{CM}(\Sigma; \mathbb{M}; \Gamma; \Delta) \not\models y : \beta$. Further, $x \leq y$, so $\text{CM}(\Sigma; \mathbb{M}; \Gamma; \Delta) \not\models x : \alpha \to \beta$.

If (b) holds, then since $x \preccurlyeq y$, $F(\alpha \to \beta) \in \text{Sfor}(y)$. By the i.h. on the world y, which is strictly smaller than x in the relation $\ll$ (since $y \neq x$), it follows that $\text{CM}(\Sigma; \mathbb{M}; \Gamma; \Delta) \not\models y : \alpha \to \beta$. Note that in $\text{CM}(\Sigma; \mathbb{M}; \Gamma; \Delta)$, $x \leq y$. So, by Lemma 5, $\text{CM}(\Sigma; \mathbb{M}; \Gamma; \Delta) \not\models x : \alpha \to \beta$, as required.

Case. $\varphi = A$ says α. Suppose $F(A \text{ says } \alpha) \in \text{Sfor}(x)$. This implies, by definition of Sfor that $x : A \text{ says } \alpha \in \Delta$. By clause (12) of the definition of saturated history, we have that either:

(a) There is a y such that $xS_Ay \in \mathbb{M}$ and $y : \alpha \in \Delta$ or
(b) There is a y such that $y \neq x$, $y \ll x$ and $x \preccurlyeq y$.

If (a) holds, then by the i.h., $\text{CM}(\Sigma; \mathbb{M}; \Gamma; \Delta) \not\models y : \alpha$. Since xS_Ay, it immediately follows that $\text{CM}(\Sigma; \mathbb{M}; \Gamma; \Delta) \not\models x : A \text{ says } \alpha$.

If (b) holds, then since $x \preccurlyeq y$, $F(A \text{ says } \alpha) \in \text{Sfor}(y)$. By the i.h. on the world y, which is strictly smaller in the order $\ll$ (since $x \neq y$), it follows that $\text{CM}(\Sigma; \mathbb{M}; \Gamma; \Delta) \not\models y : A \text{ says } \alpha$. Since in $\text{CM}(\Sigma; \mathbb{M}; \Gamma; \Delta)$ we have $x \leq y$, Lemma 5 immediately implies $\text{CM}(\Sigma; \mathbb{M}; \Gamma; \Delta) \not\models x : A \text{ says } \alpha$, as required.

Case. $\varphi = A$ sf B. Suppose $F(A \text{ sf } B) \in \text{Sfor}(x)$. Hence, $x : A \text{ sf } B \in \Delta$. By clause (13) of definition of saturated history, $x : A \text{ sf } B \notin \Gamma$. Hence, from the definition of $\text{CM}(\Sigma; \mathbb{M}; \Gamma; \Delta)$, $x \notin sf(A, B)$. So, by definition of $\models$, we get that $\text{CM}(\Sigma; \mathbb{M}; \Gamma; \Delta) \not\models x : A \text{ sf } B$, as required. ■

B. SeqC_{CM}: *Countermodels for* BL_{sf}

We define an intermediate sequent calculus SeqC_{CM}, written $\Rightarrow_{\text{CM}}$, which uses the notion of saturated histories to emit countermodels from unprovable sequents. Although this calculus is not a decision procedure, we find it a useful step in proving several results, including the correctness of the terminating calculus SeqC_{T} as well as the results on saturation.

