Kripke Semantics for BL_0 and BL
Technical report

Marcos Cramer, Deepak Garg

May 28, 2017

Abstract

We describe Kripke semantics for the access control logics BL_0 and BL, developed by Garg and Pfenning [6, 7].

1 BL_0: An Authorization Logic

BL_0 extends first-order intuitionistic logic with a modality $k \;\mathsf{says}\; s$, which means that principal k states, claims, or believes that formula s is true. Predicates P express relations between terms that are either ground constants a, bound variables x, or applications of uninterpreted function symbols f to ground terms. Terms are classified into sorts σ (sometimes called types) by the relation $\Sigma \vdash t : \sigma$, where Σ is a sorting for parameters in t. (The signature of the logic, Ψ that defines the sorts and arities of predicates and function symbols is left implicit throughout.) We stipulate at least one sort $\mathsf{principal}$ whose elements are represented by the letter k. Formulas s may either be atomic (p, q) or they may be constructed using the usual connectives of predicate logic and the special connective $k \;\mathsf{says}\; s$.

$$
\begin{array}{llll}
\text{Sorts} & \sigma & ::= & \mathsf{principal} \mid \ldots \\
\text{Terms} & t, k, i & ::= & a \mid x \mid f(t_1, \ldots, t_n) \mid \ell \\
\text{Predicates} & P & & \\
\text{Atoms} & p, q & ::= & P(t_1, \ldots, t_n) \\
\text{Constraints} & c & ::= & k_1 \succeq k_2 \\
\text{Formulas} & r, s & ::= & p \mid r \wedge s \mid r \vee s \mid r \supset s \mid \top \mid \bot \mid \forall x{:}\sigma.s \mid \exists x{:}\sigma.s \mid k \;\mathsf{says}\; s
\end{array}
$$

The proof system of BL_0 uses an unstipulated judgment $\Sigma \rhd c$, where Σ is possibly infinite. This judgment must satisfy the following requirements.

$$\Sigma \rhd k \succeq k \qquad \text{(C-refl)}$$

$$\Sigma \rhd k \succeq k' \text{ and } \Sigma \rhd k' \succeq k'' \text{ imply } \Sigma \rhd k \succeq k'' \qquad \text{(C-trans)}$$

$$\Sigma \rhd \ell \succeq k \qquad \text{(C-loca)}$$

$$\Sigma, x{:}\sigma \rhd c \text{ and } \Sigma \vdash t : \sigma \text{ imply } \Sigma \rhd c[t/x] \qquad \text{(C-subst)}$$

$$\Sigma, x{:}\sigma \rhd c \text{ and } x \notin c \text{ imply } \Sigma \rhd c \qquad \text{(C-strengthen)}$$

$$\text{If } \Sigma \rhd c \text{ and } \Sigma \subseteq \Sigma', \text{ then } \Sigma' \rhd c \qquad \text{(C-weaken)}$$

Axiomatic proof system. The primary proof system that we need for proof search is a sequent calculus. However before presenting that, we briefly describe an axiomatic proof system for BL$_0$. This proof system is obtained by extending any axiomatization of first-order intuitionistic logic with the following axioms and rules for says.

$$\begin{array}{ll} \dfrac{\Sigma \vdash s}{\Sigma \vdash k \text{ says } s} & \text{(N)} \\ \Sigma \vdash (k \text{ says } (s_1 \supset s_2)) \supset ((k \text{ says } s_1) \supset (k \text{ says } s_2)) & \text{(K)} \\ \Sigma \vdash (k \text{ says } s) \supset k' \text{ says } k \text{ says } s & \text{(I)} \\ \Sigma \vdash k \text{ says } ((k \text{ says } s) \supset s) & \text{(C)} \\ \Sigma \vdash (k' \text{ says } s) \supset k \text{ says } s \text{ if } (\Sigma \rhd k' \succeq k) & \text{(S)} \end{array}$$

Rule (N) means that each principal states at least all tautologies. Axiom (K) means that the statements of each principal are closed under implication. Together they imply that each (k says $\cdot$) is a *normal* modality (see e.g., [5]). Axiom (I) was first suggested in the context of access control by Abadi [1]. It means that statements of any principal k can be injected into the belief system of any another principal. Axiom (C) or *conceit* states that every principal k believes that each of its statements is true. (S) means that statements of each principal are believed by all weaker principals. In particular, (ℓ says s) $\supset$ k says s for each k and s.

This choice of axioms for says is quite different from any of the existing authorization logics, and has been developed to make logic programming simpler.

1.1 Sequent Calculus

Next, we develop a sequent calculus for BL$_0$, which we later use as the basis for proof search. We follow the judgmental method [4, 9], introducing a separate category of judgments that are established by deductions. For BL$_0$, we need two judgments: s true meaning that formula s is provable in the current context, and k claims s meaning that principal k believes that s must be the case. (k claims s) is logically equivalent to (k says s) true. We often abbreviate s true to s. Using the judgmental method makes the technical development easier, especially the proof of cut-elimination.

$$\begin{array}{llll} \text{Judgments} & J & ::= & s \text{ true} \mid k \text{ claims } s \\ \text{Sorting} & \Sigma & ::= & a_1{:}\sigma_1 \ldots a_n{:}\sigma_n \\ \text{Hypotheses} & \Gamma & ::= & J_1 \ldots J_n \qquad (n \geq 0) \\ \text{Sequent} & & & \Sigma; \Gamma \xrightarrow{k} s \text{ true} \end{array}$$

Sequents in BL$_0$ have the form $\Sigma; \Gamma \xrightarrow{k} s$ true. Σ is a map from term constants occurring in the sequent to their sorts, and Γ is the set of assumed judgments (hypotheses). The novelty here is the principal k on the sequent symbol, which we call the *context* of the sequent.[1] The context represents the principal relative to whose beliefs the reasoning is being performed. It affects provability in the following manner: while reasoning in context k, an assumption of the form k' claims s entails s true if $k' \succeq k$ (in particular, k claims s entails s true). This entailment does not hold in general.

The rules of our sequent calculus are summarized in Figure 1. As usual, we have left and right rules for each connective. For common connectives, the rules resemble those in intuitionistic logic, with the exception of the associated context, which remains unchanged. The judgment $\Sigma \vdash t{:}\sigma$ means that the term t has sort σ. We restrict the (init) rule to atomic formulas only. This is merely a technical convenience because we prove later that $\Sigma; \Gamma, s \xrightarrow{k} s$ for arbitrary s. Rule (claims) enforces the meaning of contexts as described above by allowing k claims s on the left to be promoted to s if the context k_0 is weaker than k.

(saysR) is the only rule which changes the context of a sequent. The notation $\Gamma|$ in this rule denotes the subset of Γ that contains exactly the claims of principals, i.e., the set $\{(k' \ \mathsf{claims}\ s') \in \Gamma\}$. The rule means that k says s is true in any context k_0 if s is true in context k using only claims of principals. Truth assumptions in Γ are eliminated in the premise because they may have been added in the context k_0 (using the rules (claims) and ($\supset$R)), but may not hold in the context k. The left rule (saysL) changes the judgment (k says s) true to the equivalent judgment k claims s.

Meta-theory. We prove two important meta-theorems about this sequent calculus: admissibility of the cut rule and the identity principle. In addition, common structural theorems such as weakening and strengthening of hypotheses are also provable, but we do not state them explicitly.

Theorem 1.1 (Identity)**.** *$\Sigma; \Gamma, s \xrightarrow{k} s$ for each s.*

Proof. By induction on s. □

Theorem 1.2 (Admissibility of cut)**.** *The following hold*

1. *$\Sigma; \Gamma \xrightarrow{k} s$ and $\Sigma; \Gamma, s \xrightarrow{k} r$ imply $\Sigma; \Gamma \xrightarrow{k} r$*
2. *$\Sigma; \Gamma| \xrightarrow{k} s$ and $\Sigma; \Gamma, k\ \mathsf{claims}\ s \xrightarrow{k_0} r$ imply $\Sigma; \Gamma \xrightarrow{k_0} r$*

Proof. By simultaneous lexicographic induction, first on the size of the cut formula, and then on the sizes of the two given derivations, as in [8]. □

Finally, we prove an equivalence between the axiomatic system and the sequent calculus.

Theorem 1.3 (Equivalence)**.** *$\Sigma; \cdot \xrightarrow{k} s$ in the sequent calculus if and only if $\Sigma \vdash k\ \mathsf{says}\ s$ in the axiomatic system.*

[1] Often in literature, context is used to refer to Γ. However, we consistently use context for k and hypotheses for Γ.

$$\frac{}{\Sigma;\Gamma, p \xrightarrow{k} p}\text{init} \qquad \frac{\Sigma \rhd k \succeq k_0 \qquad \Sigma;\Gamma, k\ \mathsf{claims}\ s, s \xrightarrow{k_0} r}{\Sigma;\Gamma, k\ \mathsf{claims}\ s \xrightarrow{k_0} r}\text{claims}$$

$$\frac{\Sigma;\Gamma| \xrightarrow{k} s}{\Sigma;\Gamma \xrightarrow{k_0} k\ \mathsf{says}\ s}\mathsf{saysR} \qquad \frac{\Sigma;\Gamma, k\ \mathsf{says}\ s, k\ \mathsf{claims}\ s \xrightarrow{k_0} r}{\Sigma;\Gamma, k\ \mathsf{says}\ s \xrightarrow{k_0} r}\mathsf{saysL}$$

$$\frac{\Sigma;\Gamma \xrightarrow{k} s \qquad \Sigma;\Gamma \xrightarrow{k} s'}{\Sigma;\Gamma \xrightarrow{k} s \wedge s'}\wedge\text{R} \qquad \frac{\Sigma;\Gamma, s \wedge s', s, s' \xrightarrow{k} r}{\Sigma;\Gamma, s \wedge s' \xrightarrow{k} r}\wedge\text{L}$$

$$\frac{\Sigma;\Gamma \xrightarrow{k} s}{\Sigma;\Gamma \xrightarrow{k} s \vee s'}\vee\ \text{R}_1 \qquad \frac{\Sigma;\Gamma \xrightarrow{k} s'}{\Sigma;\Gamma \xrightarrow{k} s \vee s'}\vee\ \text{R}_2 \qquad \frac{\Sigma;\Gamma, s \vee s', s \xrightarrow{k} r \qquad \Sigma;\Gamma, s \vee s', s' \xrightarrow{k} r}{\Sigma;\Gamma, s \vee s' \xrightarrow{k} r}\vee\ \text{L}$$

$$\frac{}{\Sigma;\Gamma \xrightarrow{k} \top}\top\text{R} \qquad \frac{}{\Sigma;\Gamma, \bot \xrightarrow{k} r}\bot\text{L} \qquad \frac{\Sigma;\Gamma, s \xrightarrow{k} s'}{\Sigma;\Gamma \xrightarrow{k} s \supset s'}\supset\text{R}$$

$$\frac{\Sigma;\Gamma, s \supset s' \xrightarrow{k} s \qquad \Sigma;\Gamma, s \supset s', s' \xrightarrow{k} r}{\Sigma;\Gamma, s \supset s' \xrightarrow{k} r}\supset\text{L} \qquad \frac{\Sigma, x{:}\sigma;\Gamma \xrightarrow{k} s}{\Sigma;\Gamma \xrightarrow{k} \forall x{:}\sigma.s}\forall\text{R}$$

$$\frac{\Sigma;\Gamma, \forall x{:}\sigma.s, s[t/x] \xrightarrow{k} r \qquad \Sigma \vdash t{:}\sigma}{\Sigma;\Gamma, \forall x{:}\sigma.s \xrightarrow{k} r}\forall\text{L} \qquad \frac{\Sigma;\Gamma \xrightarrow{k} s[t/x] \qquad \Sigma \vdash t{:}\sigma}{\Sigma;\Gamma \xrightarrow{k} \exists x{:}\sigma.s}\exists\text{R}$$

$$\frac{\Sigma, x{:}\sigma;\Gamma, \exists x{:}\sigma.s, s \xrightarrow{k} r}{\Sigma;\Gamma, \exists x{:}\sigma.s \xrightarrow{k} r}\exists\text{L}$$

Figure 1: BL_0: sequent calculus

Proof. The "if" direction follows by a direct induction on axiomatic proofs. For the "only if" direction, we generalize the statement of the theorem to allow non-empty hypothesis: if $\Sigma;\Gamma \xrightarrow{k} s$, then $\Sigma \vdash k\ \mathsf{says}\ (\Gamma \supset s)$. Next, we generalize the axiomatic system to allow hypotheses. Finally, we induct on sequent derivations to show that they can be simulated in the generalized axiomatic system. Although tedious, this approach is standard. □

2 Kripke Semantics for BL_0

We define Kripke or frame semantics for BL_0. Our Kripke semantics are extend similar semantics for constructive S4 [2] with views. Further, we add a first-order structure. Formally, a Kripke structure $\mathcal{K}$ is a tuple $(W, \leq_i, \leq_s, D, \rho, \theta)$, where:

- W is a set of worlds. Worlds are denoted w.
- $\leq_i$ is a reflexive and transitive relation over W.
- $\leq_s$ is a reflexive and transitive relation over W. We require that:
  - (K-commute) If $w \leq_s \leq_i w'$ then $w \leq_s w'$.
- D is a map from worlds to (possibly infinite) sortings of fresh constants. (Note that the proof theory disallows infinite sortings Σ). We require that:
  - (K-fresh) If $a{:}\sigma \in D(w)$ then a not be in the logic's signature.
  - (K-grow1) If $w \leq_i w'$ then $D(w) \subseteq D(w')$.
  - (K-grow2) If $w \leq_s w'$ then $D(w) \subseteq D(w')$.
- ρ is a curried function: $\rho(w)(P)$ is a subset of tuples of terms (of the same arity and types as argument of predicate symbol P) over $D(w)$. We require that:
  - (K-mon) If $w \leq_i w'$ then for every P, $\rho(w)(P) \subseteq \rho(w')(P)$.
- θ is a *view function*: $\theta(w)$ is a set of terms of sort $\mathsf{principal}$ over $D(w)$. We require that:
  - (K-viewmon) $k \in \theta(w)$ and $w \leq_i w'$ imply $k \in \theta(w')$.
  - (K-viewcl) $k \in \theta(w)$ and $D(w) \rhd k' \succeq k$ imply $k' \in \theta(w)$.

2.1 Substitutions

We denote substitutions of variables by constants using the letter ν. Given a finite sorting Σ, a Kripke structure $\mathcal{K} = (W, \leq_i, \leq_s, D, \rho, \theta)$, a substitution ν and a world $w \in W$, we say that ν conforms to Σ and $\mathcal{K}$ at w, written $\Sigma \ll \nu : (\mathcal{K}, w)$, if:

- $x \in \mathtt{dom}(\nu)$ iff there is a σ such that $x{:}\sigma \in \Sigma$.
- For all $x{:}\sigma \in \Sigma$, $D(w) \vdash \nu(x) : \sigma$.

Lemma 2.1.

1. *If* $\Sigma \vdash t : \sigma$ *and* $\Sigma \ll \nu : (\mathcal{K}, w)$*, then* $D(w) \vdash t\nu : \sigma$*.*
2. *If* $\Sigma \vdash c\ \mathsf{ok}$ *and* $\Sigma \ll \nu : (\mathcal{K}, w)$*, then* $D(w) \vdash c\nu\ \mathsf{ok}$*.*

3. *If* $\Sigma \vdash s\ \mathsf{ok}$ *and* $\Sigma \ll \nu : (\mathcal{K}, w)$, *then* $D(w) \vdash s\nu\ \mathsf{ok}$.

Proof. By induction on t, c, and s respectively. □

The above Lemma is necessary to ensure that many statements in the definitions of satisfaction are well-typed.

Lemma 2.2. *If* $\Sigma \rhd c$ *and* $\Sigma \ll \nu : (\mathcal{K}, w)$ *then* $D(w) \rhd c\nu$.

Proof. Suppose $\Sigma \rhd c$ and $\Sigma \ll \nu : (\mathcal{K}, w)$. By Lemma 2.1, $D(w) \vdash c\nu\ \mathsf{ok}$, so the conclusion makes sense. From the assumption $\Sigma \rhd c$ and (C-weaken) we get $\Sigma, D(w) \rhd c$. By (C-subst) and (C-strenghten), $D(w) \rhd c\nu$. □

2.2 Satisfaction

Satisfaction for closed formulas. Next, we define satisfaction for closed formulas. Given a Kripke structure $\mathcal{K}$ and a world w, we define the relation $w \models s$ when $D(w) \vdash s\ \mathsf{ok}$ as follows:

- $w \models P(t_1, \ldots, t_n)$ iff $(t_1, \ldots, t_n) \in \rho(w)(P)$
- $w \models s_1 \wedge s_2$ iff $w \models s_1$ and $w \models s_2$
- $w \models s_1 \vee s_2$ iff $w \models s_1$ or $w \models s_2$
- $w \models s_1 \supset s_2$ iff for all w', $w \leq_i w'$ and $w' \models s_1$ imply $w' \models s_2$
- $w \models \top$ always
- $w \models \bot$ never
- $w \models \forall x{:}\sigma.s$ iff for all w', $w \leq_i w'$ and $D(w') \vdash t : \sigma$ imply $w' \models s[t/x]$
- $w \models \exists x{:}\sigma.s$ iff there is a t such that $D(w) \vdash t : \sigma$ and $w \models s[t/x]$
- $w \models k\ \mathsf{says}\ s$ iff for all w', $w \leq_i \leq_s w'$ and $k \in \theta(w')$ imply $w' \models s$

Satisfaction for closed judgments. We say that $w \models s\ \mathsf{true}$ iff $w \models s$, and say that $w \models k\ \mathsf{claims}\ s$ iff $w \models k\ \mathsf{says}\ s$.

Satisfaction for sequents. Given a Kripke structure $\mathcal{K}$, we say that $\mathcal{K} \models (\Sigma; \Gamma \xrightarrow{k} s)$ iff:

- For all $w \in \mathcal{K}$ and ν, $\Sigma \ll \nu : (\mathcal{K}, w)$, $k\nu \in \theta(w)$, and $w \models \Gamma\nu$ imply $w \models s\nu$

2.3 Soundness

We prove that the sequent calculus is sound with respect to the Kripke semantics. We start by proving a standard Lemma.

