

From Indexed Lax Logic to Intuitionistic Logic

Deepak Garg¹ Michael Carl Tschantz²

January, 2008
CMU-CS-07-167

School of Computer Science
Carnegie Mellon University
Pittsburgh, PA 15213

Abstract

We present translations from a logic with indexed lax modalities to first-order intuitionistic logic and intuitionistic linear logic. These translations rely on a continuation passing style encoding for the lax modalities. We show that our translations preserve provability of formulas.

¹This author was partially sponsored by the Air Force Research Laboratory under grant no. FA87500720028. The views and conclusions contained in this document are those of the author and should not be interpreted as representing official policies, either expressed or implied, of any sponsoring institution, the U.S. government or any other entity.

²This author was partially sponsored by the Army Research Office through grant number DAAD19-02-1-0389 (“Perpetually Available and Secure Information Systems”) to Carnegie Mellon University’s CyLab and by a generous gift from the Hewlett-Packard Corporation. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of any sponsoring institution, the U.S. government, or any other entity.

Keywords: Lax Logic, Affirmations, Logical Transformations

1 Introduction

Lax logic is a modal logic extending intuitionistic propositional logic with a single modality lax ($\circ A$) satisfying the following axioms.

$$\begin{aligned} &\vdash A \supset \circ A \\ &\vdash \circ \circ A \supset \circ A \\ &\vdash \circ(A \supset B) \supset (\circ A \supset \circ B) \end{aligned}$$

In this report we describe two simple translations of lax logic with multiple modalities: a *first-order translation* into first-order intuitionistic logic and a *linear translation* into intuitionistic linear logic. We show that our translations preserve provability. The essence of these translations is a continuation passing style (CPS) encoding of the lax modality.

Background. In its propositional form, lax logic was introduced by Mendler *et al* [FM97] as a means of modeling digital circuits. Subsequently, a first-order version was developed for use in constraint logic programming [FW97, FMW97]. The semantics and proof theory of lax logic are well studied [PD01, FM97, How01, BBdP98, GP06, AMdPR01] and the propositional fragment is decidable [FM97, How01]. Lax logic corresponds (under the Curry-Howard isomorphism) to monads from functional programming [BBdP98].

Our primary interest in lax logic is its application to representing decentralized access-control systems where different users, machines, programs, etc (abstractly called *principals*) request access to secure resources like files or devices under the control of other principals such as administrators or the operating system. The policies governing access to resources are formalized as logical formulas in a suitably chosen logic. Access is granted to a resource if a particular proposition such as `can_read(Bob, foo.pdf)` is provable in the logic from the given policy.

A quintessential requirement on a logic of access control is a notion of statements *made by* a principal [ABLP93, LABW92]. For instance, we may want to formalize the following statements in the access control policy of a file system:

- Administrator says Bob can read foo.pdf
- Administrator says that any user X can read foo.pdf if X is a member of the group of privileged users

One convenient way of formalizing such statements is to introduce for each principal K , a modality $\langle K \rangle A$ (read “ K says A ”) with the intended meaning that K says that A is true. Then the above statements can be encoded as follows.

- $\langle \text{administrator} \rangle \text{can_read}(\text{Bob}, \text{foo.pdf})$
- $\langle \text{administrator} \rangle (\forall X. \text{privileged}(X) \supset \text{can_read}(X, \text{foo.pdf}))$.

Here `privileged(X)` is a predicate indicating that X is a privileged user and `can_read(Bob, foo.pdf)` means that Bob is allowed to read foo.pdf.