Sequents of SeqC_{CM} have the form $\Sigma; \mathbb{M}; \Gamma \Rightarrow_{\text{CM}} \Delta \searrow S$, where S is a finite set of finite models. We write $\vdash (\Sigma; \mathbb{M}; \Gamma \Rightarrow_{\text{CM}} \Delta \searrow S)$ if $\Sigma; \mathbb{M}; \Gamma \Rightarrow_{\text{CM}} \Delta \searrow S$ has a proof. The meaning of $\Sigma; \mathbb{M}; \Gamma \Rightarrow_{\text{CM}} \Delta \searrow S$ depends on S. If $\vdash (\Sigma; \mathbb{M}; \Gamma \Rightarrow_{\text{CM}} \Delta \searrow \{\})$, then $\vdash (\Sigma; \mathbb{M}; \Gamma \Rightarrow \Delta)$ and if $\vdash (\Sigma; \mathbb{M}; \Gamma \Rightarrow_{\text{CM}} \Delta \searrow S)$ with $S \neq \{\}$, then every model $\mathcal{M} \in S$ is a countermodel to $\Sigma; \mathbb{M}; \Gamma \Rightarrow \Delta$ in the sense of (the converse of) Definition 6.

Selected rules of the sequent calculus SeqC_{CM} are shown in Figure 4. First, every rule in the ordinary sequent calculus (Figure 1) is modified to have in the conclusion the union of the (counter)models in the premises. This is sound because the rules of the sequent calculus are invertible (i.e., the conclusion of each rule holds iff the premises hold). Second, there is a new rule (CM) that produces the countermodel $\text{CM}(\Sigma; \mathbb{M}; \Gamma; \Delta)$ when $\Sigma; \mathbb{M}; \Gamma; \Delta$ is a saturated history.

We emphasize again that this calculus is not necessarily a decision procedure because it includes all rules of $\Rightarrow$ and hence admits all of the latter's infinite backwards derivations as well.

Theorem 25 (Soundness 1)**.** *If* $\vdash (\Sigma; \mathbb{M}; \Gamma \Rightarrow_{CM} \Delta \searrow \{\})$*, then* $\vdash (\Sigma; \mathbb{M}; \Gamma \Rightarrow \Delta)$.

Proof: By induction on the given derivation of $\Sigma; \mathbb{M}; \Gamma \Rightarrow_{\text{CM}} \Delta \searrow \{\}$. Note that the case of rule (CM) does not apply because the set of countermodels in it is non-empty. The proof is straightforward because the rules of $\Rightarrow_{\text{CM}}$ mimic those of $\Rightarrow$. ∎

Theorem 26 (Soundness 2)**.** *If* $\vdash (\Sigma; \mathbb{M}; \Gamma \Rightarrow_{CM} \Delta \searrow S)$*, then for every model* $\mathcal{M} \in S$*,* $\mathcal{M} \not\models (\Sigma; \mathbb{M}; \Gamma \Rightarrow \Delta)$.

Proof: By induction on the given derivation of $\Sigma; \mathbb{M}; \Gamma \Rightarrow_{\text{CM}} \Delta \searrow S$ and case analysis of its last rule. For all other rules, except (CM), we simply observe that contexts in all major premises are a superset of corresponding contexts in the conclusion and hence we can trivially conclude by induction on one of the premises. The case of rule (CM) is immediate from Corollary 13. ∎

C. Proofs from Section III-B

Lemma 27 (Correctness of CM)**.** *Let* Σ*,* $\mathbb{M}$*,* Γ *and* Δ *be such that* $\mathbb{M}$ *is tree-like and no rule except (CM) applies backwards to* $\Sigma; \mathbb{M}; \Gamma \Rightarrow_T \Delta \searrow \ldots$*. Then,* $\Sigma; \mathbb{M}; \Gamma; \Delta$ *is a saturated history.*

Proof: We verify all conditions in the definition of a saturated history. Each condition corresponds to the negation of premises of one of the rules of SeqC_{T}. ∎

Lemma 28 (Tree-like $\mathbb{M}$)**.** *Let* $\mathbb{M}$ *be tree-like. Then, the* $\mathbb{M}'$ *in any sequent* $\Sigma'; \mathbb{M}'; \Gamma' \Rightarrow_T \Delta' \searrow \ldots$ *appearing in a backwards search starting from* $\Sigma; \mathbb{M}; \Gamma \Rightarrow_T \Delta \searrow \ldots$ *is tree-like.*

Proof: By backwards analysis of each rule observing that the $\mathbb{M}$ in the premises of each rule is tree-like if that in the conclusion is. ∎

Note that the underlying tree of $\mathbb{M}$ in any sequent of a backward proof search starting from a single formula consists of exactly those edges that are introduced in one of the rules ($\rightarrow$R) and (saysR).