Lemma 2.3 (Monotonicity)**.** *If $w \models s$ and $w \leq_i w'$ then $w' \models s$.*

Proof. By induction on s and case analysis of the form of s.

Case. $s = P(t_1, \ldots, t_n)$. The condition $w \models s$ implies $(t_1, \ldots, t_n) \in \rho(w)(P)$. By (K-mon) and $w \leq_i w'$, we know that $\rho(w)(P) \subseteq \rho(w')(P)$. Hence, $(t_1, \ldots, t_n) \in \rho(w')(P)$ or, equivalently, $w' \models s$ as required.

Case. $s = s_1 \wedge s_2$. Suppose $w \models s$ and $w \leq_i w'$. Then, by definition of $\models$, $w \models s_1$ and $w \models s_2$. By i.h., $w' \models s_1$ and $w' \models s_2$. Hence, $w' \models s_1 \wedge s_2$ or, equivalently, $w' \models s$.

Case. $s = s_1 \vee s_2$. Suppose $w \models s$ and $w \leq_i w'$. Then, by definition of $\models$, either $w \models s_1$ or $w \models s_2$. Suppose $w \models s_1$ (the other case is symmetric). By i.h., $w' \models s_1$. Hence, $w' \models s_1 \vee s_2$ or, equivalently, $w' \models s$.

Case. $s = s_1 \supset s_2$. Suppose $w \models s_1 \supset s_2$ and $w \leq_i w'$. We want to show $w' \models s_1 \supset s_2$. To prove that, pick an arbitrary world w'' such that $w' \leq_i w''$. It suffices to prove that $w'' \models s_1$ implies $w'' \models s_2$. However, observe that $w \leq_i w' \leq_i w''$, so $w \leq_i w''$. By definition of satisfaction on the assumption $w \models s_1 \supset s_2$, we get that $w'' \models s_1$ implies $w'' \models s_2$, as required.

Case. $s = \top$. Then $w' \models s$ follows by definition of $\models$.

Case. $s = \bot$. Here $w' \models s$ vacuously because the assumption $w \models s$ is false by definition of $\models$.

Case. $s = \forall x{:}\sigma.s_1$. Suppose $w \models \forall x{:}\sigma.s_1$ and $w \leq_i w'$. We want to show that $w' \models \forall x{:}\sigma.s_1$. Following the definition of $\models$, pick a world w'' and a t such that $w' \leq_i w''$ and $D(w'') \vdash t : \sigma$. It suffices to show that $w'' \models s_1[t/x]$. However, $w \leq_i w' \leq_i w''$ implies $w \leq_i w''$. Hence, by definition of satisfaction on the assumptions $w \models \forall x{:}\sigma.s_1$ and $D(w'') \vdash t : \sigma$, we get $w'' \models s_1[t/x]$, as required.

Case. $s = \exists x{:}\sigma.s_1$. Suppose $w \models \exists x{:}\sigma.s_1$ and $w \leq_i w'$. By definition of $\models$, there is a t such that $D(w) \vdash t : \sigma$ and $w \models s_1[t/x]$. By (K-grow1) and the i.h. respectively, we obtain $D(w') \vdash t : \sigma$ and $w' \models s_1[t/x]$. The last two facts imply $w' \models \exists x{:}\sigma.s_1$ by definition of $\models$.

Case. $s = k \text{ says } s'$. Suppose $w \models k \text{ says } s'$ and $w \leq_i w'$. We want to show that $w' \models k \text{ says } s'$. Following the definition of $\models$, pick a w'' such that $w' \leq_i \leq_s w''$ and

$k \in \theta(w'')$. It suffices to show that $w'' \models s'$. However, $w \leq_i w' \leq_i \leq_s w''$, so $w \leq_i \leq_s w''$. The required fact $w'' \models s'$ now follows from definition of $\models$ applied to $w \models k \; \mathsf{says} \; s'$. □

Lemma 2.4 (Monotonicity of says)**.** *$w \models k \; \mathsf{says} \; s$ and $w \leq_s w'$ imply $w' \models k \; \mathsf{says} \; s$. (It follows from this statement that $w \models k \; \mathsf{claims} \; s$ and $w \leq_s w'$ imply $w' \models k \; \mathsf{claims} \; s$.)*

Proof. Suppose $w \models k \; \mathsf{says} \; s$ and $w \leq_s w'$. We want to show that $w' \models k \; \mathsf{says} \; s$. Following the definition of $\models$, pick a w'' such that $w' \leq_i \leq_s w''$ and $k \in \theta(w'')$. It suffices to show that $w'' \models s$. However, $w \leq_s \leq_i \leq_s w''$, so by (K-commute), $w \leq_s \leq_s w''$, i.e., $w \leq_s w''$. Since $\leq_i$ is reflexive, we also get $w \leq_i \leq_s w''$. From definition of $w \models k \; \mathsf{says} \; s$, we have $w'' \models s$, as required. □

Theorem 2.5 (Soundness)**.** *If $\Sigma; \Gamma \xrightarrow{k} s$ then for any $\mathcal{K}$, $\mathcal{K} \models (\Sigma; \Gamma \xrightarrow{k} s)$.*

Proof. By induction on the derivation of $\Sigma; \Gamma \xrightarrow{k} s$ and a case analysis the last rule in it. By definition of $\models$, we are trying to prove that for all ν and w, $\Sigma \ll \nu : (\mathcal{K}, w)$, $k\nu \in \theta(w)$, and $w \models \Gamma\nu$ imply $w \models s\nu$. We show some interesting cases below.

Case. $$\frac{}{\Sigma; \Gamma, p \xrightarrow{k} p}\text{init}$$

Assume that $\Sigma \ll \nu : (\mathcal{K}, w)$, $k\nu \in \theta(w)$, and $w \models (\Gamma, p)\nu$. By the last assumption, we immediately obtain $w \models p\nu$, as required.

Case. $$\frac{\Sigma \rhd k \succeq k_0 \qquad \Sigma; \Gamma, k \; \mathsf{claims} \; s, s \xrightarrow{k_0} r}{\Sigma; \Gamma, k \; \mathsf{claims} \; s \xrightarrow{k_0} r}\text{claims}$$

Assume that $\Sigma \ll \nu : (\mathcal{K}, w)$, $k_0\nu \in \theta(w)$, and $w \models (\Gamma, k \; \mathsf{claims} \; s)\nu$. We want to show that $w \models r\nu$. We have:

1. $\Sigma \ll \nu : (\mathcal{K}, w)$, $k_0\nu \in \theta(w)$, and $w \models (\Gamma, k \; \mathsf{claims} \; s, s)\nu$ imply $w \models r\nu$ (i.h. on 2nd premise)
2. $D(w) \rhd k\nu \succeq k_0\nu$ (Lemma 2.2 on 1st premise and $\Sigma \ll \nu : (\mathcal{K}, w)$)
3. $k\nu \in \theta(w)$ ((K-viewcl) on 2)
4. $w \leq_i \leq_s w$ ($\leq_i$ and $\leq_s$ are reflexive)
5. $w \models k\nu \; \mathsf{says} \; s\nu$ (Assumption $w \models (\Gamma, k \; \mathsf{claims} \; s)\nu$)
6. $w \models s\nu$ (3–5)
7. $w \models (\Gamma, k \; \mathsf{claims} \; s, s)\nu$ (Assumption $w \models (\Gamma, k \; \mathsf{claims} \; s)\nu$ and 6)
8. $w \models r\nu$ (1,7, and assumptions $\Sigma \ll \nu : (\mathcal{K}, w)$ and $k_0\nu \in \theta(w)$)

Case. $\dfrac{\Sigma;\Gamma| \xrightarrow{k} s}{\Sigma;\Gamma \xrightarrow{k_0} k \mathsf{\ says\ } s}\mathsf{saysR}$

Assume that $\Sigma \ll \nu : (\mathcal{K}, w)$, $k_0\nu \in \theta(w)$, and $w \models \Gamma\nu$. We want to show that $w \models k\nu \mathsf{\ says\ } s\nu$. Following the definition of $\models$, pick any w' such that $w \leq_i \leq_s w'$ and $k\nu \in \theta(w')$. It suffices to show that $w' \models s\nu$. Now observe that by assumption, $w \models \Gamma\nu$. Hence, in particular, $w \models (\Gamma|)\nu$. By Lemmas 2.3 and 2.4, $w' \models (\Gamma|)\nu$. (Note that $\Gamma|$ only contains assumptions of the form $k' \mathsf{\ claims\ } s'$, so Lemma 2.4 can be applied.)

Next, we have the assumption $\Sigma \ll \nu : (\mathcal{K}, w)$. Since $D(w) \subseteq D(w')$ by (K-grow1) and (K-grow2), it follows from definition of $\ll$ that $\Sigma \ll \nu : (\mathcal{K}, w')$. Further, $k\nu \in \theta(w')$ by assumption and we just proved $w' \models (\Gamma|)\nu$. Applying the i.h. to the premise (at w', not w), and using the last three facts, we immediately obtain $w' \models s\nu$, as required.

Case. $\dfrac{\Sigma;\Gamma, s \xrightarrow{k} s'}{\Sigma;\Gamma \xrightarrow{k} s \supset s'}{\supset}\mathrm{R}$

Assume that $\Sigma \ll \nu : (\mathcal{K}, w)$, $k\nu \in \theta(w)$, and $w \models \Gamma\nu$. We want to show that $w \models s\nu \supset s'\nu$. Following the definition of $\models$, pick any w' such that $w \leq_i w'$ and $w' \models s\nu$. It suffices to show that $w' \models s'\nu$. By Lemma 2.3, $w' \models \Gamma\nu$. Hence, $w' \models (\Gamma, s)\nu$. By (K-viewmon), $k\nu \in \theta(w')$. By i.h. on the premise at w', we get $w' \models s'\nu$, as required.

Case. $\dfrac{\Sigma, x{:}\sigma;\Gamma \xrightarrow{k} s}{\Sigma;\Gamma \xrightarrow{k} \forall x{:}\sigma.s}\forall\mathrm{R}$

Assume that $\Sigma \ll \nu : (\mathcal{K}, w)$, $k\nu \in \theta(w)$, and $w \models \Gamma\nu$. We want to show that $w \models \forall x{:}\sigma.(s\nu)$. Following the definition of $\models$, pick any w' and t such that $w \leq_i w'$ and $D(w') \vdash t : \sigma$. It suffices to prove that $w' \models s\nu[t/x]$. Consider the substitution $\nu' = \nu, t/x$. First observe that because $\Sigma \ll \nu : (\mathcal{K}, w)$, $D(w) \subseteq D(w')$ (by (K-grow1)) and $D(w') \vdash t : \sigma$, it is also the case that $\Sigma, x{:}\sigma \ll \nu' : (\mathcal{K}, w')$. Second, by (K-viewmon), $k\nu' = k\nu \in \theta(w')$. Finally, observe that $\Gamma\nu = \Gamma\nu'$ because x is fresh and cannot occur in Γ. Hence, it follows from Lemma 2.3 that $w' \models \Gamma\nu'$. By i.h. applied to the premise at w', ν' and the previous three facts, we get $w' \models s\nu'$ or, equivalently, $w' \models s\nu[t/x]$, as required.

Case. $\dfrac{\Sigma;\Gamma, \forall x{:}\sigma.s, s[t/x] \xrightarrow{k} r \qquad \Sigma \vdash t{:}\sigma}{\Sigma;\Gamma, \forall x{:}\sigma.s \xrightarrow{k} r}\forall\mathrm{L}$

Assume that $\Sigma \ll \nu : (\mathcal{K}, w)$, $k\nu \in \theta(w)$, and $w \models (\Gamma, \forall x{:}\sigma.s)\nu$. In particular, the last assumption implies $w \models \forall x{:}\sigma.(s\nu)$. We want to show that $w \models r\nu$. Observe that $\Sigma \vdash t : \sigma$ (second premise) and $\Sigma \ll \nu : (\mathcal{K}, w)$ imply by Lemma 2.1 that $D(w) \vdash t\nu : \sigma$. Further, $w \leq_i w$. So, by definition of $\models$ applied to $w \models \forall x{:}\sigma.(s\nu)$, we also obtain that $w \models (s\nu)[t\nu/x]$ or, equivalently, $w \models (s[t/x])\nu$. Hence, $w \models (\Gamma, \forall x{:}\sigma.s, s[t/x])\nu$. Applying i.h. to the premise, we immediately obtain $w \models r\nu$, as required.

Case. $$\frac{\Sigma; \Gamma \xrightarrow{k} s[t/x] \qquad \Sigma \vdash t{:}\sigma}{\Sigma; \Gamma \xrightarrow{k} \exists x{:}\sigma.s}\exists\mathrm{R}$$

Assume that $\Sigma \ll \nu : (\mathcal{K}, w)$, $k\nu \in \theta(w)$, and $w \models \Gamma\nu$. We want to show that $w \models \exists s{:}\sigma.(s\nu)$. By i.h. on the premise, $w \models s[t/x]\nu$ or, equivalently, $w \models s\nu[t\nu/x]$. Applying Lemma 2.1 to second premise and $\Sigma \ll \nu : (\mathcal{K}, w)$ we have $D(w) \vdash t\nu : \sigma$. Hence, by definition of $\models$ for existential quantifiers (choosing $t \leftarrow t\nu$), we have $w \models \exists s{:}\sigma.(s\nu)$, as required.

Case. $$\frac{\Sigma, x{:}\sigma; \Gamma, \exists x{:}\sigma.s, s \xrightarrow{k} r}{\Sigma; \Gamma, \exists x{:}\sigma.s \xrightarrow{k} r}\exists\mathrm{L}$$

Assume that $\Sigma \ll \nu : (\mathcal{K}, w)$, $k\nu \in \theta(w)$, and $w \models (\Gamma, \exists x{:}\sigma.s)\nu$. We want to show that $w \models r\nu$. From the last assumption it follows that $w \models \exists x{:}\sigma.(s\nu)$. Hence, there is a t such that $D(w) \vdash t : \sigma$ and $w \models s\nu[t/x]$. Define $\nu' = \nu, t/x$. First, observe that because $\Sigma \ll \nu : (\mathcal{K}, w)$ and $D(w) \vdash t : \sigma$, it must also be that $\Sigma, x{:}\sigma \ll \nu' : (\mathcal{K}, w)$. Second, $w \models s\nu[t/x]$ is the same as $w \models s\nu'$ and $w \models (\Gamma, \exists x{:}\sigma.s)\nu$ is the same as $w \models (\Gamma, \exists x{:}\sigma.s)\nu'$ (because x is fresh). So, $w \models (\Gamma, \exists x{:}\sigma.s, s)\nu'$. Finally, $k\nu \in \theta(w)$ implies $k\nu' \in \theta(w)$ (because $k\nu = k\nu'$). Therefore, by i.h. on premise with $\nu \leftarrow \nu'$ we obtain $w \models r\nu'$. However, $r\nu = r\nu'$, so $w \models r\nu$, as required. □

2.4 Completeness

Next, we prove that our Kripke semantics are also complete. In order to do that we build a canonical Kripke model and show that satisfaction in that model entails provability. We assume a countably infinite universe $\mathcal{U}$ of first-order symbols. Since the logic has a finite signature, there are countably infinite number of symbols outside of this signature in $\mathcal{U}$. All sets denoted S in the following are assumed to be subsets of $\mathcal{U}$.

Definition 2.6 (Theory)**.** A theory is a triple (S, Γ, K) where S is a (possibly infinite) sorting disjoint from the logic's signature, Γ is a (possibly infinite) set of formulas well-formed over S, and K is a (possibly infinite) set of terms of sort $\mathsf{principal}$ under S.

Definition 2.7 (Filter)**.** A set K of terms of sort $\mathsf{principal}$ in sorting S is called a filter with respect to S (written $S \curlyvee K$) if there is term $k_m \in K$ such that $K = \{k \mid S \rhd k \succeq k_m\}$. (So K contains both a least element k_m under the order $\succeq$.)

Definition 2.8 (Prime theory)**.** We call a theory (S, Γ, K) prime if the following hold:

1. (Prin-closure) $S \curlyvee K$.
2. (Fact-closure) If $k \in K$ and $S; \Gamma \xrightarrow{k} s$, then $s \in \Gamma$.
3. (Primality1) If $s_1 \vee s_2 \in \Gamma$, then either $s_1 \in \Gamma$ or $s_2 \in \Gamma$.
4. (Primality2) If $\exists x{:}\sigma.s \in \Gamma$, then there is a term t such that $S \vdash t : \sigma$ and $s[t/x] \in \Gamma$.

5. (Primality3) $\bot \notin \Gamma$.

We take as worlds of our canonical model prime theories.

Definition 2.9 (Canonical model)**.** The canonical Kripke model for BL_0 is defined as $(W, \leq_i, \leq_s, D, \rho, \theta)$, where:

- $W = \{(S, \Gamma, K) \mid (S, \Gamma, K) \text{ is a prime theory}\}$
- $(S, \Gamma, K) \leq_i (S', \Gamma', K')$ iff $S \subseteq S'$, $\Gamma \subseteq \Gamma'$ and $K \subseteq K'$.
- $(S, \Gamma, K) \leq_s (S', \Gamma', K')$ iff $S \subseteq S'$ and for all k, s, $k \mathsf{\ says\ } s \in \Gamma$ and $k \in K'$ imply $s \in \Gamma'$.
- $D(S, \Gamma, K) = S$.
- $(t_1, \ldots, t_n) \in \rho(S, \Gamma, K)(P)$ iff $P(t_1, \ldots, t_n) \in \Gamma$.
- $\theta(S, \Gamma, K) = K$.

Lemma 2.10 (Canonical model is a Kripke model)**.** *The canonical model as defined above is a Kripke model for BL_0.*

Proof. We verify the conditions in the definition of Kripke models (Section 2).