There is reasonable flexibility in choosing the logical rules governing the modality $\langle K \rangle A$ and a number of proposals have been made [LABW92, ABLP93, Aba03, GP06, Aba06]. For instance the \square operator from modal logic K can be used. However, more recently, an increasingly large number

of proposals [GP06, Aba06, CCD⁺07, GBB⁺06, LLFS⁺07, GA08] have chosen $\langle K \rangle A$ to be a lax modality, with the rules described earlier:

$$\begin{aligned} &\vdash A \supset \langle K \rangle A \\ &\vdash \langle K \rangle \langle K \rangle A \supset \langle K \rangle A \\ &\vdash \langle K \rangle (A \supset B) \supset (\langle K \rangle A \supset \langle K \rangle B) \end{aligned}$$

With these rules, the access control logic becomes an indexed lax logic, with one lax modality for every principal. We briefly mention the merits of making $\langle K \rangle A$ a lax modality, referring the interested reader to existing work for more details on modeling access control systems in the logic [LABW92, ABLP93, GP06].

- Owing to a well studied proof theory, the notion of proof is well understood for lax logic. This is crucial in access control systems that often rely on the existence of proof of a certain proposition (like `can_read(Bob, foo.pdf)`) in order to grant access to resources. This is particularly the case with proof-carrying authorization architectures [AF99, Bau03].
- The axiom $A \supset \langle K \rangle A$ forces every principal to state every true statement A . This indicates that proof is irrefutable evidence, i.e., if A has a proof, then every principal will believe it. This is not the case in a number of modal logics, such as K.
- It is not the case that $(\langle K \rangle \perp) \supset \perp$. Thus, individual principals may make inconsistent statements without making the logic inconsistent. This is important since principals may be malicious.

In this report, we present a translation from an access control logic with lax modalities (called INLL for *INDEXED Lax Logic* here) to two different logics: first-order intuitionistic logic and intuitionistic propositional linear logic. We show in each case that the translations preserve provability of formulas. In particular, we prove two complementary theorems in each case: *soundness*, which states that a translated formula is provable only if the original formula is, and *completeness* which states the converse.

The main motivation for studying these translations is automation of the proof search procedure for INLL, which is central to implementations of access control systems using the logic. Rather than prove a formula in INLL (for which theorem provers are not known), one could simply translate it to (say) first-order logic and use a standard theorem prover. Besides automation, our results are interesting from a theoretical perspective. To the best of our knowledge, these are the first sound and complete translations from lax logic to logics without any modalities (with the exception of translations based on explicit encodings of Kripke interpretations at first-order).

Related Work. Our translations rely on encoding the lax modalities in a continuation passing style (CPS). Our translations extend a *complete but unsound* translation from lax logic to propositional logic proposed by Mendler *et al* [FM97], which maps $\bigcirc A$ to $(\ulcorner A \urcorner \supset C) \supset C$, where C is a fixed formula. Special cases of our translations suggest that soundness can be recovered in two different ways. The first is to add a universally quantified parameter, mapping $\bigcirc A$ to $\forall x. (\ulcorner A \urcorner \supset C(x)) \supset C(x)$. The other possibility is to allow linearity and translate $\bigcirc A$ to $(\ulcorner A \urcorner \supset C) \multimap C$.

It is well known in functional programming that all monads (the Curry-Howard equivalents of the lax modality) can be encoded using similar CPS transformations [Fil89, Fil94]. These

translations preserve *equality* of proofs under $\beta\eta$ -reduction. We show that CPS translations of lax modalities also preserve the *existence* of proofs. This expands earlier results from the level of proof terms to the level of provability. The correctness of our linear translation critically uses the fact that continuations arising from the translation have to be used exactly once. This is well understood in functional programming [DDP99, BORT02, Ber04].

There is rather limited work on translating logics for access control into simpler logics. We are aware of only one substantial effort in this direction [GA08]. However, this work is targeted at modal S4 rather than intuitionistic logic. Other previous work on translating lax logic has targeted intuitionistic S4 [PD01].

Organization of the Report. Section 2 describes the syntax and proof-system of the access control logic INLL. Section 3 describes the translation from INLL to first-order logic. In section 4 we modify this translation to obtain the linear translation. Section 5 concludes the report with directions for future work.