Theorem 29 (Termination, Theorem 14)**.** *The following hold:*

1) *Any backwards derivation in* SeqC_{T} *starting from a sequent* $\Sigma; \mathbb{M}; \Gamma \Rightarrow_T \Delta$ *with* $\mathbb{M}$ *tree-like terminates.*
2) *For any* $\Sigma; \mathbb{M}; \Gamma; \Delta$ *with* $\mathbb{M}$ *tree-like, there is an* S *such that* $\vdash (\Sigma; \mathbb{M}; \Gamma \Rightarrow_T \Delta \searrow S)$ *and such an* S *can be finitely computed.*

Proof: Proof of (1): Suppose, for the sake of contradiction, that there is an infinite backward proof starting from $\Sigma; \mathbb{M}; \Gamma \Rightarrow_{\text{T}} \Delta \searrow \ldots$. Since the proof is finitely branching (every rule has a bounded number of premises), it must have an infinite path. Observe that $\mathbb{M}, \Gamma, \Delta$ are monotonic backwards, so the applicability conditions in the rules prevent application of the same rule on the same principal *labeled formula* more than once in any branch. Since there are only a finite number of formulas that can appear in any search (weak subformula property, Theorem 8), it follows that in the infinite path there must be an infinite number of labels. Let T be the underlying tree of this entire path (i.e., the underlying tree of the union of $\mathbb{M}$ for each sequent on this path). Since the tree is finitely branching (because we cannot apply rules ($\rightarrow$R) and (saysR) to the same label infinitely often), it must have an infinite path. Let this path be $x_0 \ll x_1 \ll \ldots$. Let S_i be the value of $\text{Sfor}(x_i)$ when either of the rules ($\rightarrow$R) and (saysR) is applied to create x_{i+1}. Note that for $i < j$, $S_i \not\supseteq S_j$, because if $S_i \supseteq S_j$, then at the time that x_{j+1} is created, $\text{Sfor}(x_i) \supseteq S_i \supseteq S_j = \text{Sfor}(x_j)$, so the application of the rules ($\rightarrow$R) and (saysR) on x_j would be blocked, so x_{j+1} could not have been created. Hence, for $i < j$, $S_i \not\supseteq S_j$. Call this fact (A). (The reader may note that the deduction $\text{Sfor}(x_i) \supseteq S_i$ two sentences ago relies on the fact that $\text{Sfor}(x)$ increases monotonically as we move backwards in a derivation.)

If Φ is the set of all subformulas of the original sequent we start from, together with formulas of the form A sf B where A, B are in the sequent, then by Theorem 8, each $S_i \subseteq \{T(\alpha) \mid \alpha \in \Phi\} \cup \{F(\alpha) \mid \alpha \in \Phi\}$. Note that the right hand side is a finite set, so its subsets form a finite partial order under set inclusion. Call this partial order P. Since P is finite, it has a finite number of chains and since the sequence $S_1, S_2, \ldots$ is infinite, at least one infinite subsequence R of $S_1, S_2, \ldots$ must contain elements from only a single chain in P. Consider any two elements $S_i, S_j \in P$ with $i < j$. Since P is a chain, we must have either $S_i \supseteq S_j$ or $S_i \subsetneq S_j$.