- $\leq_i$ is reflexive and transitive because $\subseteq$ is reflexive and transitive.
- $\leq_s$ is reflexive: By definition of $\leq_s$ in the canonical model, we need to show that for any prime theory (S, Γ, K), (a) $S \subseteq S$ (which is trivial) and (b) $k \mathsf{\ says\ } s \in \Gamma$ and $k \in K$ imply $s \in \Gamma$. The latter follows from (Fact-closure) because $S; \Gamma \xrightarrow{k} s$ if $k \mathsf{\ says\ } s \in \Gamma$.
- $\leq_s$ is transitive: Suppose $(S_1, \Gamma_1, K_1) \leq_s (S_2, \Gamma_2, K_2) \leq_s (S_3, \Gamma_3, K_3)$. We want to show $(S_1, \Gamma_1, K_1) \leq_s (S_3, \Gamma_3, K_3)$. Accordingly, we must show that (a) $S_1 \subseteq S_3$ and (b) $k \mathsf{\ says\ } s \in \Gamma_1$ and $k \in K_3$ imply $s \in \Gamma_3$. (a) follows because $S_1 \subseteq S_2 \subseteq S_3$. To prove (b), observe that because (S_1, Γ_1, K_1) and (S_2, Γ_2, K_2) are prime theories, both K_1 and K_2 are non-empty. So let $k_1 \in K_1$ and $k_2 \in K_2$. In the sequent calculus, $S_1; \Gamma_1 \xrightarrow{k_1} k_2 \mathsf{\ says\ } k \mathsf{\ says\ } s$ (because $k \mathsf{\ says\ } s \in \Gamma_1$). So by (Fact-closure), $k_2 \mathsf{\ says\ } k \mathsf{\ says\ } s \in \Gamma_1$. Because $k_2 \in K_2$, $k \mathsf{\ says\ } s \in \Gamma_2$. Finally, because $k \in K_3$, $s \in \Gamma_3$, as required.
- (K-commute) Suppose $(S_1, \Gamma_1, K_1) \leq_i (S_2, \Gamma_2, K_2) \leq_s (S_3, \Gamma_3, K_3)$. We need to show that $(S_1, \Gamma_1, K_1) \leq_s (S_3, \Gamma_3, K_3)$. By definition of $\leq_s$ in the canonical model, we must check two conditions: (a) $S_1 \subseteq S_3$, and (b) $k \mathsf{\ says\ } s \in \Gamma_1$ and $k \in K_3$ imply $s \in \Gamma_3$. (a) follows immediately because $S_1 \subseteq S_2 \subseteq S_3$. To prove (b), observe that $k \mathsf{\ says\ } s \in \Gamma_1$ implies $k \mathsf{\ says\ } s \in \Gamma_2$ (because $\Gamma_1 \subseteq \Gamma_2$). Therefore, the definition of $(S_2, \Gamma_2, K_2) \leq_s (S_3, \Gamma_3, K_3)$ in the canonical model implies that $s \in \Gamma_3$, as required.

- (K-fresh) follows from the requirement that $D(S, \Gamma, K) = S$ in a theory be disjoint from the logic's signature.

- (K-grow1) Suppose $(S_1, \Gamma_1, K_1) \leq_i (S_2, \Gamma_2, K_2)$. Then, by definition of $\leq_i$ in the canonical model we get $D(S_1, \Gamma_1, K_1) = S_1 \subseteq S_2 = D(S_2, \Gamma_2, K_2)$.

- (K-grow2) Suppose $(S_1, \Gamma_1, K_1) \leq_s (S_2, \Gamma_2, K_2)$. Then, by definition of $\leq_s$ in the canonical model we get $D(S_1, \Gamma_1, K_1) = S_1 \subseteq S_2 = D(S_2, \Gamma_2, K_2)$.

- (K-mon) Suppose $(S_1, \Gamma_1, K_1) \leq_i (S_2, \Gamma_2, K_2)$. We want to show that $\rho(S_1, \Gamma_1, K_1)(P) \subseteq \rho(S_2, \Gamma_2, K_2)(P)$. Suppose $(t_1, \ldots, t_n) \in \rho(S_1, \Gamma_1, K_1)(P)$. By definition of the canonical model, $P(t_1, \ldots, t_n) \in \Gamma_1$. Since $\Gamma_1 \subseteq \Gamma_2$, $P(t_1, \ldots, t_n) \in \Gamma_2$ or, equivalently, $(t_1, \ldots, t_n) \in \rho(S_2, \Gamma_2, K_2)(P)$. Since $(t_1, \ldots, t_n)$ is arbitrary, $\rho(S_1, \Gamma_1, K_1)(P) \subseteq \rho(S_2, \Gamma_2, K_2)(P)$.

- (K-viewmon) Suppose $k \in \theta(S_1, \Gamma_1, K_1) = K_1$ and $(S_1, \Gamma_1, K_1) \leq_i (S_2, \Gamma_2, K_2)$. We need to show that $k \in \theta(S_2, \Gamma_2, K_2) = K_2$. However, this is trivial because $K_1 \subseteq K_2$ by definition of $\leq_i$ in the canonical model.

- (K-viewcl) Suppose $k \in \theta(S, \Gamma, K) = K$ and $S = D(S, \Gamma, K) \rhd k' \succeq k$. We need to show that $k' \in K$. From (Prin-closure), it follows that there is a $k_m \in K$ such that $S \rhd k \succeq k_m$. Using (C-trans), $S \rhd k' \succeq k_m$. Since $K = \{k \mid S \rhd k \succeq k_m\}$, $k' \in K$, as required.

□

Definition 2.11 (s-consistent theory)**.** If $S \vdash s$ ok, we call a (not necessarily prime) theory (S, Γ, K) s-consistent if for all $k \in K$, $S; \Gamma \not\xrightarrow{k} s$.

Lemma 2.12 (Consistent extensions)**.** *Suppose (S, Γ, K) is s-consistent and $S \curlyvee K$. Then there is a prime theory (S^*, Γ^*, K^*) such that $S \subseteq S^*$, $\Gamma \subseteq \Gamma^*$, $K \subseteq K^*$, and (S^*, Γ^*, K^*) is s-consistent.*

Proof. Our proof follows a similar construction for hybrid propositional logic in [3], although the construction in that paper does not consider views. Because $S \curlyvee K$, there is a $k_m \in K$ such that $K = \{k \mid S \rhd k \succeq k_m\}$. We inductively construct a sequence of pairs (S_n, Γ_n) with $(S_0, \Gamma_0) = (S, \Gamma \cup \{c)$, satisfying the following properties:

1. $S_n \subseteq S_{n+1}$ and $\Gamma_n \subseteq \Gamma_{n+1}$.

2. For each $s_n \in \Gamma_n$, $S_n \vdash s_n$ ok

3. $S_n; \Gamma_n \not\xrightarrow{k_m, u_1, u_2} s$.

Fix an enumeration $E = s_0, s_1, \ldots$ of all (possibly ill-typed) formulas that can be created using the symbols in the logic's signature and those in $\mathcal{U}$. The intuitive idea of our construction is to alternately look at formulas of the forms $s_1 \vee s_2$ and $\exists x{:}\sigma.s'$ that can be proved from the sets constructed so far, and to complete the primality conditions for them. We keep track of formulas we have already looked at through two sequences of sets $\mathit{treated}^{\vee}_n$ and $\mathit{treated}^{\exists}_n$. We set $\mathit{treated}^{\vee}_0 = \mathit{treated}^{\exists}_0 = \emptyset$. To define S_{n+1}, Γ_{n+1}, $\mathit{treated}^{\vee}_{n+1}$ and $\mathit{treated}^{\exists}_{n+1}$, we case analyze the parity of $n+1$. We also simultaneously prove the conditions (1)–(3) for S_{n+1} and Γ_{n+1}.

Case. $n+1$ is even. Let $s_1 \vee s_2$ be the first formula in the enumeration E with a top level disjunction that satisfies two conditions: (a) $S_n; \Gamma_n \xrightarrow{k_m} s_1 \vee s_2$, and (b) $s_1 \vee s_2 \notin \mathit{treated}^{\vee}_n$. (If no such formula exists, set $S_{n+1} = S_n$, $\Gamma_{n+1} = \Gamma_n$, $\mathit{treated}^{\vee}_{n+1} = \mathit{treated}^{\vee}_n$, and $\mathit{treated}^{\exists}_{n+1} = \mathit{treated}^{\exists}_n$.) Now we argue that either $S_n; \Gamma_n, s_1 \not\xrightarrow{k_m} s$ or $S_n; \Gamma_n, s_2 \not\xrightarrow{k_m} s$. Suppose on the contrary that $S_n; \Gamma_n, s_1 \xrightarrow{k_m} s$ and $S_n; \Gamma_n, s_2 \xrightarrow{k_m} s$. Then, $S_n; \Gamma_n, s_1 \vee s_2 \xrightarrow{k_m} s$. Because $S_n; \Gamma_n \xrightarrow{k_m} s_1 \vee s_2$, by the cut principle, we also obtain $S_n; \Gamma_n \xrightarrow{k_m} s$, which contradicts condition (2) for (S_n, Γ_n). Hence, either $S_n; \Gamma_n, s_1 \not\xrightarrow{k_m} s$ or $S_n; \Gamma_n, s_2 \not\xrightarrow{k_m} s$. In the former case, set $\Gamma_{n+1} = \Gamma_n, s_1$; in the latter case set $\Gamma_{n+1} = \Gamma_n, s_2$. In both cases, set $S_{n+1} = S_n$, $\mathit{treated}^{\vee}_{n+1} = \mathit{treated}^{\vee}_n, s_1 \vee s_2$, and $\mathit{treated}^{\exists}_{n+1} = \mathit{treated}^{\exists}_n$.

Condition (1) holds by construction. Condition (2) holds because $S_n; \Gamma_n \xrightarrow{k_m} s_1 \vee s_2$, so $S_n = S_{n+1} \vdash s_i\ \mathsf{ok}$. Condition (3) holds at $n+1$ by construction.

Case. $n+1$ is odd. Let $\exists x{:}\sigma.s'$ be the first formula in the enumeration E with a top level existential quantification that satisfies two conditions: (a) $S_n; \Gamma_n \xrightarrow{k_m} \exists x{:}\sigma.s'$, and (b) $\exists x{:}\sigma.s' \notin \mathit{treated}^{\exists}_n$. (If no such formula exists, set $S_{n+1} = S_n$, $\Gamma_{n+1} = \Gamma_n$, $\mathit{treated}^{\vee}_{n+1} = \mathit{treated}^{\vee}_n$, and $\mathit{treated}^{\exists}_{n+1} = \mathit{treated}^{\exists}_n$.) Pick a fresh constant $a \in \mathcal{U}$. Set $S_{n+1} = S_n, a{:}\sigma$, $\Gamma_{n+1} = \Gamma_n, s'[a/x]$, $\mathit{treated}^{\vee}_{n+1} = \mathit{treated}^{\vee}_n$, and $\mathit{treated}^{\exists}_{n+1} = \mathit{treated}^{\exists}_n, \exists x{:}\sigma.s'$.

Condition (1) holds by construction. Condition (2) holds: $S_{n+1} \vdash s'[a/x]\ \mathsf{ok}$ because $S_{n+1} \vdash a : \sigma$ and $S_n, x{:}\sigma \vdash s'\ \mathsf{ok}$. To prove that condition (3) holds for $n+1$, we reason by contradiction. Suppose not. Then, $S_{n+1}; \Gamma_{n+1} \xrightarrow{k_m} s$ or, equivalently, $S_n, a{:}\sigma; \Gamma_n, s'[a/x] \xrightarrow{k_m} s$. From the latter we derive $S_n; \Gamma_n, \exists x{:}\sigma.s' \xrightarrow{k_m} s$. Since $S_n; \Gamma_n \xrightarrow{k_m} \exists x{:}\sigma.s'$, by the cut principle, $S_n; \Gamma_n \xrightarrow{k_m} s$, which contradicts condition (3) for n. Hence (3) must hold at $n+1$.

This completes our inductive construction. Let $S^* = \cup_i S_i$, $\Gamma' = \cup_i \Gamma_i$, and $K^* = \{k \mid S^* \rhd k \succeq k_m\}$. Finally, define $\Gamma^* = \{s^* \mid S^*; \Gamma' \xrightarrow{k_m} s^*\}$.

Clearly, (S^*, Γ^*, K^*) is a theory. Also, by construction, $S = S_0 \subseteq S^*$ and $\Gamma = \Gamma_0 \subseteq \Gamma' \subseteq \Gamma^*$ ($\Gamma' \subseteq \Gamma^*$ follows from the identity principle of the sequent calculus). Further, $K \subseteq K^*$ because for every k, $S \rhd k \succeq k_m$ implies $S^* \rhd k \succeq k_m$ by (C-weaken).

Next, we check that (S^*, Γ^*, K^*) is s-consistent. Suppose for the sake of contradiction that it is not. Then, it follows that $S^*; \Gamma^* \xrightarrow{k} s$ for some $k \in K^*$. Hence, there are finite subsets $S^f \subseteq S^*$ and $\Gamma^f \subseteq \Gamma^*$ such that $S^f; \Gamma^f \xrightarrow{k} s$. By the view subsumption principle, $S^f; \Gamma^f \xrightarrow{k_m} s$. Since each s^* in Γ^f satisfies $S^*; \Gamma' \xrightarrow{k_m} s^*$, it follows by $|\Gamma^f|$ applications of the cut principle that $S^*; \Gamma' \xrightarrow{k_m} s$. Since $S^* = \cup_i S_i$ and $\Gamma' = \cup_i \Gamma_i$, there must be some

n such that $S_n; \Gamma_n \xrightarrow{k_m} s$, which contradicts condition (3) for that n. So (S^*, Γ^*, K^*) is s-consistent.

It remains only to check that (S^*, Γ^*, K^*) is prime. To do that we check the conditions in the definition of a prime theory.

- (Prin-closure) By definition, $K^* = \{k \mid S^* \rhd k \succeq k_m\}$. Hence $S^* \curlyvee K^*$.

- (Fact-closure) Suppose $S^*; \Gamma^* \xrightarrow{k} s'$ for some $k \in K^*$. We need to show that $s' \in \Gamma^*$. Since $S^*; \Gamma^* \xrightarrow{k} s'$, there are finite subsets $S^f \subseteq S^*$ and $\Gamma^f \subseteq \Gamma^*$ such that $S^f; \Gamma^f \xrightarrow{k} s'$. By the view subsumption principle, $S^f; \Gamma^f \xrightarrow{k_m} s'$. Since each s^* in Γ^f satisfies $S^*; \Gamma' \xrightarrow{k_m} s^*$, it follows by $|\Gamma^f|$ applications of the cut principle that $S^*; \Gamma' \xrightarrow{k_m} s'$. By definition of Γ^*, $s' \in \Gamma^*$.

- (Primality1) Suppose $s_1 \vee s_2 \in \Gamma^*$. Therefore, $S^*; \Gamma' \xrightarrow{k_m} s_1 \vee s_2$. Hence, there is some n such that $S_n; \Gamma_n \xrightarrow{k_m} s_1 \vee s_2$. If $s_1 \vee s_2 \in \mathit{treated}_n^{\vee}$, then by construction either s_1 or s_2 must be in Γ_n (whenever we add $s_1 \vee s_2$ to $\mathit{treated}_i^{\vee}$, we also add either s_1 or s_2 to Γ_i). Hence, either s_1 or s_2 must be in Γ^*, which is a superset of each Γ_n. If $s_1 \vee s_2 \notin \mathit{treated}_n^{\vee}$, let $s_1 \vee s_2$ have index k in the enumeration E. Then, in at most $2k$ further steps we would consider $s_1 \vee s_2$ as a candidate and add either s_1 or s_2 to Γ'.

- (Primality2) Suppose $\exists x{:}\sigma.s' \in \Gamma^*$. Therefore, $S^*; \Gamma' \xrightarrow{k_m} \exists x{:}\sigma.s'$. Hence, there is some n such that $S_n; \Gamma_n \xrightarrow{k_m} \exists x{:}\sigma.s'$. If $\exists x{:}\sigma.s' \in \mathit{treated}_n^{\exists}$, then by construction there must be a constant a such that $a{:}\sigma \in S_n$ and $s'[a/x] \in \Gamma_n$ (whenever we add $\exists x{:}\sigma.s'$ to $\mathit{treated}_i^{\exists}$, we also add a fresh $a{:}\sigma$ to S_i and $s'[a/x]$ to Γ_i). This immediately implies the primality condition because $\Gamma^* \supseteq \Gamma_n$. If $\exists x{:}\sigma.s' \notin \mathit{treated}_n^{\exists}$, let $\exists x{:}\sigma.s'$ have index k in the enumeration E. Then, in at most $2k$ further steps we would consider $\exists x{:}\sigma.s'$ as a candidate and add $a{:}\sigma$ to S and $s'[a/x]$ to Γ'.

- (Primality3) Suppose for the sake of contradiction that $\bot \in \Gamma^*$. Then, $S^*; \Gamma^* \xrightarrow{k_m} s$, which contradicts the previously derived fact that (S^*, Γ^*, K^*) is s-consistent. Hence $\bot \notin \Gamma^*$.

□

Lemma 2.13 (Satisfaction). *For any formula s and any prime theory (S, Γ, K), it is the case that $(S, \Gamma, K) \models s$ in the canonical model if and only if $s \in \Gamma$.*

Proof. By induction on s and case analysis of its top-level constructor.

Case. $s = P(t_1, \ldots, t_n)$.

$P(t_1, \ldots, t_n) \in \Gamma \iff (t_1, \ldots, t_n) \in \rho(S, \Gamma, K)(P) \iff (S, \Gamma, K) \models P(t_1, \ldots, t_n)$. The first step follows from definition of ρ in the canonical model and the second step follows from the definition of $\models$.

Case. $s = s_1 \wedge s_2$.

Suppose $s_1 \wedge s_2 \in \Gamma$. We need to prove that $(S, \Gamma, K) \models s_1 \wedge s_2$. Since $s_1 \wedge s_2 \in \Gamma$, $S; \Gamma \xrightarrow{k} s_i$ for any $k \in K$ and $i \in \{1, 2\}$. By (Fact-closure), $s_1, s_2 \in \Gamma$. By i.h., $(S, \Gamma, K) \models s_1$ and $(S, \Gamma, K) \models s_2$. Hence, by definition of $\models$, $(S, \Gamma, K) \models s_1 \wedge s_2$, as required.

Conversely, suppose that $(S, \Gamma, K) \models s_1 \wedge s_2$. We need to prove that $s_1 \wedge s_2 \in \Gamma$. By definition of $\models$, $(S, \Gamma, K) \models s_1$ and $(S, \Gamma, K) \models s_2$. Hence, by the i.h., $s_1, s_2 \in \Gamma$. Therefore, for any $k \in K$, $S; \Gamma \xrightarrow{k} s_1 \wedge s_2$. By (Fact-closure), $s_1 \wedge s_2 \in \Gamma$, as required.