Axiom Rules

$$\frac{\Sigma; \mathbb{M}; \Gamma; \Delta \text{ is a saturated history}}{\Sigma; \mathbb{M}; \Gamma \Rightarrow_{\text{CM}} \Delta \searrow \{\text{CM}(\Sigma; \mathbb{M}; \Gamma; \Delta)\}}\text{CM} \qquad \frac{}{\Sigma; \mathbb{M}, x \leq y; \Gamma, x : p \Rightarrow_{\text{CM}} y : p, \Delta \searrow \{\}}\text{init}$$

$$\frac{}{\Sigma; \mathbb{M}; \Gamma, x : A \mathsf{\ sf\ } B \Rightarrow_{\text{CM}} x : A \mathsf{\ sf\ } B, \Delta \searrow \{\}}\text{sf}$$

Logical Rules

$$\frac{\Sigma; \mathbb{M}; \Gamma \Rightarrow_{\text{CM}} x : \alpha, x : \alpha \wedge \beta, \Delta \searrow S_1 \qquad \Sigma; \mathbb{M}; \Gamma \Rightarrow_{\text{CM}} x : \beta, x : \alpha \wedge \beta, \Delta \searrow S_2}{\Sigma; \mathbb{M}; \Gamma \Rightarrow_{\text{CM}} x : \alpha \wedge \beta, \Delta \searrow S_1 \cup S_2}\wedge\text{R}$$

$$\frac{\Sigma, y; \mathbb{M}, x \leq y; \Gamma, y : \alpha \Rightarrow_{\text{CM}} y : \beta, x : \alpha \to \beta, \Delta \searrow S}{\Sigma; \mathbb{M}; \Gamma \Rightarrow_{\text{CM}} x : \alpha \to \beta, \Delta \searrow S}\to\text{R}$$

$$\frac{\Sigma; \mathbb{M}, x \leq y; \Gamma, x : \alpha \to \beta \Rightarrow_{\text{CM}} y : \alpha, \Delta \searrow S_1 \qquad \Sigma; \mathbb{M}, x \leq y; \Gamma, x : \alpha \to \beta, y : \beta \Rightarrow_{\text{CM}} \Delta \searrow S_2}{\Sigma; \mathbb{M}, x \leq y; \Gamma, x : \alpha \to \beta \Rightarrow_{\text{CM}} \Delta \searrow S_1 \cup S_2}\to\text{L}$$

$$\frac{\Sigma, y; \mathbb{M}, xS_Ay; \Gamma \Rightarrow_{\text{CM}} y : \alpha, x : A \mathsf{\ says\ } \alpha, \Delta \searrow S}{\Sigma; \mathbb{M}; \Gamma \Rightarrow_{\text{CM}} x : A \mathsf{\ says\ } \alpha, \Delta \searrow S}\text{saysR} \qquad \frac{\Sigma; \mathbb{M}, xS_Ay; \Gamma, x : A \mathsf{\ says\ } \alpha, y : \alpha \Rightarrow_{\text{CM}} \Delta \searrow S}{\Sigma; \mathbb{M}, xS_Ay; \Gamma, x : A \mathsf{\ says\ } \alpha \Rightarrow_{\text{CM}} \Delta \searrow S}\text{saysL}$$

Frame Rules

$$\frac{\Sigma; \mathbb{M}, x \leq y, yS_Az, xS_Az; \Gamma \Rightarrow_{\text{CM}} \Delta \searrow S}{\Sigma; \mathbb{M}, x \leq y, yS_Az; \Gamma \Rightarrow_{\text{CM}} \Delta \searrow S}\text{mon-S} \qquad \frac{\Sigma; \mathbb{M}, xS_By, yS_Az, xS_Az; \Gamma \Rightarrow_{\text{CM}} \Delta \searrow S}{\Sigma; \mathbb{M}, xS_By, yS_Az; \Gamma \Rightarrow_{\text{CM}} \Delta \searrow S}\text{I}$$

$$\frac{\Sigma; \mathbb{M}, xS_By, xS_Ay; \Gamma, x : A \mathsf{\ sf\ } B \Rightarrow_{\text{CM}} \Delta \searrow S}{\Sigma; \mathbb{M}, xS_By; \Gamma, x : A \mathsf{\ sf\ } B \Rightarrow_{\text{CM}} \Delta \searrow S}\text{basic-sf}$$

Fig. 4. SeqC$_{\text{CM}}$: Countermodel producing sequent calculus for BL$_{\text{sf}}$, selected rules

The former is ruled out fact (A). So $S_i \subsetneq S_j$. Hence, we have $S_1 \subsetneq S_2 \subsetneq S_3 \ldots$, so the chain P contains an infinite ascending sequence, which is a contradiction because P is finite.