Case. $s = s_1 \vee s_2$.

Suppose $s_1 \vee s_2 \in \Gamma$. We need to show that $(S, \Gamma, K) \models s_1 \vee s_2$. By (Primality1), either $s_1 \in \Gamma$ or $s_2 \in \Gamma$. Suppose the former (the other case is similar). By i.h., $(S, \Gamma, K) \models s_1$. By definition of $\models$, $(S, \Gamma, K) \models s_1 \vee s_2$, as required.

Conversely, suppose that $(S, \Gamma, K) \models s_1 \vee s_2$. We need to show that $s_1 \vee s_2 \in \Gamma$. By definition of $\models$, either $(S, \Gamma, K) \models s_1$ or $(S, \Gamma, K) \models s_2$. Suppose the former (the other case is similar). By i.h., $s_1 \in \Gamma$. Therefore, $S; \Gamma \xrightarrow{k} s_1 \vee s_2$ for any $k \in K$. By (Fact-closure), $s_1 \vee s_2 \in \Gamma$, as required.

Case. $s = s_1 \supset s_2$.

Suppose $s_1 \supset s_2 \in \Gamma$. We need to show that $(S, \Gamma, K) \models s_1 \supset s_2$. Following the definition of $\models$, pick any (S', Γ', K') such that $(S, \Gamma, K) \leq_i (S', \Gamma', K')$ and assume that $(S', \Gamma', K') \models s_1$. It suffices to prove that $(S', \Gamma', K') \models s_2$. Observe that from the definition of $\leq_i$ in the canonical model, it follows that $\Gamma \subseteq \Gamma'$. So $s_1 \supset s_2 \in \Gamma'$. Hence both s_1 and $s_1 \supset s_2$ are in Γ'. It follows from the sequent calculus that $S'; \Gamma' \xrightarrow{k'} s_2$ for any $k' \in K'$. By (Fact-closure), $s_2 \in \Gamma'$ as required.

Conversely, suppose $(S, \Gamma, K) \models s_1 \supset s_2$. We need to show that $s_1 \supset s_2 \in \Gamma$. Assume for the sake of contradiction that $s_1 \supset s_2 \notin \Gamma$. Pick any $k \in K$. Due to (Fact-closure), $S; \Gamma \overset{k}{\not\to} s_1 \supset s_2$. Due to rule ($\supset$R) in the sequent calculus, $S; \Gamma, s_1 \overset{k}{\not\to} s_2$. Hence, $(S, \Gamma \cup \{s_1\}, K)$ is s_2-consistent. By Lemma 2.12 there is a prime theory $w = (S^*, \Gamma^*, K^*)$ such that $S \subseteq S^*$, $\Gamma \cup \{s_1\} \subseteq \Gamma^*$, $K \subseteq K^*$ and (S^*, Γ^*, K^*) is s_2-consistent. Clearly, $s_1 \in \Gamma^*$ so by i.h. $w \models s_1$. Further, $(S, \Gamma, K) \leq_i w$ and $(S, \Gamma, K) \models s_1 \supset s_2$, so $w \models s_2$. By i.h., $s_2 \in \Gamma^*$, which violates the s_2-consistency of (S^*, Γ^*, K^*). Hence it must be the case that $s_1 \supset s_2 \in \Gamma$.

Case. $s = \top$.

Suppose $\top \in \Gamma$. We want to show that $(S, \Gamma, K) \models \top$. The latter follows from definition of $\models$.

Conversely, suppose that $(S, \Gamma, K) \models \top$. We want to show that $\top \in \Gamma$. Observe that $S; \Gamma \xrightarrow{k} \top$ for any $k \in K$. Therefore, by (Fact-closure), $\top \in \Gamma$, as required.

Case. $s = \bot$.

Suppose $\bot \in \Gamma$. We want to show that $(S, \Gamma, K) \models \bot$. However, the condition $\bot \in \Gamma$ is impossible by (Primality3), so the conclusion holds vacuously.

Conversely, suppose $(S, \Gamma, K) \models \bot$. We want to show that $\bot \in \Gamma$. However, the condition $\bot \in \Gamma$ is impossible by definition of $\models$, so the conclusion holds vacuously.

Case. $s = \forall x{:}\sigma.s'$.

Suppose $\forall x{:}\sigma.s' \in \Gamma$. We want to show that $(S, \Gamma, K) \models \forall x{:}\sigma.s'$. Following the definition of $\models$, pick any (S', Γ', K') such that $(S, \Gamma, K) \leq_i (S', \Gamma', K')$ and any t such that $S' \vdash t : \sigma$. It suffices to prove that $(S', \Gamma', K') \models s'[t/x]$. Because $\Gamma \subseteq \Gamma'$, $\forall x{:}\sigma.s' \in \Gamma'$. Further, $S' \vdash t : \sigma$, so in the sequent calculus, $S'; \Gamma' \xrightarrow{k'} s'[t/x]$ for any $k' \in K'$. By (Fact-closure), $s'[t/x] \in \Gamma'$. By i.h., $(S', \Gamma', K') \models s'[t/x]$, as required.

Conversely, suppose that $(S, \Gamma, K) \models \forall x{:}\sigma.s'$. We want to show that $\forall x{:}\sigma.s' \in \Gamma$. Assume for the sake of contradiction that $\forall x{:}\sigma.s' \notin \Gamma$. By (Fact-closure), $S; \Gamma \not\xrightarrow{k} \forall x{:}\sigma.s'$ for every $k \in K$. Let a be a fresh constant. It follows due to rule ($\forall$R) of the sequent calculus that $S, a{:}\sigma; \Gamma \not\xrightarrow{k} s'[a/x]$ for every $k \in K$. Hence, the theory $(S \cup \{a{:}\sigma\}, \Gamma, K)$ is $s'[a/x]$-consistent. By Lemma 2.12, there is a prime theory (S^*, Γ^*, K^*) such that $S \cup \{a{:}\sigma\} \subseteq S^*$, $\Gamma \subseteq \Gamma^*$, $K \subseteq K^*$, and (S^*, Γ^*, K^*) is $s'[a/x]$-consistent. Now observe that $(S, \Gamma, K) \leq_i (S^*, \Gamma^*, K^*)$ and $S^* \vdash a : \sigma$. Hence, from the definition of $\models$ and the assumption $(S, \Gamma, K) \models \forall x{:}\sigma.s'$ we obtain $(S^*, \Gamma^*, K^*) \models s'[a/x]$. By i.h., $s'[a/x] \in \Gamma^*$, which contradicts the $s'[a/x]$-consistency of (S^*, Γ^*, K^*). Therefore, $\forall x{:}\sigma.s' \in \Gamma$.

Case. $s = \exists x{:}\sigma.s'$.

Suppose $\exists x{:}\sigma.s' \in \Gamma$. We want to show that $(S, \Gamma, K) \models \exists x{:}\sigma.s'$. By (Primality2), there is a term t such that $S \vdash t : \sigma$ and $s'[t/x] \in \Gamma$. By i.h., $(S, \Gamma, K) \models s'[t/x]$. Hence, by definition of $\models$, we get $(S, \Gamma, K) \models \exists x{:}\sigma.s'$ as required.

Conversely, suppose that $(S, \Gamma, K) \models \exists x{:}\sigma.s'$. We want to show that $\exists x{:}\sigma.s' \in \Gamma$. By definition of $\models$, there is a t such that $S \vdash t : \sigma$ and $(S, \Gamma, K) \models s'[t/x]$. By i.h., $s'[t/x] \in \Gamma$. Therefore, for any $k \in K$, we have $S; \Gamma \xrightarrow{k} \exists x{:}\sigma.s'$. By (Fact-closure), $\exists x{:}\sigma.s' \in \Gamma$ as required.

Case. $s = k \ \mathsf{says}\ s'$.

Suppose $k \ \mathsf{says}\ s' \in \Gamma$. We want to show that $(S, \Gamma, K) \models k \ \mathsf{says}\ s'$. Following the definition of $\models$, pick any (S_1, Γ_1, K_1) and (S_2, Γ_2, K_2) such that $(S, \Gamma, K) \leq_i (S_1, \Gamma_1, K_1) \leq_s (S_2, \Gamma_2, K_2)$ and $k \in \theta(S_2, \Gamma_2, K_2) = K_2$. It suffices to prove that $(S_2, \Gamma_2, K_2) \models s'$. Since $\Gamma \subseteq \Gamma_1$, $k \ \mathsf{says}\ s' \in \Gamma_1$. By definition of $\leq_s$ in the canonical model and the fact $k \in K_2$, we obtain $s' \in \Gamma_2$. By i.h., $(S_2, \Gamma_2, K_2) \models s'$, as required.

Conversely, suppose that $(S, \Gamma, K) \models k \ \mathsf{says}\ s'$. We want to show that $k \ \mathsf{says}\ s' \in \Gamma$. Assume for the sake of contradiction that $k \ \mathsf{says}\ s' \notin \Gamma$. Pick any $k' \in K$. By (Fact-closure), $S; \Gamma \not\xrightarrow{k'} k \ \mathsf{says}\ s'$. So by properties of the sequent calculus, $S; \Gamma| \not\xrightarrow{k} s'$.[2] Define $K_0 = \{k' \mid S \rhd k' \succeq k\}$. Then, because $S; \Gamma| \not\xrightarrow{k} s'$, we also get that $(S, \Gamma|, K_0)$ is s'-consistent. By Lemma 2.12, there is a prime theory (S^*, Γ^*, K^*) such that $S \subseteq S^*$, $\Gamma| \subseteq \Gamma^*$,

[2] $\Gamma|$ is defined here as $\{(k_1 \ \mathsf{says}\ s_1) \mid (k_1 \ \mathsf{says}\ s_1) \in \Gamma\}$.

$K_0 \subseteq K^*$, and (S^*, Γ^*, K^*) is s'-consistent. Next we argue that $(S, \Gamma, K) \leq_s (S^*, \Gamma^*, K^*)$. To do that, assume that k_1 says $s_1 \in \Gamma$ and $k_1 \in K^*$. We need to show that $s_1 \in \Gamma^*$. Because k_1 says $s_1 \in \Gamma$, k_1 says $s_1 \in \Gamma|$. Hence, k_1 says $s_1 \in \Gamma^*$. Therefore, $S^*; \Gamma^* \xrightarrow{k_1} s_1$. By (Fact-closure), $s_1 \in \Gamma^*$. This establishes $(S, \Gamma, K) \leq_s (S^*, \Gamma^*, K^*)$.

It follows that $(S, \Gamma, K) \leq_i (S, \Gamma, K) \leq_s (S^*, \Gamma^*, K^*)$. Since $(S, \Gamma, K) \models k$ says s' and $k \in K_0 \subseteq K^* = \theta(S^*, \Gamma^*, K^*)$, it follows that $(S^*, \Gamma^*, K^*) \models s'$. By i.h., $s' \in \Gamma^*$, which contradicts the s'-consistency of (S^*, Γ^*, K^*). Hence, we must have k says $s' \in \Gamma$. □

Lemma 2.14 (Completeness for closed formulas)**.** *Let $\mathcal{C}$ be the canonical Kripke model and s a closed formula. If $\mathcal{C} \models s$, then $\cdot; \cdot \xrightarrow{\ell} s$.*

Proof. Suppose for the sake of contradiction that $\mathcal{C} \models s$, but $\cdot; \cdot \overset{\ell}{\not\rightarrow} s$. Define $K = \{k \mid \cdot \rhd k \succeq \ell\}$. Observe that because $\cdot; \cdot \overset{\ell}{\not\rightarrow} s$, the theory $(\cdot, \cdot, K)$ is s-consistent. Hence, by Lemma 2.12, there is a prime theory (S^*, Γ^*, K^*) that is s-consistent. It follows from s-consistency of (S^*, Γ^*, K^*) that $s \notin \Gamma^*$. Hence, from Lemma 2.13, $(S^*, \Gamma^*, K^*) \not\models s$. This contradicts the assumption $\mathcal{C} \models s$. □

Theorem 2.15 (Completeness)**.** *Let $\mathcal{C}$ be the canonical Kripke model. If $\mathcal{C} \models (\Sigma; \Gamma \xrightarrow{k} s)$, then $\Sigma; \Gamma \xrightarrow{k} s$.*

Proof. Suppose $\mathcal{C} \models (\Sigma; \Gamma \xrightarrow{k} s)$. We first argue that $\mathcal{C} \models \forall\Sigma.\ k$ says $(\Gamma \supset s)$. To prove this we follow the definition of $\models$. This proof does not use any property specific to canonical models, and will work for any Kripke model $\mathcal{C}$. We pick any world w_1 in the model. It suffices to prove that $w_1 \models \forall\Sigma.\ k$ says $(\Gamma \supset s)$. Pick any w_2 such that $w_1 \leq_i w_2$ and any substitution ν such that $\Sigma \ll \nu : (\mathcal{C}, w_2)$. It suffices to show that $w_2 \models k\nu$ says $(\Gamma\nu \supset s\nu)$. Pick worlds w_3, w_4 such that $w_2 \leq_i w_3 \leq_s w_4$ and $k\nu \in \theta(w_4)$. It suffices to prove that $w_4 \models \Gamma\nu \supset s\nu$. Pick w_5 such that $w_5 \models \Gamma\nu$. It suffices to prove that $w_5 \models s\nu$.

Applying the definition of $\models$ on sequents to the assumption $\mathcal{C} \models (\Sigma; \Gamma \xrightarrow{k} s)$, we obtain that $\Sigma \ll \nu : (\mathcal{C}, w_5)$, $k\nu \in \theta(w_5)$, and $w_5 \models \Gamma\nu$ imply $w_5 \models s\nu$. We now check that $\Sigma \ll \nu : (\mathcal{C}, w_5)$, $k\nu \in \theta(w_5)$, and $w_5 \models \Gamma\nu$ all hold, thus implying $w_5 \models s\nu$, as required. $\Sigma \ll \nu : (\mathcal{C}, w_5)$ follows from the assumption $\Sigma \ll \nu : (\mathcal{C}, w_2)$ and the fact that $D(w_2) \subseteq D(w_5)$ (because $w_2 \leq_i w_3 \leq_s w_4 \leq_i w_5$). $k\nu \in \theta(w_5)$ follows from (K-viewmon) because $k\nu \in \theta(w_4)$ and $w_4 \leq_i w_5$. Finally, $w_5 \models \Gamma\nu$ holds by assumption.

Hence, $\mathcal{C} \models \forall\Sigma.\ k$ says $(\Gamma \supset s)$. By Lemma 2.14, $\cdot; \cdot \xrightarrow{\ell} \forall\Sigma.\ k$ says $(\Gamma \supset s)$. Using properties of the sequent calculus, this implies that $\Sigma; \Gamma \xrightarrow{k} s$, as required. □

Theorem 2.16 (Soundness and completeness)**.** $\Sigma; \Gamma \xrightarrow{k} s$ *if and only if* $\mathcal{K} \models (\Sigma; \Gamma \xrightarrow{k} s)$ *for every Kripke model* $\mathcal{K}$*.*

Proof. Immediate from Theorems 2.5 and 2.15. □

3 Kripke Semantics for BL

We now define a a Kripke semantics for BL in a similar way as for BL_0.

BL is a logic with explicit time: A BL judgement is always relative to some time interval $[u_1, u_2]$, where $u_1, u_2 \in \mathbb{Z} \cup \{-\infty, +\infty\}$ with $u_1 \leq u_2$. For meaningful policies, we expect to have $u_1 > u_2$ for every interval $[u_1, u_2]$ mentioned in the BL formalization of the policy. However in the proof theory and semantics of BL we have no restrictions to ensure $u_1 > u_2$ for intervals $[u_1, u_2]$ appearing in the formulas, as these restrictions would unnecessarily complicate the theory.

We write $[u_1, u_2] \subseteq [u'_1, u'_2]$ as an abbreviation for "$u'_1 \leq u_1$ and $u_2 \leq u'_2$". (Note that for meaningful time intervals this is the standard notation, whereas for $[u_1, u_2]$ with $u_1 > u_2$ it's an abuse of notation.)

We assume that we have an arithmetic aperator $+$ of type $\mathsf{time} \times \mathsf{time} \to \mathsf{time}$. We recursively define an evaluation ev function from ground terms of sort time to constants of sort time as follows:

- $\mathsf{ev}(c) = c$ for every constant c
- $\mathsf{ev}(t_1 + t_2) = \mathsf{ev}(t_1) + \mathsf{ev}(t_2)$ if $\mathsf{ev}(t_1)$ and $\mathsf{ev}(t_2)$ are integers (while the first $+$ is the arithmetic operator of BL, the second $+$ is the standard integer addition)
- $\mathsf{ev}(t_1 + t_2) = +\infty$ if either $\mathsf{ev}(t_2) = +\infty$ or $\mathsf{ev}(t_1) = +\infty$ and $\mathsf{ev}(t_2) \neq -\infty$
- $\mathsf{ev}(t_1 + t_2) = -\infty$ if either $\mathsf{ev}(t_2) = -\infty$ or $\mathsf{ev}(t_1) = -\infty$ and $\mathsf{ev}(t_2) \neq +\infty$

In BL, constraints can not only take the form $k_1 \succeq k_2$, but also the form $u_1 \leq u_2$. Additionally, they can serve as atomic formulas of BL. A notational and terminological difference between this technical report and [6] is that we include constraints among the judgments in a sequent instead of listing it separately (thus a constraint also counts as a judgment). Given a set Γ of judgments, we write $C(\Gamma)$ for the set of constraints in Γ.