Proof of (2): Follows immediately from (1), Lemma 28, and the observation that all applicability conditions are finitely computable. ∎

Lemma 30 (Simulation)**.** *If $\mathbb{M}$ is tree-like and $\vdash (\Sigma; \mathbb{M}; \Gamma \Rightarrow_T \Delta \searrow S)$, then $\vdash (\Sigma; \mathbb{M}; \Gamma \Rightarrow_{CM} \Delta \searrow S)$.*

Proof: By induction on the given derivation of $\Sigma; \mathbb{M}; \Gamma \Rightarrow_{\text{T}} \Delta \searrow S$. The case of rule (CM) follows from Lemma 27. The rest of the cases are immediate from the i.h. The only fact to take care of is that the tree-like property holds for each i.h. application. This follows from Lemma 28. ∎

Theorem 31 (Correctness, Theorem 15)**.** *For a tree-like $\mathbb{M}$, suppose that S is such that $\vdash (\Sigma; \mathbb{M}; \Gamma \Rightarrow_T \Delta \searrow S)$ (such an S must exist and can be computed using Theorem 29). Then:*

1) *If $S = \{\}$, then $\models (\Sigma; \mathbb{M}; \Gamma \Rightarrow \Delta)$.*
2) *If $S \neq \{\}$, then every model $\mathcal{M}$ in S is a countermodel to the sequent, i.e., $\mathcal{M} \not\models (\Sigma; \mathbb{M}; \Gamma \Rightarrow \Delta)$.*

Proof: By Lemma 30, we have that $\vdash (\Sigma; \mathbb{M}; \Gamma \Rightarrow_{\text{CM}} \Delta \searrow S)$. Now, (1) follows from Theorems 25 and 7 and (2) follows from Theorem 26. ∎

D. Proofs from Section IV

Lemma 32 (Comprehensiveness 1)**.** *Suppose $\vdash (\Sigma; \mathbb{M}; \Gamma \Rightarrow_{CM} \Delta \searrow S)$. Suppose x and p are such that $\forall \mathcal{M} \in S.\ \mathcal{M} \models x : p$. Then, $\vdash (\Sigma; \mathbb{M}; \Gamma \Rightarrow_{CM} x : p, \Delta \searrow \{\})$.*

Proof: By induction on the given derivation of $\Sigma; \mathbb{M}; \Gamma \Rightarrow_{\text{CM}} \Delta \searrow S$ and case analysis of its last rule (the rules are listed in Figure 4). Representative cases are shown below:

Case. $\dfrac{\Sigma; \mathbb{M}; \Gamma; \Delta \text{ is a saturated history}}{\Sigma; \mathbb{M}; \Gamma \Rightarrow_{\text{CM}} \Delta \searrow \{\text{CM}(\Sigma; \mathbb{M}; \Gamma; \Delta)\}}\text{CM}$

Here $S = \{\text{CM}(\Sigma; \mathbb{M}; \Gamma; \Delta)\}$. The given condition $\forall \mathcal{M} \in S.\ \mathcal{M} \models x : p$ implies (by definition of CM) that there is a z such that $z \leq x$ and $z : p \in \Gamma$. Therefore, by rule (init), $\vdash (\Sigma; \mathbb{M}; \Gamma \Rightarrow_{\text{CM}} x : p, \Delta \searrow \{\})$, as required.

Case. $\dfrac{}{\Sigma; \mathbb{M}, y' \leq y; \Gamma, y' : q \Rightarrow_{\text{CM}} y : q, \Delta \searrow \{\}}\text{init}$

By rule (init), we have $\vdash (\Sigma; \mathbb{M}, y' \leq y; \Gamma, y' : q \Rightarrow_{\text{CM}} x : p, y : q, \Delta \searrow \{\})$, which is what we need to prove.

Case. $\dfrac{\Sigma;\mathbb{M};\Gamma \Rightarrow_{\text{CM}} y:\alpha, y:\alpha\wedge\beta, \Delta \searrow S_1 \quad \Sigma;\mathbb{M};\Gamma \Rightarrow_{\text{CM}} y:\beta, y:\alpha\wedge\beta, \Delta \searrow S_2}{\Sigma;\mathbb{M};\Gamma \Rightarrow_{\text{CM}} y:\alpha\wedge\beta, \Delta \searrow S_1 \cup S_2}\wedge\text{R}$

Here, $S = S_1 \cup S_2$. We are given that $\forall\mathcal{M} \in (S_1 \cup S_2).\ \mathcal{M} \models x:p$.

1) $\forall\mathcal{M} \in S_1.\ \mathcal{M} \models x:p$ (From assumption $\forall\mathcal{M} \in (S_1 \cup S_2).\ \mathcal{M} \models x:p$)
2) $\vdash (\Sigma;\mathbb{M};\Gamma \Rightarrow_{\text{CM}} x:p, y:\alpha, y:\alpha\wedge\beta, \Delta \searrow \{\})$ (i.h. on 1st premise and (1))
3) $\forall\mathcal{M} \in S_2.\ \mathcal{M} \models x:p$ (From assumption $\forall\mathcal{M} \in (S_1 \cup S_2).\ \mathcal{M} \models x:p$)
4) $\vdash (\Sigma;\mathbb{M};\Gamma \Rightarrow_{\text{CM}} x:p, y:\beta, y:\alpha\wedge\beta, \Delta \searrow \{\})$ (i.h. on 2nd premise and (2))
5) $\vdash (\Sigma;\mathbb{M};\Gamma \Rightarrow_{\text{CM}} x:p, y:\alpha\wedge\beta, \Delta \searrow \{\})$ (Rule ($\wedge$R) on 2,4)

■

Lemma 33 (Comprehensiveness 2)**.** *Suppose* $\vdash (\Sigma;\mathbb{M};\Gamma \Rightarrow_{CM} \Delta \searrow S)$. *Suppose* x *and* p *are such that* $\vdash (\Sigma;\mathbb{M};\Gamma \Rightarrow_{CM} x:p, \Delta \searrow \{\})$. *Then,* $\forall\mathcal{M} \in S.\ \mathcal{M} \models x:p$.

Proof: Suppose $\mathcal{M} \in S$. From Theorem 26, we know that (1) $\forall w, w' \in \Sigma.\ (wRw' \in \mathbb{M}) \Rightarrow (wRw' \in \mathcal{M})$, (2) $\forall(w:\varphi) \in \Gamma.\ \mathcal{M} \models w:\varphi$ and (3) $\forall(w:\varphi) \in \Delta.\ \mathcal{M} \not\models w:\varphi$. By Theorem 25 applied to the assumption $\vdash (\Sigma;\mathbb{M};\Gamma \Rightarrow_{\text{CM}} x:p, \Delta \searrow \{\})$, we know that $\vdash (\Sigma;\mathbb{M};\Gamma \Rightarrow x:p, \Delta)$. Applying Theorem 7, we get that $\mathcal{M}, \rho \models (\Sigma;\mathbb{M};\Gamma \Rightarrow x:p, \Delta)$ for every ρ and, in particular, for $\rho(x) = x$. Using (1)–(3) and the definition of $\models$ on sequents, we immediately get $\mathcal{M} \models x:p$, as required. ■

Theorem 34 (Comprehensiveness, Theorem 18)**.** *Suppose* $\mathbb{M}$ *is tree-like and* $\vdash (\Sigma;\mathbb{M};\Gamma \Rightarrow_T \Delta \searrow S)$. *Then* $\vdash (\Sigma;\mathbb{M};\Gamma \Rightarrow x:p, \Delta)$ *iff* $\forall\mathcal{M} \in S.\ \mathcal{M} \models x:p$.