BL uses an unstipulated judgment $\Sigma; \Gamma \rhd c$ instead of the unstipulated judgment $\Sigma \rhd c$ used in BL_0. The requirements that $\Sigma; \Gamma \rhd c$ is assumed to satisfy are defined in Section 4.2.1 of [6] (where the notation $\Sigma; \Psi \models c$ is used instead of $\Sigma; \Gamma \rhd c$). Additionally to the requirements mentioned there, we also assume the following three requirements:

$$\Sigma; \Gamma \rhd c \text{ iff } \Sigma; C(\Gamma) \rhd c \qquad \text{(C-constr)}$$

$$\text{If } \Sigma, x{:}\sigma; \Gamma \rhd c \text{ and } x \text{ does not occur in } \Gamma, c, \text{ then } \Sigma, \Gamma \rhd c \qquad \text{(C-strengthen)}$$

$$\text{If } t_1 \text{ and } t_2 \text{ are ground terms of sort } \mathsf{time} \text{ such that } \mathsf{ev}(t_1) \leq \mathsf{ev}(t_2), \text{ then } \Sigma; \Gamma \rhd t_1 \leq t_2. \qquad \text{(C-ground-time)}$$

(C-constr) is implicit in the notation of [6] and thus not explicitly listed there. (C-strengthen) is analogous to the requirement of the same name assumed for the unstipulated judgment $\Sigma \rhd c$ in Section 1. Furthermore, the requirements (C-weaken) and (C-cut) from [6] need to be rephrased as follows in order to be applicable to infinite sets:

$\Sigma; \Gamma \rhd c$ iff there are finite sets $\Sigma' \subseteq \Sigma$ and $\Gamma' \subseteq \Gamma$ such that $\Sigma'; \Gamma' \rhd c$ (C-weaken)

If $\Sigma; \Gamma, \Gamma' \rhd c$ and for every constraint $c' \in \Gamma'$, $\Sigma; \Gamma \rhd c'$, then $\Sigma; \Gamma \rhd c$. (C-cut)

We are now ready to define Kripke structures for BL:

Definition 3.1. A Kripke structure $\mathcal{K}$ is a tuple $(W, \leq_i, \leq_s, T, D, \pi, \rho, \theta)$, where:

- W is a set of worlds. Worlds are denoted w.
- $\leq_i$ is a reflexive and transitive relation over W.
- $\leq_s$ is a reflexive and transitive relation over W. We require that:
    - (K-commute) If $w \leq_s \leq_i w'$ then $w \leq_s w'$.
- T is a map from W to $(\mathbb{Z} \cup \{-\infty, +\infty\})^2$. Instead of "$T(w) = (u_1, u_2)$", we often say "$w$ is a $[u_1, u_2]$-world". We require that:
    - (T-mon) If $w \leq_i w'$, then $T(w) = T(w')$.
- D is a map from worlds to (possibly infinite) sortings of fresh constants. (Note that the proof theory disallows infinite sortings Σ). We require that:
    - (K-fresh) If $a{:}\sigma \in D(w)$ then a is not in the logic's signature.
    - (K-grow1) If $w \leq_i w'$ then $D(w) \subseteq D(w')$.
    - (K-grow2) If $w \leq_s w'$ then $D(w) \subseteq D(w')$.
- π is a map from worlds to sets of constraints. We require that:
    - (K-consclosure) If $C(\Gamma) \subseteq \pi(w)$ and $D(w); \Gamma \rhd c$, then $c \in \pi(w)$.
- ρ is a curried function: $\rho(w, [u_1, u_2])(P)$ is a subset of tuples of terms (of the same arity and types as argument of predicate symbol P) over $D(w)$. We require that:
    - (K-mon) If $w \leq_i w'$ and $[u_1', u_2'] \subseteq [u_1, u_2]$ then for every P, $\rho(w, [u_1, u_2])(P) \subseteq \rho(w', [u_1', u_2'])(P)$.
    - (K-prin) $(k, k') \in \rho(w, [u_1, u_2])(\succeq)$ iff $(k \succeq k') \in \pi(w)$.
    - (K-time) $(k, k') \in \rho(w, [u_1, u_2])(\leq)$ iff $(k \leq k') \in \pi(w)$.
- θ is a *view function*: $\theta(w)$ is a set of terms of sort $\mathsf{principal}$ over $D(w)$. We require that:
    - (K-viewmon) $k \in \theta(w)$ and $w \leq_i w'$ imply $k \in \theta(w')$.
    - (K-viewcl) $k \in \theta(w)$ and $(k' \succeq k) \in \pi(w)$ imply $k' \in \theta(w)$.

3.1 Substitutions

We denote substitutions of variables by constants using the letter μ. Given a finite sorting Σ, a Kripke structure $\mathcal{K} = (W, \leq_i, \leq_s, T, D, \pi, \rho, \theta)$, a substitution μ and a world $w \in W$, we say that μ conforms to Σ and $\mathcal{K}$ at w, written $\Sigma \ll \mu : (\mathcal{K}, w)$, if:

- $x \in \mathtt{dom}(\mu)$ iff there is a σ such that $x{:}\sigma \in \Sigma$.
- For all $x{:}\sigma \in \Sigma$, $D(w) \vdash \mu(x) : \sigma$.

Lemma 3.2.

1. *If* $\Sigma \vdash t : \sigma$ *and* $\Sigma \ll \mu : (\mathcal{K}, w)$*, then* $D(w) \vdash t\mu : \sigma$*.*
2. *If* $\Sigma \vdash c\ \mathsf{ok}$ *and* $\Sigma \ll \mu : (\mathcal{K}, w)$*, then* $D(w) \vdash c\mu\ \mathsf{ok}$*.*
3. *If* $\Sigma \vdash s\ \mathsf{ok}$ *and* $\Sigma \ll \mu : (\mathcal{K}, w)$*, then* $D(w) \vdash s\mu\ \mathsf{ok}$*.*

Proof. By induction on t, c, and s respectively. □

The above Lemma is necessary to ensure that many statements in the definitions of satisfaction are well-typed.

Lemma 3.3. *If* $\Sigma; \Gamma \rhd c$ *and* $\Sigma \ll \mu : (\mathcal{K}, w)$ *then* $D(w); \Gamma\mu \rhd c\mu$*.*

Proof. Suppose $\Sigma; \Gamma \rhd c$ and $\Sigma \ll \mu : (\mathcal{K}, w)$. By Lemma 3.2, $D(w) \vdash c\mu\ \mathsf{ok}$, so the conclusion makes sense. From the assumption $\Sigma; \Gamma \rhd c$ and (C-weaken) we get $\Sigma, D(w); \Gamma \rhd c$. By (C-subst) and (C-strengthen), $D(w); \Gamma\mu \rhd c\mu$. □

3.2 Satisfaction

Satisfaction for closed judgements. Next, we define satisfaction for closed formulas. Given a Kripke structure $\mathcal{K}$ and a world w, we define the relation $w \models s$ when $D(w) \vdash s\ \mathsf{ok}$ as follows:

- $w \models c$ iff $c \in \pi(w)$
- $w \models P(t_1, \ldots, t_n) \circ [u_1, u_2]$ iff $(t_1, \ldots, t_n) \in \rho(w, [\mathsf{ev}(u_1), \mathsf{ev}(u_2)])(P)$
- $w \models s@[t_1, t_2] \circ [u_1, u_2]$ iff $w \models s \circ [t_1, t_2]$.
- $w \models s_1 \wedge s_2 \circ [u_1, u_2]$ iff $w \models s_1 \circ [u_1, u_2]$ and $w \models s_2 \circ [u_1, u_2]$
- $w \models s_1 \vee s_2 \circ [u_1, u_2]$ iff $w \models s_1 \circ [u_1, u_2]$ or $w \models s_2 \circ [u_1, u_2]$
- $w \models s_1 \supset s_2 \circ [u_1, u_2]$ iff for all $[u_1', u_2'] \subseteq [\mathsf{ev}(u_1), \mathsf{ev}(u_2)]$ and all w', $w \leq_i w'$ and $w \models s_1 \circ [u_1', u_2']$ imply $w' \models s_2 \circ [u_1', u_2']$
- $w \models \top \circ [u_1, u_2]$ always

- $w \models \bot \circ [u_1, u_2]$ never
- $w \models \forall x{:}\sigma.s \circ [u_1, u_2]$ iff for all w, $w \leq_i w'$ and $D(w) \vdash t : \sigma$ imply $w \models s \circ [u_1, u_2][t/x]$
- $w \models \exists x{:}\sigma.s \circ [u_1, u_2]$ iff there is a term t such that $D(w) \vdash t : \sigma$ and $w \models s \circ [u_1, u_2][t/x]$
- $w \models u_1 \leq u_2$ iff $\mathsf{ev}(u_1) \leq \mathsf{ev}(u_2)$
- $w \models k$ says $s \circ [u_1, u_2]$ iff for every $[u_1', u_2'] \subseteq [\mathsf{ev}(u_1), \mathsf{ev}(u_2)]$ and every $[u_1', u_2']$-world w' with $w \leq_i \leq_s w'$ and $k \in \theta(w')$, $w' \models s \circ [u_1, u_2]$
- $w \models k$ claims $s \circ [u_1, u_2]$ iff $w \models k$ says $s \circ [u_1, u_2]$

Satisfaction for sequents. Given a Kripke structure $\mathcal{K}$, we say that $\mathcal{K} \models (\Sigma; \Gamma \xrightarrow{k,u_1,u_2} s \circ [t_1, t_2])$ iff:

- For every μ, every $[u_1', u_2'] \subseteq [\mathsf{ev}(u_1\mu), \mathsf{ev}(u_2\mu)]$ and every $[u_1', u_2']$-world $w \in \mathcal{K}$, $\Sigma \ll \mu : (\mathcal{K}, w)$, $k\mu \in \theta(w)$ and $w \models \Gamma\mu$ imply $w \models (s \circ [t_1, t_2])\mu$

3.3 Soundness

We prove that the sequent calculus is sound with respect to the Kripke semantics. We start by proving a standard Lemma.

Lemma 3.4 (Monotonicity). *If $w \models s \circ [u_1, u_2]$, $w \leq_i w'$ and $[\mathsf{ev}(u_1'), \mathsf{ev}(u_2')] \subseteq [\mathsf{ev}(u_1), \mathsf{ev}(u_2)]$, then $w' \models s \circ [u_1', u_2']$.*

Proof. By induction on s and case analysis of the form of s.

Case. $s = P(t_1, \ldots, t_n)$. The condition $w \models s \circ [u_1, u_2]$ implies $(t_1, \ldots, t_n) \in \rho(w, [\mathsf{ev}(u_1), \mathsf{ev}(u_2)])(P)$. By (K-mon), $w \leq_i w'$ and $[\mathsf{ev}(u_1'), \mathsf{ev}(u_2')] \subseteq [\mathsf{ev}(u_1), \mathsf{ev}(u_2)]$, we know that $\rho(w, [\mathsf{ev}(u_1), \mathsf{ev}(u_2)])(P) \subseteq \rho(w', [\mathsf{ev}(u_1'), \mathsf{ev}(u_2')])(P)$. Hence, $(t_1, \ldots, t_n) \in \rho(w', [\mathsf{ev}(u_1'), \mathsf{ev}(u_2')])(P)$ or, equivalently, $w' \models s \circ [u_1', u_2']$ as required.

Case. $s = s'@[u_b, u_e]$. Suppose $w \models s \circ [u_1, u_2]$, $w \leq_i w'$ and $[\mathsf{ev}(u_1'), \mathsf{ev}(u_2')] \subseteq [\mathsf{ev}(u_1), \mathsf{ev}(u_2)]$. Then by definition, $w \models s' \circ [u_b, u_e]$. Then by i.h., $w' \models s' \circ [u_b, u_e]$. But then by definition $w' \models s \circ [u_1', u_2']$, as required.

Case. $s = s_1 \wedge s_2$. Suppose $w \models s \circ [u_1, u_2]$, $w \leq_i w'$ and $[\mathsf{ev}(u_1'), \mathsf{ev}(u_2')] \subseteq [\mathsf{ev}(u_1), \mathsf{ev}(u_2)]$. Then, by definition of $\models$, $w \models s_1 \circ [u_1, u_2]$ and $w \models s_2 \circ [u_1, u_2]$. By i.h., $w' \models s_1 \circ [u_1', u_2']$ and $w' \models s_2 \circ [u_1', u_2']$. Hence, $w' \models s_1 \wedge s_2 \circ [u_1', u_2']$ or, equivalently, $w' \models s \circ [u_1', u_2']$.

Case. $s = s_1 \vee s_2$. Suppose $w \models s \circ [u_1, u_2]$, $w \leq_i w'$ and $[\mathsf{ev}(u_1'), \mathsf{ev}(u_2')] \subseteq [\mathsf{ev}(u_1), \mathsf{ev}(u_2)]$. Then, by definition of $\models$, either $w \models s_1 \circ [u_1, u_2]$ or $w \models s_2 \circ [u_1, u_2]$. Suppose $w \models s_1 \circ [u_1, u_2]$ (the other case is symmetric). By i.h., $w' \models s_1 \circ [u_1', u_2']$. Hence, $w' \models s_1 \vee s_2 \circ [u_1', u_2']$ or, equivalently, $w' \models s \circ [u_1', u_2']$.

Case. $s = s_1 \supset s_2$. Suppose $w \models s_1 \supset s_2 \circ [u_1, u_2]$, $w \leq_i w'$ and $[\mathsf{ev}(u_1'), \mathsf{ev}(u_2')] \subseteq [\mathsf{ev}(u_1), \mathsf{ev}(u_2)]$. We want to show $w' \models s_1 \supset s_2 \circ [u_1', u_2']$. To prove that, pick an arbitrary world w'' such that $w' \leq_i w''$ and an arbitrary interval $[u_1'', u_2'']$ such that $[u_1'', u_2''] \subseteq [\mathsf{ev}(u_1'), \mathsf{ev}(u_2')]$. It suffices to prove that $w'' \models s_1 \circ [u_1'', u_2'']$ implies $w'' \models s_2 \circ [u_1'', u_2'']$. However, observe that $w \leq_i w' \leq_i w''$, so $w \leq_i w''$. Furthermore, $[u_1'', u_2''] \subseteq [\mathsf{ev}(u_1'), \mathsf{ev}(u_2')] \subseteq [\mathsf{ev}(u_1), \mathsf{ev}(u_2)]$, so $[u_1'', u_2''] \subseteq [\mathsf{ev}(u_1), \mathsf{ev}(u_2)]$. By definition of satisfaction on the assumption $w \models s_1 \supset s_2 \circ [u_1, u_2]$, we get that $w'' \models s_1 \circ [u_1'', u_2'']$ implies $w'' \models s_2 \circ [u_1'', u_2'']$, as required.

Case. $s = \top$. Then $w' \models s \circ [u_1', u_2']$ follows by definition of $\models$.

Case. $s = \bot$. Here $w' \models s \circ [u_1', u_2']$ vacuously because the assumption $w \models s \circ [u_1, u_2]$ is false by definition of $\models$.

Case. $s = \forall x{:}\sigma.s_1$. Suppose $w \models \forall x{:}\sigma.s_1 \circ [u_1, u_2]$, $w \leq_i w'$ and $[\mathsf{ev}(u_1'), \mathsf{ev}(u_2')] \subseteq [\mathsf{ev}(u_1), \mathsf{ev}(u_2)]$. We want to show that $w' \models \forall x{:}\sigma.s_1 \circ [u_1', u_2']$. Following the definition of $\models$, pick a world w'' and a t such that $w' \leq_i w''$ and $D(w) \vdash t : \sigma$. It suffices to show that $w'' \models s_1[t/x] \circ [u_1', u_2']$. However, $w \leq_i w' \leq_i w''$ implies $w \leq_i w''$. Hence, by definition of satisfaction on the assumptions $w \models \forall x{:}\sigma.s_1 \circ [u_1, u_2]$ and $D(w) \vdash t : \sigma$, we get $w'' \models s_1[t/x] \circ [u_1, u_2]$. By the i.h. we get $w'' \models s_1[t/x] \circ [u_1', u_2']$, as required.

Case. $s = \exists x{:}\sigma.s_1$. Suppose $w \models \exists x{:}\sigma.s_1 \circ [u_1, u_2]$, $w \leq_i w'$ and $[\mathsf{ev}(u_1'), \mathsf{ev}(u_2')] \subseteq [\mathsf{ev}(u_1), \mathsf{ev}(u_2)]$. By definition of $\models$, there is a t such that $D(w) \vdash t : \sigma$ and $w \models s_1[t/x] \circ [u_1, u_2]$. By (K-grow1) and the i.h. respectively, we obtain $D(w) \vdash t : \sigma$ and $w' \models s_1[t/x] \circ [u_1', u_2']$. The last two facts imply $w' \models \exists x{:}\sigma.s_1 \circ [u_1', u_2']$ by definition of $\models$.

Case. $s = k \;\mathsf{says}\; s'$. Suppose $w \models k \;\mathsf{says}\; s' \circ [u_1, u_2]$, $w \leq_i w'$ and $[\mathsf{ev}(u_1'), \mathsf{ev}(u_2')] \subseteq [\mathsf{ev}(u_1), \mathsf{ev}(u_2)]$. We want to show that $w' \models k \;\mathsf{says}\; s' \circ [u_1', u_2']$. Following the definition of $\models$, pick a $[\mathsf{ev}(u_1'), \mathsf{ev}(u_2')]$-world w'' such that $w' \leq_i \leq_s w''$ and $k \in \theta(w'')$. It suffices to show that $w'' \models s' \circ [u_1', u_2']$. We now get $w'' \models s' \circ [u_1, u_2]$ from definition of $\models$ applied to $w' \models k \;\mathsf{says}\; s' \circ [u_1, u_2]$. The required fact $w'' \models s' \circ [u_1', u_2']$ now follows from the i.h. $\square$

Lemma 3.5 (Monotonicity of says)**.** *Suppose that $w \models k \;\mathsf{says}\; \mathsf{s} \circ [u_1, u_2]$ and that w' is a $[\mathsf{ev}(u_1), \mathsf{ev}(u_2)]$-world such that $w \leq_s w'$. Then $w' \models k \;\mathsf{says}\; \mathsf{s} \circ [u_1, u_2]$.*

Proof. Following the definition of $\models$, let $[u_1', u_2'] \subseteq [\mathsf{ev}(u_1), \mathsf{ev}(u_2)]$, and pick a $[u_1', u_2']$-world w'' such that $w' \leq_i \leq_s w''$ and $k \in \theta(w'')$. It suffices to show that $w'' \models s \circ [u_1, u_2]$. However, $w \leq_s \leq_i \leq_s w''$, so by (K-commute) $w \leq_s \leq_s w''$, i.e. $w \leq_s w''$. From definition of $w \models k \;\mathsf{says}\; s \circ [u_1, u_2]$, we have $w'' \models s \circ [u_1, u_2]$, as required. $\square$

Theorem 3.6 (Soundness)**.** *If $\Sigma; \Gamma \xrightarrow{k, u_1, u_2} s \circ [t_1, t_2]$ then for any $\mathcal{K}$, $\mathcal{K} \models (\Sigma; \Gamma \xrightarrow{k, u_1, u_2} s \circ [t_1, t_2])$.*

Proof. By induction on the derivation of $\Sigma; \Gamma \xrightarrow{k,u_1,u_2} s \circ [t_1, t_2]$ and a case analysis the last rule in it. By definition of $\models$, we are trying to prove that for every μ, every $[u_1', u_2'] \subseteq [\mathsf{ev}(u_1\mu), \mathsf{ev}(u_2\mu)]$ and every $[u_1', u_2']$-world w, $\Sigma \ll \mu : (\mathcal{K}, w)$, $k\mu \in \theta(w)$ and $w \models \Gamma\mu$ imply $w \models (s \circ [t_1, t_2])\mu$. We show some interesting cases below.

Case.
$$\frac{\Sigma; \Gamma \rhd u_1' \leq_s u_1 \qquad \Sigma; \Gamma \rhd u_2 \leq_s u_2'}{\Sigma; \Gamma, p \circ [u_1', u_2'] \overset{\nu}{\to} p \circ [u_1, u_2]}\text{init}$$

Assume that $\Sigma \ll \mu : (\mathcal{K}, w)$, $k\mu \in \theta(w)$, and $w \models (\Gamma, p \circ [u_1', u_2'])\mu$. By the last assumption, we obtain $w \models (p \circ [u_1', u_2'])\mu$. From the two premises we can conclude that $[\mathsf{ev}(u_1\mu), \mathsf{ev}(u_2\mu)] \subseteq [\mathsf{ev}(u_1'\mu), \mathsf{ev}(u_2'\mu)]$, so by Lemma 3.4 we get $w \models (p \circ [u_1, u_2])\mu$, as required.

Case.
$$\frac{\begin{array}{c}\Sigma; \Gamma, k \;\mathsf{claims}\; s \circ [u_1, u_2], s \circ [u_1, u_2] \overset{\nu}{\to} r \circ [u_1', u_2'] \\ \nu = k, u_b, u_e \qquad \Sigma; \Gamma \rhd u_1 \leq_s u_b \qquad \Sigma; \Gamma \rhd u_e \leq_s u_2 \qquad \Sigma; \Gamma \rhd k \succeq k_0\end{array}}{\Sigma; \Gamma, k \;\mathsf{claims}\; s \circ [u_1, u_2] \overset{\nu}{\to} r \circ [u_1', u_2']}\text{claims}$$

Assume that $[u_b', u_e'] \subseteq [\mathsf{ev}(u_b\mu), \mathsf{ev}(u_e\mu)]$ and that w is a $[u_b', u_e']$-world such that $\Sigma \ll \mu : (\mathcal{K}, w)$, $k_0\mu \in \theta(w)$ and $w \models (\Gamma, k \;\mathsf{claims}\; s \circ [u_1, u_2])\mu$. We want to show that $w \models (r \circ [u_1', u_2'])\mu$. We have:

1. $\Sigma \ll \mu : (\mathcal{K}, w)$, $k_0\mu \in \theta(w)$, and $w \models (\Gamma, k \;\mathsf{claims}\; s \circ [u_1, u_2], s \circ [u_1, u_2])\mu$ imply $w \models (r \circ [u_1', u_2'])\mu$ (i.h. on 1st premise)
2. $D(w); \Gamma\mu \rhd k\mu \succeq k_0\mu$ (Lemma 3.3 on last premise and $\Sigma \ll \mu : (\mathcal{K}, w)$)
3. $C(\Gamma\mu) \subseteq \pi(w)$ (Assumption $w \models (\Gamma, k \;\mathsf{claims}\; s)\mu$, definition of $\models$)
4. $(k\mu \succeq k_0\mu) \in \pi(w)$ (2, 3 and (K-consclosure))
5. $k\mu \in \theta(w)$ ((K-viewcl) on 4)
6. $[\mathsf{ev}(u_b\mu), \mathsf{ev}(u_e\mu)] \subseteq [\mathsf{ev}(u_1\mu), \mathsf{ev}(u_2\mu)]$ (3rd an 4th premise)
7. $[u_b', u_e'] \subseteq [\mathsf{ev}(u_1\mu), \mathsf{ev}(u_2\mu)]$ ($[u_b', u_e'] \subseteq [\mathsf{ev}(u_b\mu), \mathsf{ev}(u_e\mu)]$ and 6)
8. $w \leq_i \leq_s w$ ($\leq_i$ and $\leq_s$ is reflexive)
9. $w \models k\mu \;\mathsf{says}\; s\mu \circ [u_1\mu, u_2\mu]$ (Assumption $w \models (\Gamma, k \;\mathsf{claims}\; s)\mu$)
10. $w \models (s \circ [u_1, u_2])\mu$ (5, 7–9, w is a $[u_b', u_e']$-world, definition of $\models$)
11. $w \models (\Gamma, k \;\mathsf{claims}\; s \circ [u_1, u_2], s \circ [u_1, u_2])\mu$

    (Assumption $w \models (\Gamma, k \;\mathsf{claims}\; s \circ [u_1, u_2])\mu$ and 10)
12. $w \models (r \circ [u_1', u_2'])\mu$ (1, 11 and assumptions $\Sigma \ll \mu : (\mathcal{K}, w)$ and $k_0\mu \in \theta(w)$)

Case. $\dfrac{\Sigma; \Gamma \xrightarrow{\nu} s \circ [u_1, u_2]}{\Sigma; \Gamma \xrightarrow{\nu} (s@[u_1, u_2]) \circ [u_1', u_2']}@\mathrm{R}$

Assume that $\Sigma \ll \mu : (\mathcal{K}, w)$, $k_0\mu \in \theta(w)$, and $w \models \Gamma\mu$. By i.h., $w \models s \circ [u_1\mu, u_2\mu]$, so by definition of $\models$, we have $w \models (s\mu@[u_1\mu, u_2\mu]) \circ [u_1'\mu, u_2'\mu]$, as required.

Case. $\dfrac{\Sigma; \Gamma \xrightarrow{\nu} (s@[u_1, u_2]) \circ [u_1', u_2'] \qquad \Sigma; \Gamma, s \circ [u_1, u_2] \xrightarrow{\nu} s' \circ [u_1'', u_2'']}{\Sigma; \Gamma \xrightarrow{\nu} s' \circ [u_1'', u_2'']}@\mathrm{L}$

Assume that $\Sigma \ll \mu : (\mathcal{K}, w)$, $k_0\mu \in \theta(w)$, and $w \models \Gamma\mu$. We want to show that $w \models s'\mu \circ [u_1''\mu, u_2''\mu]$. By i.h. applied to $\Sigma; \Gamma \xrightarrow{\nu} (s@[u_1, u_2]) \circ [u_1', u_2']$, we have that $w \models (s\mu@[u_1\mu, u_2\mu]) \circ [u_1'\mu, u_2'\mu]$. By the definition of $\models$, it follows that $w \models s\mu \circ [u_1\mu, u_2\mu]$. Then by i.h. applied to $\Sigma; \Gamma, s \circ [u_1, u_2] \xrightarrow{\nu} s' \circ [u_1'', u_2'']$, we get $w \models s'\mu \circ [u_1''\mu, u_2''\mu]$, as required.

Assume that $\Sigma \ll \mu : (\mathcal{K}, w)$, $k_0\mu \in \theta(w)$, and $w \models \Gamma\mu$. By i.h., $w \models s \circ [u_1\mu, u_2\mu]$, so by definition of $\models$, we have $w \models (s\mu@[u_1\mu, u_2\mu]) \circ [u_1'\mu, u_2'\mu]$, as required.

Case. $\dfrac{\Sigma; \Gamma| \xrightarrow{k, u_1, u_2} s \circ [u_1, u_2]}{\Sigma; \Gamma \xrightarrow{\nu} (k \ \mathsf{says}\ s) \circ [u_1, u_2]}\mathsf{saysR}$

Assume that $\Sigma \ll \mu : (\mathcal{K}, w)$, $k_0\mu \in \theta(w)$, and $w \models \Gamma\mu$. We want to show that $w \models k\mu \ \mathsf{says}\ s\mu \circ [u_1\mu, u_2\mu]$. Following the definition of $\models$, pick any $[u_1', u_2'] \subseteq [u_1\mu, u_2\mu]$ and any $[u_1', u_2']$-world w' such that $w \leq_i \leq_s w'$ and $k\mu \in \theta(w')$. It suffices to show that $w' \models (s \circ [u_1, u_2])\mu$. Now observe that by assumption, $w \models \Gamma\mu$. Hence, in particular, $w \models (\Gamma|)\mu$. By Lemmas 3.4 and 3.5, $w' \models (\Gamma|)\mu$. (Note that $\Gamma|$ only contains assumptions of the form $k' \ \mathsf{claims}\ s' \circ [u_b, u_e]$, so Lemma 3.5 can be applied.)

Next, we have the assumption $\Sigma \ll \mu : (\mathcal{K}, w)$. Since $D(w) \subseteq D(w')$ by (K-grow1) and (K-grow2), it follows from definition of $\ll$ that $\Sigma \ll \mu : (\mathcal{K}, w')$. Further, $k\mu \in \theta(w')$ by assumption and we just proved $w' \models (\Gamma|)\mu$. Applying the i.h. to the premise (at w', not w), and using the last three facts, we immediately obtain $w' \models (s \circ [u_1, u_2])\mu$, as required.

Case. $\dfrac{\Sigma, x_1 : \mathsf{time}, x_2 : \mathsf{time}; \Gamma, u_1 \leq x_1, x_2 \leq u_2, s \circ [x_1, x_2] \xrightarrow{\nu} s' \circ [x_1, x_2]}{\Sigma; \Gamma \xrightarrow{\nu} s \supset s' \circ [u_1, u_2]}\supset\mathrm{R}$

Assume that $\Sigma \ll \mu : (\mathcal{K}, w)$, $k\mu \in \theta(w)$, and $w \models \Gamma\mu$. We want to show that $w \models s\mu \supset s'\mu \circ [u_1, u_2]$. Following the definition of $\models$, pick any $[u_1', u_2'] \subseteq [\mathsf{ev}(u_1\mu), \mathsf{ev}(u_2\mu)]$ and any w' such that $w \leq_i w'$ and $w' \models s\mu \circ [u_1', u_2']$. It suffices to show that $w' \models s'\mu \circ [u_1', u_2']$. Define $\mu' := \mu \cup \{x_1 \mapsto u_1', x_2 \mapsto u_2'\}$. Then $w' \models (s \circ [x_1, x_2])\mu$, and it suffices to show $w' \models (s' \circ [x_1, x_2])\mu$. By Lemma 3.4, $w' \models \Gamma\mu$, i.e. $w' \models \Gamma\mu'$. Hence, $w' \models (\Gamma, s \circ [x_1, x_2])\mu'$. By (K-viewmon), $k\mu' \in \theta(w')$. By i.h. on the premise at w', we get $w' \models (s' \circ [x_1, x_2])\mu'$, as required.

□

3.4 Completeness

Next, we prove that our Kripke semantics is also complete. In order to do that we build a canonical Kripke model and show that satisfaction in that model entails provability. We assume a countably infinite universe $\mathcal{U}$ of first-order symbols. Since the logic has a finite signature, there are countably infinite number of symbols outside of this signature in $\mathcal{U}$. All sets denoted S in the following are assumed to be subsets of $\mathcal{U}$.

Definition 3.7 (Theory)**.** A theory is a quadruple $(S, \Gamma, K, [u_1, u_2])$ where S is a (possibly infinite) sorting disjoint from the logic's signature, Γ is a (possibly infinite) set of formulas well-formed over S, K is a (possibly infinite) set of terms of sort $\mathsf{principal}$ under S and $[u_1, u_2] \in (\mathbb{Z} \cup \{-\infty, +\infty\})^2$.

Definition 3.8 (Filter)**.** A set K of terms of sort $\mathsf{principal}$ in sorting S is called a filter with respect to S and Γ (written $(S, \Gamma) \curlyvee K$) if there is term $k_m \in K$ such that $K = \{k \mid S; \Gamma \rhd k \succeq k_m\}$. (So K contains both a least element k_m under the order $\succeq$.)

Definition 3.9 (Prime theory)**.** We call a theory $(S, \Gamma, K, [u_1, u_2])$ prime if the following hold:

1. (Prin-closure) $(S, \Gamma) \curlyvee K$.
2. (Fact-closure) If $k \in K$ and $S; \Gamma \xrightarrow{k,u_1',u_2'} s \circ [t_1, t_2]$ and $[u_1, u_2] \subseteq [\mathsf{ev}(u_1'), \mathsf{ev}(u_2')]$, then $s \circ [t_1, t_2] \in \Gamma$.
3. (Primality1) If $s_1 \vee s_2 \circ [t_1, t_2] \in \Gamma$, then either $s_1 \circ [t_1, t_2] \in \Gamma$ or $s_2 \circ [t_1, t_2] \in \Gamma$.
4. (Primality2) If $\exists x{:}\sigma.s \circ [t_1, t_2] \in \Gamma$, then there is a term t such that $S \vdash t : \sigma$ and $s \circ [t_1, t_2][t/x] \in \Gamma$.
5. (Primality3) $\bot \circ [t_1, t_2] \notin \Gamma$ for any t_1, t_2.
6. (Primality4) If c is a constraint such that $c \circ [t_1, t_2] \in \Gamma$, then $S; \Gamma \rhd c$.

We take as worlds of our canonical model prime theories.

Definition 3.10 (Canonical model)**.** The canonical Kripke model for BL is defined as $(W, \leq_i, \leq_s, T, D, \pi, \rho, \theta)$, where:

- $W = \{(S, \Gamma, K, [u_1, u_2]) \mid (S, \Gamma, K, [u_1, u_2])$ is a prime theory$\}$
- $(S, \Gamma, K, [u_1, u_2]) \leq_i (S', \Gamma', K', [u_1', u_2'])$ iff $S \subseteq S'$, $\Gamma \subseteq \Gamma'$, $K \subseteq K'$ and $[u_1, u_2] = [u_1', u_2']$.
- $(S, \Gamma, K, [u_1, u_2]) \leq_s (S', \Gamma', K', [u_1', u_2'])$ iff $S \subseteq S'$ and for all k, s, k says $s \circ [t_1, t_2] \in \Gamma$, $k \in K'$ and $[u_1', u_2'] \subseteq [\mathsf{ev}(t_1), \mathsf{ev}(t_2)]$ imply $s \circ [t_1, t_2] \in \Gamma'$.
- $T((S, \Gamma, K, [u_1, u_2])) = [u_1, u_2]$

- $D((S, \Gamma, K, [u_1, u_2])) = S$.

- $\pi((S, \Gamma, K, [u_1, u_2])) = \{c \mid S; \Gamma \triangleright c\}$

- $(t_1, \ldots, t_n) \in \rho((S, \Gamma, K, [u_1, u_2]), [u'_1, t'_2])(P)$ iff $P(t_1, \ldots, t_n) \circ [u'_1, u'_2] \in \Gamma$.

- $\theta(S, \Gamma, K, [u_1, u_2]) = K$.

Lemma 3.11 (Canonical model is a Kripke model)**.** *The canonical model as defined above is a Kripke model for BL.*

Proof. We verify the conditions in the definition of Kripke models (Section 3).

- $\leq_i$ is trivially reflexive and transitive.

- $\leq_s$ is reflexive: By definition of $\leq_s$ in the canonical model, we need to show that for any prime theory $(S, \Gamma, K, [u_1, u_2])$, (a) $S \subseteq S$ (which is trivial), (b) $[u_1, u_2] \subseteq [u_1, u_2]$ (which is also trivial and (c) $k \;\mathsf{says}\; s \circ [t_1, t_2] \in \Gamma$, $k \in K$ and $[u_1, u_2] \subseteq [t_1, t_2]$ imply $s \circ [t_1, t_2] \in \Gamma$. The latter follows from (Fact-closure) because $S; \Gamma \xrightarrow{k, u_1, u_2} s \circ [t_1, t_2]$ if $k \;\mathsf{says}\; s \circ [t_1, t_2] \in \Gamma$.

- $\leq_s$ is transitive: Suppose $(S_1, \Gamma_1, K_1, [u_1, u'_1]) \leq_s (S_2, \Gamma_2, K_2, [u_2, u'_2]) \leq_s (S_3, \Gamma_3, K_3, [u_3, u'_3])$. We want to show $(S_1, \Gamma_1, K_1, u_1, u'_1]) \leq_s (S_3, \Gamma_3, K_3, [u_3, u'_3])$. Accordingly, we must show that (a) $S_1 \subseteq S_3$, and (b) $k \;\mathsf{says}\; s \circ [t_1, t_2] \in \Gamma_1$, $k \in K_3$ and $[u_3, u'_3] \subseteq [\mathsf{ev}(t_1), \mathsf{ev}(t_2)]$ imply $s \circ [t_1, t_2] \in \Gamma_3$. (a) follows because $S_1 \subseteq S_2 \subseteq S_3$. To prove (b), observe that because $(S_1, \Gamma_1, K_1, [u_1, u'_1])$ and $(S_2, \Gamma_2, K_2, [u_2, u'_2])$ are prime theories, both K_1 and K_2 are non-empty. So let $k_1 \in K_1$ and $k_2 \in K_2$. Since $k \;\mathsf{says}\; s \circ [t_1, t_2] \in \Gamma_1$, we have $\Gamma_1 \xrightarrow{k_2, u_2, u'_2} (k \;\mathsf{says}\; s)@[t_1, t_2] \circ [u_2, u'_2]$, i.e. $S_1; \Gamma_1 \xrightarrow{k_1, u_1, u'_1} k_2 \;\mathsf{says}\; ((k \;\mathsf{says}\; s)@[t_1, t_2]) \circ [u_2, u'_2]$. From (Fact-closure), we get $k_2 \;\mathsf{says}\; ((k \;\mathsf{says}\; s)@[t_1, t_2]) \circ [u_2, u'_2] \in \Gamma_1$. So $(k \;\mathsf{says}\; s)@[t_1, t_2] \circ [u_2, u'_2] \in \Gamma_2$ by the definition of $\leq_s$. Hence $S_2; \Gamma_2 \xrightarrow{k_2, u_2, u'_2} k \;\mathsf{says}\; s \circ [t_1, t_2]$, i.e. by (Fact-closure) $k \;\mathsf{says}\; s \circ [t_1, t_2] \in \Gamma_2$. Finally, because $k \in K_3$, $s \circ [t_1, t_2] \in \Gamma_3$, as required.