Proof: If $\vdash (\Sigma;\mathbb{M};\Gamma \Rightarrow_{\text{T}} \Delta \searrow S)$, then by Lemma 30, $\vdash (\Sigma;\mathbb{M};\Gamma \Rightarrow_{\text{CM}} \Delta \searrow S)$.

Suppose $\vdash (\Sigma;\mathbb{M};\Gamma \Rightarrow x:p, \Delta)$. Then, by Theorems 29 and 31, $\vdash (\Sigma;\mathbb{M};\Gamma \Rightarrow_{\text{T}} x:p, \Delta \searrow \{\})$. By Lemma 30, $\vdash (\Sigma;\mathbb{M};\Gamma \Rightarrow_{\text{CM}} x:p, \Delta \searrow \{\})$. By Lemma 33, $\forall\mathcal{M} \in S.\ \mathcal{M} \models x:p$.

Conversely, suppose that $\forall\mathcal{M} \in S.\ \mathcal{M} \models x:p$. By Lemma 32, $\vdash (\Sigma;\mathbb{M};\Gamma \Rightarrow_{\text{CM}} x:p, \Delta \searrow \{\})$. By Theorem 25, $\vdash (\Sigma;\mathbb{M};\Gamma \Rightarrow x:p, \Delta)$. ■

E. Proofs from Section V

Theorem 35 (Soundness, Theorem 20)**.** *If* $\vdash (\Sigma;\mathbb{M};\Gamma \Rightarrow_A \Delta \searrow \Theta)$ *and* $F \models \Theta$, *then* $\vdash (\Sigma;\mathbb{M};\Gamma, \mathit{root}(\mathbb{M}) : F \Rightarrow \Delta)$.

Proof: By induction on the given derivation of $\Sigma;\mathbb{M};\Gamma \Rightarrow_{\text{A}} \Delta \searrow \Theta$ and case analysis of its last rule. There is only one interesting case, that of the rule (AB).

Case. $\dfrac{\text{No other rule applies}}{\Sigma;\mathbb{M};\Gamma \Rightarrow_{\text{A}} \Delta \searrow \text{AB}(\Sigma;\mathbb{M};\Gamma;\Delta)}\text{AB}$

By definition, we know that

$$\begin{gathered}\text{AB}(\Sigma;\mathbb{M};\Gamma;\Delta) \ = \\ (\bigvee\{p \mid y:p \in \Delta \text{ and } (\text{root}(\mathbb{M})) \leq y \in \mathbb{M}\}) \vee \\ (\bigvee\{A \text{ says } p \mid y:p \in \Delta \text{ and } (\text{root}(\mathbb{M}))S_A y \in \mathbb{M}\})\end{gathered}$$

We are given that $F \models \text{AB}(\Sigma;\mathbb{M};\Gamma;\Delta)$, so one of the following must be true:

1) There is a $y:p \in \Delta$, $(\text{root}(\mathbb{M})) \leq y \in \mathbb{M}$ and $p \in F$: Then, $\Sigma;\mathbb{M};\Gamma, \text{root}(\mathbb{M}) : F \Rightarrow \Delta$ by rule (init).
2) There is a $y : p \in \Delta$, $(\text{root}(\mathbb{M}))S_A y \in \mathbb{M}$ and $(A \text{ says } p) \in F$: Then, we have can complete a proof of $\Sigma;\mathbb{M};\Gamma, \text{root}(\mathbb{M}) : F \Rightarrow \Delta$ as follows:
   a) $\Sigma;\mathbb{M};\Gamma, \text{root}(\mathbb{M}) : F, y:p \Rightarrow \Delta$ (Rule (init))
   b) $\Sigma;\mathbb{M};\Gamma, \text{root}(\mathbb{M}) : F \Rightarrow \Delta$ (Rule (saysL))

   The rule (saysL) in step (b) is correct because $(A \text{ says } p) \in F$ and $(\text{root}(\mathbb{M}))S_A y \in \mathbb{M}$.

■