- (K-commute) Suppose $(S_1, \Gamma_1, K_1, [u_1, u'_1]) \leq_i (S_2, \Gamma_2, K_2, [u_2, u'_2]) \leq_s (S_3, \Gamma_3, K_3, [u_3, u'_3])$. We need to show that $(S_1, \Gamma_1, K_1, [u_1, u'_1]) \leq_s (S_3, \Gamma_3, K_3, [u_3, u'_3])$. By definition of $\leq_s$ in the canonical model, we must check two conditions: (a) $S_1 \subseteq S_3$, and (b) $k \;\mathsf{says}\; s \circ [t_1, t_2] \in \Gamma_1$, $k \in K_3$ and $[u_3, u'_3] \subseteq [t_1, t_2]$ imply $s \circ [t_1, t_2] \in \Gamma_3$. (a) follows immediately because $S_1 \subseteq S_2 \subseteq S_3$. To prove (b), observe that $k \;\mathsf{says}\; s \circ [t_1, t_2] \in \Gamma_1$ implies $k \;\mathsf{says}\; s \circ [t_1, t_2] \in \Gamma_2$ (because $\Gamma_1 \subseteq \Gamma_2$). Therefore, the definition of $(S_2, \Gamma_2, K_2) \leq_s (S_3, \Gamma_3, K_3)$ in the canonical model implies that $s \circ [t_1, t_2] \in \Gamma_3$, as required.

- (T-mon) directly follows from the definitions of $\leq_i$ and T in the canonical model.

- (K-fresh) follows from the requirement that $D(S, \Gamma, K, [u_1, u_2]) = S$ in a theory be disjoint from the logic's signature.

- (K-grow1) $D(S, \Gamma, K, [u_1, u_2]) = S = D(S, \Gamma, K, [u_1, u_2])$.
- (K-grow2) Suppose $(S_1, \Gamma_1, K_1, [u_1, u_1']) \leq_s (S_2, \Gamma_2, K_2, [u_2, u_2'])$. Then, by definition of $\leq_s$ in the canonical model we get $D(S_1, \Gamma_1, K_1, [u_1, u_1']) = S_1 \subseteq S_2 = D(S_2, \Gamma_2, K_2, [u_2, u_2'])$.
- (K-conclosure) Suppose $C(\Gamma') \subseteq \pi((S, \Gamma, K, [u_1, u_2]))$ and $S; \Gamma' \rhd c$. Then by the definition of π, $S; \Gamma \rhd c'$ for every constrain $c' \in \Gamma'$. Additionally, $S; \Gamma, \Gamma' \rhd c$ by (C-weaken). So by (C-cut), $S; \Gamma \rhd c$, i.e. $c \in \pi((S, \Gamma, K, [u_1, u_2]))$, as required.
- (K-mon) Suppose $(S, \Gamma, K, [u_1, u_2]) \leq_i (S', \Gamma', K', [u_1', u_2'])$ and $[u_b', u_e'] \subseteq [u_e, u_e]$. We want to show that $\rho((S, \Gamma, K, [u_1, u_2]), [u_b, u_e])(P) \subseteq \rho((S', \Gamma', K', [u_1', u_2']), [u_b', u_e'])(P)$. Suppose $(t_1, \ldots, t_n) \in \rho((S, \Gamma, K, [u_1, u_2]), [u_b, u_e])(P)$. By definition of the canonical model, $P(t_1, \ldots, t_n) \circ [u_b, u_e] \in \Gamma$. Since $\Gamma \subseteq \Gamma'$, $P(t_1, \ldots, t_n) \circ [u_b, u_e] \in \Gamma'$. Let $k \in K$. In the sequent calculus, $S'; \Gamma' \xrightarrow{k, u_1', u_2'} P(t_1, \ldots, t_n) \circ [u_b', u_e']$, so by (Fact-closure), $P(t_1, \ldots, t_n) \circ [u_b', u_e'] \in \Gamma'$, or, equivalently, $(t_1, \ldots, t_n) \in \rho((S', \Gamma', K', [u_1', u_2']), [u_b', u_e'])(P)$, as required.
- (K-prin) and (K-time) directly follow from (Fact-closure) and (Primality4).
- (K-viewmon) Suppose $k \in \theta(S_1, \Gamma_1, K_1) = K_1$ and $(S_1, \Gamma_1, K_1) \leq_i (S_2, \Gamma_2, K_2)$. We need to show that $k \in \theta(S_2, \Gamma_2, K_2) = K_2$. However, this is trivial because $K_1 \subseteq K_2$ by definition of $\leq_i$ in the canonical model.
- (K-viewcl) Suppose $k \in \theta((S, \Gamma, K, [u_1, u_2])) = K$ and $(k' \succeq k) \in \pi((S, \Gamma, K, [u_1, u_2]))$. We need to show that $k' \in K$. By the definition of $\pi((S, \Gamma, K, [u_1, u_2]))$, $S; \Gamma \rhd k' \succeq k$. From (Prin-closure), it follows that there is a $k_m \in K$ such that $S; \Gamma \rhd k \succeq k_m$. Using (C-trans-prin), $S; \Gamma \rhd k' \succeq k_m$. Since $K = \{k \mid S; \Gamma \rhd k \succeq k_m\}$, $k' \in K$, as required.

□

Definition 3.12 (s-consistent theory)**.** If $S \vdash s$ ok, we say that a (not necessarily prime) theory $(S, \Gamma, K, [u_1, u_2])$ is $(s \circ [t_1, t_2])$-consistent if for all $k \in K$, $S; \Gamma \not\xrightarrow{k, u_1, u_2} s \circ [t_1, t_2]$.

Lemma 3.13 (Consistent extensions)**.** *Suppose* $(S, \Gamma, K, [u_1, u_2])$ *is* $(s \circ [t_1, t_2])$*-consistent and* $(S, \Gamma) \curlyvee K$*. Then there is a prime theory* (S^*, Γ^*, K^*) *such that* $S \subseteq S^*$*,* $\Gamma \subseteq \Gamma^*$*,* $K \subseteq K^*$*, and* $(S^*, \Gamma^*, K^*, [u_1, u_2])$ *is* $(s \circ [t_1, t_2])$*-consistent.*

Proof. Our proof follows a similar construction for hybrid propositional logic in [3], although the construction in that paper does not consider views. Because $(S, \Gamma) \curlyvee K$, there is a $k_m \in K$ such that $K = \{k \mid S; \Gamma \rhd k \succeq k_m\}$. We inductively construct a sequence of pairs (S_n, Γ_n) with $(S_0, \Gamma_0) = (S, \Gamma)$, satisfying the following properties:

1. $S_n \subseteq S_{n+1}$ and $\Gamma_n \subseteq \Gamma_{n+1}$.
2. For each $s_n \circ [u_n, u_n'] \in \Gamma_n$, $S_n \vdash s_n$ ok
3. $S_n; \Gamma_n \not\xrightarrow{k_m} s \circ [t_1, t_2]$.

Fix an enumeration E of all (possibly ill-typed) judgements of the form $s' \circ [u_b, u_e]$ that can be created using the symbols in the logic's signature and those in $\mathcal{U}$. The intuitive idea of our construction is to alternately look at formulas of the forms $s_1 \vee s_2 \circ [u_b, u_e]$ and $\exists x{:}\sigma.s' \circ [u_b, u_e]$ that can be proved from the sets constructed so far, and to complete the primality conditions for them. We keep track of formulas we have already looked at through two sequences of sets $\mathit{treated}_n^{\vee}$ and $\mathit{treated}_n^{\exists}$. We set $\mathit{treated}_0^{\vee} = \mathit{treated}_0^{\exists} = \emptyset$. To define S_{n+1}, Γ_{n+1}, $\mathit{treated}_{n+1}^{\vee}$ and $\mathit{treated}_{n+1}^{\exists}$, we case analyze the parity of $n+1$. We also simultaneously prove the conditions (1)–(3) for S_{n+1} and Γ_{n+1}.

Case. $n+1$ is even. Let $s_1 \vee s_2 \circ [u_b, u_e]$ be the first judgement in the enumeration E with a top level disjunction that satisfies two conditions: (a) $S_n; \Gamma_n \xrightarrow{k_m,u_1,u_2} s_1 \vee s_2 \circ [u_b, u_e]$, and (b) $s_1 \vee s_2 \circ [u_b, u_e] \notin \mathit{treated}_n^{\vee}$. (If no such formula exists, set $S_{n+1} = S_n$, $\Gamma_{n+1} = \Gamma_n$, $\mathit{treated}_{n+1}^{\vee} = \mathit{treated}_n^{\vee}$, and $\mathit{treated}_{n+1}^{\exists} = \mathit{treated}_n^{\exists}$.) Now we argue that either $S_n; \Gamma_n, s_1 \circ [u_b, u_e] \not\xrightarrow{k_m,u_1,u_2} s \circ [t_1, t_2]$ or $S_n; \Gamma_n, s_2 \circ [u_b, u_e] \not\xrightarrow{k_m,u_1,u_2} s \circ [t_1, t_2]$. Suppose on the contrary that $S_n; \Gamma_n, s_1 \circ [u_b, u_e] \xrightarrow{k_m,u_1,u_2} s \circ [t_1, t_2]$ and $S_n; \Gamma_n, s_2 \circ [u_b, u_e] \xrightarrow{k_m,u_1,u_2} s \circ [t_1, t_2]$. Then, $S_n; \Gamma_n, s_1 \vee s_2 \circ [u_b, u_e] \xrightarrow{k_m,u_1,u_2} s \circ [t_1, t_2]$. Because $S_n; \Gamma_n \xrightarrow{k_m,u_1,u_2} s_1 \vee s_2 \circ [u_b, u_e]$, by the cut principle, we also obtain $S_n; \Gamma_n \xrightarrow{k_m,u_1,u_2} s \circ [t_1, t_2]$, which contradicts condition (2) for (S_n, Γ_n). Hence, either $S_n; \Gamma_n, s_1 \circ [u_b, u_e] \not\xrightarrow{k_m,u_1,u_2} s \circ [t_1, t_2]$ or $S_n; \Gamma_n, s_2 \circ [u_b, u_e] \not\xrightarrow{k_m,u_1,u_2} s \circ [t_1, t_2]$. In the former case, set $\Gamma_{n+1} = \Gamma_n, s_1 \circ [u_b, u_e]$; in the latter case set $\Gamma_{n+1} = \Gamma_n, s_2 \circ [u_b, u_e]$. In both cases, set $S_{n+1} = S_n$, $\mathit{treated}_{n+1}^{\vee} = \mathit{treated}_n^{\vee}, s_1 \vee s_2$, and $\mathit{treated}_{n+1}^{\exists} = \mathit{treated}_n^{\exists}$.

Condition (1) holds by construction. Condition (2) holds because $S_n; \Gamma_n \xrightarrow{k_m,u_1,u_2} s_1 \vee s_2 \circ [u_b, u_e]$, so $S_n = S_{n+1} \vdash s_i\ \mathsf{ok}$. Condition (3) holds at $n+1$ by construction.

Case. $n+1$ is odd. Let $\exists x{:}\sigma.s' \circ [u_b, u_e]$ be the first formula in the enumeration E with a top level existential quantification that satisfies two conditions: (a) $S_n; \Gamma_n \xrightarrow{k_m,u_1,u_2} \exists x{:}\sigma.s' \circ [u_b, u_e]$, and (b) $\exists x{:}\sigma.s' \circ [u_b, u_e] \notin \mathit{treated}_n^{\exists}$. (If no such formula exists, set $S_{n+1} = S_n$, $\Gamma_{n+1} = \Gamma_n$, $\mathit{treated}_{n+1}^{\vee} = \mathit{treated}_n^{\vee}$, and $\mathit{treated}_{n+1}^{\exists} = \mathit{treated}_n^{\exists}$.) Pick a fresh constant $a \in \mathcal{U}$. Set $S_{n+1} = S_n, a{:}\sigma$, $\Gamma_{n+1} = \Gamma_n, s' \circ [u_b, u_e][a/x]$, $\mathit{treated}_{n+1}^{\vee} = \mathit{treated}_n^{\vee}$, and $\mathit{treated}_{n+1}^{\exists} = \mathit{treated}_n^{\exists}, \exists x{:}\sigma.s' \circ [u_b, u_e]$.

Condition (1) holds by construction. Condition (2) holds: $S_{n+1} \vdash s'[a/x]\ \mathsf{ok}$ because $S_{n+1} \vdash a : \sigma$ and $S_n, x{:}\sigma \vdash s'\ \mathsf{ok}$. To prove that condition (3) holds for $n+1$, we reason by contradiction. Suppose not. Then, $S_{n+1}; \Gamma_{n+1} \xrightarrow{k_m,u_1,u_2} s \circ [t_1, t_2]$ or, equivalently, $S_n, a{:}\sigma; \Gamma_n, s' \circ [u_b, u_e][a/x] \xrightarrow{k_m,u_1,u_2} s \circ [t_1, t_2]$. From the latter we derive $S_n; \Gamma_n, \exists x{:}\sigma.s' \circ [u_b, u_e] \xrightarrow{k_m,u_1,u_2} s \circ [t_1, t_2]$. Since $S_n; \Gamma_n \xrightarrow{k_m,u_1,u_2} \exists x{:}\sigma.s' \circ [u_b, u_e]$, by the cut principle, $S_n; \Gamma_n \xrightarrow{k_m,u_1,u_2} s \circ [t_1, t_2]$, which contradicts condition (3) for n. Hence (3) must hold at $n+1$.

This completes our inductive construction. Let $S^* = \cup_i S_i$, $\Gamma' = \cup_i \Gamma_i$, and $K^* =$

$\{k \mid S^*, \Gamma' \rhd k \succeq k_m\}$. Finally, define $\Gamma^* = \{c \mid c$ is a contraint s.t. for some u_b, u_e, we have $S^*; \Gamma' \xrightarrow{k_m,u_1,u_2} c \circ [u_b, u_e]\} \cup \{s^* \circ [u_b, u_e] \mid S^*; \Gamma' \xrightarrow{k_m,u_1,u_2} s^* \circ [u_b, u_e]\}$.

Clearly, $(S^*, \Gamma^*, K^*, [u_1, u_2])$ is a theory. Also, by construction, $S = S_0 \subseteq S^*$ and $\Gamma = \Gamma_0 \subseteq \Gamma' \subseteq \Gamma^*$ ($\Gamma' \subseteq \Gamma^*$ follows from the identity principle of the sequent calculus). Further, $K \subseteq K^*$ because for every k, $S; \Gamma \rhd k \succeq k_m$ implies $S^*, \Gamma' \rhd k \succeq k_m$ by (C-weaken).

Next, we check that $(S^*, \Gamma^*, K^*, [u_1, u_2])$ is $(s \circ [t_1, t_2])$-consistent. Suppose for the sake of contradiction that it is not. Then, it follows that $S^*; \Gamma^* \xrightarrow{k,u_1,u_2} s \circ [t_1, t_2]$ for some $k \in K^*$. Hence, there are finite subsets $S^f \subseteq S^*$ and $\Gamma^f \subseteq \Gamma^*$ such that $S^f; \Gamma^f \xrightarrow{k,u_1,u_2} s \circ [t_1, t_2]$. By the view subsumption principle (Theorem 4.3 of [6]), $S^f; \Gamma^f \xrightarrow{k_m,u_1,u_2} s \circ [t_1, t_2]$. Since each $s^* \circ [u_b, u_e]$ in Γ^f satisfies $S^*; \Gamma' \xrightarrow{k_m} s^* \circ [u_b, u_e]$, it follows by $|\Gamma^f|$ applications of the cut principle that $S^*; \Gamma' \xrightarrow{k_m} s \circ [t_1, t_2]$. Since $S^* = \cup_i S_i$ and $\Gamma' = \cup_i \Gamma_i$, there must be some n such that $S_n; \Gamma_n \xrightarrow{k_m,u_1,u_2} s \circ [t_1, t_2]$, which contradicts condition (3) for that n. So $(S^*, \Gamma^*, K^*, [u_1, u_2])$ is $(s \circ [t_1, t_2])$-consistent.

It remains only to check that $(S^*, \Gamma^*, K^*, [u_1, u_2])$ is prime. To do that we check the conditions in the definition of a prime theory.

- (Prin-closure) By definition, $K^* = \{k \mid S^*, \Gamma' \rhd k \succeq k_m\}$. Hence $(S^*, \Gamma') \curlyvee K^*$, i.e. $(S^*, \Gamma^*) \curlyvee K^*$ by (C-constr).

- (Fact-closure) Suppose $k \in K^*$, $S^*; \Gamma^* \xrightarrow{k,u_1',u_2'} s' \circ [u_b, u_e]$ and $[\mathsf{ev}(u_1), \mathsf{ev}(u_2)] \subseteq [u_1', u_2']$. We need to show that $s' \circ [u_b, u_e] \in \Gamma^*$. Since $S^*; \Gamma^* \xrightarrow{k,u_1',u_2'} s' \circ [u_b, u_e]$, there are finite subsets $S^f \subseteq S^*$ and $\Gamma^f \subseteq \Gamma^*$ such that $S^f; \Gamma^f \xrightarrow{k,u_1',u_2'} s' \circ [u_b, u_e]$. By (C-ground-time), $S^f; \Gamma^f \rhd u_1' \leq u_1$ and $S^f; \Gamma^f \rhd u_2 \leq u_2'$. So by the view subsumption principle, $S^f; \Gamma^f \xrightarrow{k_m,u_1,u_2} s' \circ [u_b, u_e]$. Since each $s^* \circ [u_b, u_e]$ in Γ^f satisfies $S^*; \Gamma' \xrightarrow{k_m,u_1,u_2} s^* \circ [u_b, u_e]$, it follows by $|\Gamma^f|$ applications of the cut principle that $S^*; \Gamma' \xrightarrow{k_m,u_1,u_2} s' \circ [u_b, u_e]$. By definition of Γ^*, $s' \circ [u_b, u_e] \in \Gamma^*$.

- (Primality1) Suppose $s_1 \vee s_2 \circ [u_b, u_e] \in \Gamma^*$. Therefore, $S^*; \Gamma' \xrightarrow{k_m,u_1,u_2} s_1 \vee s_2 \circ [u_b, u_e]$. Hence, there is some n such that $S_n; \Gamma_n \xrightarrow{k_m,u_1,u_2} s_1 \vee s_2 \circ [u_b, u_e]$. If $s_1 \vee s_2 \circ [u_b, u_e] \in \mathit{treated}_n^{\vee}$, then by construction either $s_1 \circ [u_b, u_e]$ or $s_2 \circ [u_b, u_e]$ must be in Γ_n (whenever we add $s_1 \vee s_2 \circ [u_b, u_e]$ to $\mathit{treated}_i^{\vee}$, we also add either $s_1 \circ [u_b, u_e]$ or $s_2 \circ [u_b, u_e]$ to Γ_i). Hence, either $s_1 \circ [u_b, u_e]$ or $s_2 \circ [u_b, u_e]$ must be in Γ^*, which is a superset of each Γ_n. If $s_1 \vee s_2 \circ [u_b, u_e] \notin \mathit{treated}_n^{\vee}$, let $s_1 \vee s_2 \circ [u_b, u_e]$ have index k in the enumeration E. Then, in at most $2k$ further steps we would consider $s_1 \vee s_2 \circ [u_b, u_e]$ as a candidate and add either $s_1 \circ [u_b, u_e]$ or $s_2 \circ [u_b, u_e]$ to Γ'.

- (Primality2) Suppose $\exists x{:}\sigma.s' \circ [u_b, u_e] \in \Gamma^*$. Therefore, $S^*; \Gamma' \xrightarrow{k_m,u_1,u_2} \exists x{:}\sigma.s' \circ [u_b, u_e]$. Hence, there is some n such that $S_n; \Gamma_n \xrightarrow{k_m,u_1,u_2} \exists x{:}\sigma.s' \circ [u_b, u_e]$. If $\exists x{:}\sigma.s' \circ [u_b, u_e] \in \mathit{treated}_n^{\exists}$, then by construction there must be a constant a such that $a{:}\sigma \in S_n$ and

$s' \circ [u_b, u_e][a/x] \in \Gamma_n$ (whenever we add $\exists x{:}\sigma.s' \circ [u_b, u_e]$ to $\mathit{treated}_i^{\exists}$, we also add a fresh $a{:}\sigma$ to S_i and $s' \circ [u_b, u_e][a/x]$ to Γ_i). This immediately implies the primality condition because $\Gamma^* \supseteq \Gamma_n$. If $\exists x{:}\sigma.s' \circ [u_b, u_e] \notin \mathit{treated}_n^{\exists}$, let $\exists x{:}\sigma.s' \circ [u_b, u_e]$ have index k in the enumeration E. Then, in at most $2k$ further steps we would consider $\exists x{:}\sigma.s' \circ [u_b, u_e]$ as a candidate and add $a{:}\sigma$ to S and $s' \circ [u_b, u_e][a/x]$ to Γ'.

- (Primality3) Suppose for the sake of contradiction that $\bot \circ [u_b, u_e] \in \Gamma^*$. Then, $S^*; \Gamma^* \xrightarrow{k_m, u_1, u_2} s \circ [t_1, t_2]$, which contradicts the previously derived fact that $(S^*, \Gamma^*, K^*, [u_1, u_2])$ is $(s \circ [t_1, t_2])$-consistent. Hence $\bot \circ [u_b, u_e] \notin \Gamma^*$.

- (Primality4) Suppose c is a constraint such that $c \circ [u_b, u_e] \in \Gamma^*$. Then by the definition of Γ^*, $c \in \Gamma^*$, so $S^*; \Gamma^* \rhd c$ by (c-hyp).

□

Lemma 3.14 (Satisfaction)**.** *For any judgement of the form $s \circ [t_1, t_2]$ and any prime theory $(S, \Gamma, K, [u_1, u_2])$, it is the case that $(S, \Gamma, K, [u_1, u_2]) \models s \circ [t_1, t_2]$ in the canonical model if and only if $s \circ [t_1, t_2] \in \Gamma$.*

Proof. By induction on s and case analysis of its top-level constructor. Most cases can be treated similarly as in the proof of the corresponding lemma for BL, Lemma 2.13. We show two cases, the first of which does not exist in the proof of Lemma 2.13, and the second of which needs some non-trivial modification.

Case. $s = s'@[u_b, u_e]$.

Suppose $s'@[u_b, u_e] \circ [t_1, t_2] \in \Gamma$. We need to prove that $(S, \Gamma, K, [u_1, u_2]) \models s'@[u_b, u_e] \circ [t_1, t_2]$. $S; \Gamma \xrightarrow{k, u_1, u_2} s' \circ [u_b, u_e]$ for any $k \in K$. So by (Fact-closure) $s' \circ [u_b, u_e] \in \Gamma$. So by i.h., $(S, \Gamma, K, [u_1, u_2]) \models s' \circ [u_b, u_e]$, i.e. $(S, \Gamma, K, [u_1, u_2]) \models s'@[u_b, u_e] \circ [t_1, t_2]$ by the definition of $\models$, as required.

Conversely suppose $(S, \Gamma, K, [u_1, u_2]) \models s'@[u_b, u_e] \circ [t_1, t_2]$. We need to prove that $s'@[u_b, u_e] \circ [t_1, t_2] \in \Gamma$. By the definition of $\models$, $(S, \Gamma, K, [u_1, u_2]) \models s' \circ [u_b, u_e]$. By i.h., $s' \circ [u_b, u_e] \in \Gamma$. Now $S; \Gamma \xrightarrow{k, u_1, u_2} s'@[u_b, u_e] \circ [t_1, t_2]$ for any $k \in K$. So by (Fact-closure) $s'@[u_b, u_e] \circ [t_1, t_2] \in \Gamma$, as required.

Case. $s = k \ \mathsf{says}\ s'$.

Suppose $k \ \mathsf{says}\ s' \circ [t_1, t_2] \in \Gamma$. We want to show that $(S, \Gamma, K, [u_1, u_2]) \models k \ \mathsf{says}\ s' \circ [t_1, t_2]$. Following the definition of $\models$, pick any $[u_1'', u_2''] \subseteq [t_1, t_2]$, $(S_1, \Gamma_1, K_1, [u_1', u_2'])$ and $(S_2, \Gamma_2, K_2, [u_1'', u_2''])$ such that $(S, \Gamma, K, [u_1, u_2]) \leq_i (S_1, \Gamma_1, K_1, [u_1', u_2']) \leq_s (S_2, \Gamma_2, K_2, [u_1'', u_2''])$ and $k \in \theta(S_2, \Gamma_2, K_2, [u_1'', u_2]'') = K_2$. It suffices to prove that $(S_2, \Gamma_2, K_2, [u_1'', u_2'']) \models s' \circ [t_1, t_2]$. Since $\Gamma \subseteq \Gamma_1$, $k \ \mathsf{says}\ s' \circ [t_1, t_2] \in \Gamma_1$. By definition of $\leq_s$ in the canonical model, we obtain $s' \circ [t_1, t_2] \in \Gamma_2$. By i.h., $(S_2, \Gamma_2, K_2, [u_1'', u_2'']) \models s' \circ [t_1, t_2]$, as required.

Conversely, suppose that $(S, \Gamma, K, [u_1, u_2]) \models k \ \mathsf{says}\ s' \circ [t_1, t_2]$. We want to show that $k \ \mathsf{says}\ s' \circ [t_1, t_2] \in \Gamma$. Assume for the sake of contradiction that $k \ \mathsf{says}\ s' \circ [t_1, t_2] \notin \Gamma$. Pick any $k' \in K$. By (Fact-closure), $S; \Gamma \not\xrightarrow{k', u_1, u_2} k \ \mathsf{says}\ s' \circ [t_1, t_2]$. So by properties of the sequent calculus, $S;\Gamma| \not\xrightarrow{k,t_1,t_2} s' \circ [t_1,t_2]$.[3] Define $K_0 = \{k' \mid S;\Gamma \rhd k' \succeq k\}$. Then $(S,\Gamma|,K_0,[t_1,t_2])$ is $(s' \circ [t_1,t_2])$-consistent. By Lemma 3.13, there is an $(s' \circ [t_1,t_2])$-consistent prime theory $(S^*,\Gamma^*,K^*,[t_1,t_2])$ such that $S \subseteq S^*$, $\Gamma| \subseteq \Gamma^*$, $K_0 \subseteq K^*$. Because k says $s' \circ [t_1,t_2] \in \Gamma$, k says $s' \circ [t_1,t_2] \in \Gamma|$. Hence, k says $s' \circ [t_1,t_2] \in \Gamma^*$. Therefore, $S^*;\Gamma^* \xrightarrow{k,t_1,t_2} s' \circ [t_1,t_2]$. By (Fact-closure) and the fact that $k \in K_0 \subseteq K^*$, $s' \circ [t_1,t_2] \in \Gamma^*$, which contradicts the $(s' \circ [t_1,t_2])$-consistency of $(S^*,\Gamma^*,K^*,[t_1,t_2])$. Hence, we must have k says $s' \circ [t_1,t_2] \in \Gamma$. □

Lemma 3.15 (Completeness for closed formulas). *Let $\mathcal{C}$ be the canonical Kripke model. If $\mathcal{C} \models (\cdot;\cdot \xrightarrow{\ell,t_1,t_2} s \circ [u_1,u_2])$, then $\cdot;\cdot \xrightarrow{\ell,t_1,t_2} s \circ [u_1,u_2]$.*

Proof. Suppose for the sake of contradiction that $\mathcal{C} \models (\cdot;\cdot \xrightarrow{\ell,t_1,t_2} s \circ [u_1,u_2])$, but $\cdot;\cdot \not\xrightarrow{\ell,t_1,t_2} s \circ [u_1,u_2]$. Define $K = \{k \mid \cdot;\cdot \rhd k \succeq \ell\}$. Observe that because $\cdot;\cdot \not\xrightarrow{\ell,t_1,t_2} s \circ [u_1,u_2]$, the theory $(\cdot,\cdot,K,[t_1,t_2])$ is $(s \circ [u_1,u_2])$-consistent. Hence, by Lemma 3.13, there is a prime theory $(S^*,\Gamma^*,K^*,[t_1,t_2])$ that is $(s \circ [u_1,u_2])$-consistent. It follows from $(s \circ [u_1,u_2])$-consistency of $(S^*,\Gamma^*,K^*,[t_1,t_2])$ that $s \circ [u_1,u_2] \notin \Gamma^*$. Hence, from Lemma 3.14, $(S^*,\Gamma^*,K^*,[t_1,t_2]) \not\models s \circ [u_1,u_2]$. This contradicts the assumption $\mathcal{C} \models (\cdot;\cdot \xrightarrow{\ell,t_1,t_2} s \circ [u_1,u_2])$. □

Definition 3.16. For a judgment J we define $\bar{J}$ by

$$\bar{J} := \begin{cases} s@[u_1,u_2] & \text{if } J = s \circ [u_1,u_2] \\ (k \ \mathsf{says}\ s)@[u_1,u_2] & \text{if } J = k \ \mathsf{claims}\ s \circ [u_1,u_2] \end{cases}$$

Theorem 3.17 (Completeness). *Let $\mathcal{C}$ be the canonical Kripke model. If $\mathcal{C} \models (\Sigma;\Gamma \xrightarrow{k,t_1,t_2} s \circ [u_1,u_2])$, then $\Sigma;\Gamma \xrightarrow{k,t_1,t_2} s \circ [u_1,u_2]$.*

Proof. Suppose $\mathcal{C} \models (\Sigma;\Gamma \xrightarrow{k,t_1,t_2} s \circ [u_1,u_2])$. We first argue that $\mathcal{C} \models (\cdot;\cdot \xrightarrow{\ell,u_b,u_e} \forall\Sigma.\ k$ says $(\bigwedge\bar{\Gamma} \supset (s@[u_1,u_2])) \circ [t_1,t_2])$. To prove this we follow the definition of $\models$. This proof does not use any property specific to canonical models, and will work for any Kripke model $\mathcal{C}$. We pick any world w_1 in the model. It suffices to prove that $w_1 \models \forall\Sigma.\ k$ says $(\bigwedge\bar{\Gamma} \supset (s@[u_1,u_2])) \circ [t_1,t_2]$. Pick any w_2 such that $w_1 \leq_i w_2$ and any substitution μ such that $\Sigma \ll \mu : (\mathcal{C},w_2)$. It suffices to show that $w_2 \models k\mu$ says $(\bigwedge\bar{\Gamma}\mu \supset (s\mu@[u_1\mu,u_2\mu])) \circ [t_1\mu,t_2\mu]$. Pick worlds w_3,w_4 such that $w_2 \leq_i w_3 \leq_s w_4$, $k\mu \in \theta(w_4)$ and w_4 is a $[t'_1,t'_2]$-world for some $[t'_1,t'_2] \subseteq [\mathsf{ev}(t_1\mu),\mathsf{ev}(t_2\mu)]$. It suffices to prove that $w_4 \models \bigwedge\bar{\Gamma}\mu \supset (s\mu@[u_1\mu,u_2\mu]) \circ [t_1\mu,t_2\mu]$. Pick w_5 with $w_4 \leq_i w_5$ such that $w_5 \models \Gamma\mu$. It suffices to prove that $w_5 \models s\mu \circ [u_1\mu,u_2\mu]$.

Applying the definition of $\models$ on sequents to the assumption $\mathcal{C} \models (\Sigma;\Gamma \xrightarrow{k,t_1,t_2} s \circ [u_1,u_2])$, we obtain $w_5 \models s\mu \circ [u_1\mu,u_2\mu]$ under the assumptions that $\Sigma \ll \mu : (\mathcal{C},w_5)$, that $k\mu \in \theta(w_5)$, that $w_5 \models \Gamma\mu$ and that w_5 is a $[u'_1,u'_2]$-world for some $[u'_1,u'_2] \subseteq [\mathsf{ev}(t_1\mu),\mathsf{ev}(t_2\mu)]$. So it is enough to check these four assumptions. $\Sigma \ll \mu : (\mathcal{C},w_5)$ follows from the assumption $\Sigma \ll \mu : (\mathcal{C},w_2)$ and the fact that $D(w_2) \subseteq D(w_5)$ (because $w_2 \leq_i w_3 \leq_s w_4 \leq_i w_5$).

[3] $\Gamma|$ is defined here as $\{(k_1 \ \mathsf{says}\ s_1 \circ [u_b,u_e]) \mid (k_1 \ \mathsf{says}\ s_1 \circ [u_b,u_e]) \in \Gamma\}$.

$k\mu \in \theta(w_5)$ follows from (K-viewmon) because $k\mu \in \theta(w_4)$ and $w_4 \leq_i w_5$. $w_5 \models \Gamma\mu$ holds by assumption. Finally, w_5 is a $[t'_1, t'_2]$-world (since w_4 is a $[t'_1, t'_2]$-world and $w_4 \leq_i w_5$) and $[t'_1, t'_2] \subseteq [\mathsf{ev}(t_1\mu), \mathsf{ev}(t_2\mu)]$.

Hence, $\mathcal{C} \models (\cdot; \cdot \xrightarrow{\ell, u_b, u_e} \forall\Sigma.\ k \textsf{ says } (\bigwedge \bar{\Gamma} \supset (s@[u_1, u_2])) \circ [t_1, t_2])$. By Lemma 3.15, $\cdot; \cdot \xrightarrow{\ell, u_b, u_e} \forall\Sigma.\ k \textsf{ says } (\bigwedge \bar{\Gamma} \supset (s@[u_1, u_2])) \circ [t_1, t_2]$. Using properties of the sequent calculus, this implies that $\Sigma; \Gamma \xrightarrow{k, t_1, t_2} s \circ [u_1, u_2]$, as required. □

Theorem 3.18 (Soundness and completeness)**.** $\Sigma; \Gamma \xrightarrow{k, t_1, t_2} s@[u_1, u_2]$ *if and only if* $\mathcal{K} \models (\Sigma; \Gamma \xrightarrow{k, t_1, t_2} s@[u_1, u_2])$ *for every Kripke model* $\mathcal{K}$.

Proof. Immediate from Theorems 3.6 and 3.17. □

References

[1] Martín Abadi. Logic in Access Control. In *Proceedings of the 18th Annual Symposium on Logic in Computer Science (LICS'03)*, pages 228–233, June 2003.

[2] Natasha Alechina, Michael Mendler, Valeria de Paiva, and Eike Ritter. Categorical and Kripke Semantics for Constructive S4 Modal Logic. In *CSL '01: Proceedings of the 15th International Workshop on Computer Science Logic*, pages 292–307, London, UK, 2001. Springer-Verlag.

[3] Rohit Chadha, Damiano Macedonio, and Vladimiro Sassone. A Hybrid Intuitionistic Logic: semantics and Decidability. *Journal of Logic and Computation*, 16(1):27–59, 2005.

[4] Bor-Yuh Evan Chang, Kaustuv Chaudhuri, and Frank Pfenning. A Judgmental Analysis of Linear Logic. Technical Report CMU-CS-03-131R, Carnegie Mellon University, 2003.

[5] E. A. Emerson. Temporal and Modal Logic. In *Handbook of Theoretical Computer Science*. The MIT Press, 1990.

[6] Deepak Garg. *Proof Theory for Authorization Logic and Its Application to a Practical File System*. PhD thesis, Carnegie Mellon University, 2010.

[7] Deepak Garg and Frank Pfenning. *Stateful Authorization Logic:*, pages 210–225. Springer Berlin Heidelberg, Berlin, Heidelberg, 2011.

[8] Frank Pfenning. Structural Cut Elimination I. Intuitionistic and Classical Logic. *Information and Computation*, 157(1/2):84–141, March 2000.

[9] Frank Pfenning and Rowan Davies. A Judgmental Reconstruction of Modal Logic. *Mathematical Structures in Computer Science*, 11:511–540, 2001.