2 INLL: Indexed Lax Logic

In this section we describe indexed lax logic INLL, which is the source of our translations. INLL extends intuitionistic propositional logic with a number of lax modalities, indexed by elements of a countable domain of principals. We use A, B to denote arbitrary formulas and P to denote atomic formulas. The letter K ranges over principals.

$$A, B ::= P \mid A \supset B \mid A \wedge B \mid A \vee B \mid \perp \mid \top \mid \langle K \rangle A$$

The axioms governing the lax modalities $\langle K \rangle A$ have been described in section 1. Both natural deduction and sequent calculus presentations of the proof theory are known for this logic [PD01, FM97, How01, BBdP98]. In the following we describe a cut free sequent calculus from an earlier work by one of the authors [GP06] to an extent necessitated by further discussion. Details of the proof theory may be found in earlier papers.

The sequent calculus for INLL is presented in judgmental style, where the subjects of knowledge are statements about propositions called *categorical* judgments. We use two categorical judgments: A *true*, meaning that proposition A is true, and K *affirms* A meaning that principal K states that A is true. Based on these categorical judgments, we construct *hypothetical* judgments which are the subjects of proofs. Hypothetical judgments take one of the following two forms:

$$\begin{aligned} & A_1 \text{ true}, \dots, A_n \text{ true} \Rightarrow B \text{ true} \\ & A_1 \text{ true}, \dots, A_n \text{ true} \Rightarrow K \text{ affirms } B \end{aligned}$$

The judgments $A_1 \text{ true}, \dots, A_n \text{ true}$ are called hypotheses or assumptions, and the intended meaning is that if these judgments hold, then the judgment to the right of \Rightarrow ($B \text{ true}$ or $K \text{ affirms } B$) holds. We use the symbol Γ to denote a set of hypothesis, and γ to denote the judgment on the right of \Rightarrow when its exact form does not matter. We elide the judgment name *true* from $A \text{ true}$.

Connectives are described in the sequent calculus using left and right rules. As an example, the rules for implication \supset are:

$$\frac{\Gamma, A \Rightarrow B}{\Gamma \Rightarrow A \supset B} \supset R \qquad \frac{\Gamma, A \supset B \Rightarrow A \quad \Gamma, A \supset B, B \Rightarrow \gamma}{\Gamma, A \supset B \Rightarrow \gamma} \supset L$$

Rules for the connectives $\wedge, \vee, \top, \perp$ are standard, and may be found in Appendix A. The rules for $\langle K \rangle A$ are:

$$\frac{\Gamma \Rightarrow K \text{ affirms } A}{\Gamma \Rightarrow \langle K \rangle A} \langle \rangle R \qquad \frac{\Gamma, \langle K \rangle A, A \Rightarrow K \text{ affirms } C}{\Gamma, \langle K \rangle A \Rightarrow K \text{ affirms } C} \langle \rangle L$$

The first rule states that in order to establish that $\langle K \rangle A$ is true, it is enough to establish that $K \text{ affirms } A$. The second rule states that if we assume that $\langle K \rangle A$ is true, then we are justified in assuming that A is true provided we are trying to prove a goal of the form $K \text{ affirms } C$. Note the accordance of principal K on the left and right of \Rightarrow in this rule. The final rule connects the two basic judgments:

$$\frac{\Gamma \Rightarrow A}{\Gamma \Rightarrow K \text{ affirms } A} \text{affirms}$$

This rule states that if A is true, then it is also the case that $K \text{ affirms } A$. Together these three rules capture the lax nature of the modality $\langle K \rangle A$. Appendix A summarizes the sequent calculus. It can be shown that this sequent calculus is equivalent to the three axioms described earlier, and that in the degenerate case where we consider only one principal, this logic reduces to lax logic. The following cut admissibility theorem was proved in [GP06].

Theorem 2.1 (Admissibility of Cut).

1. If $\Gamma \Rightarrow A$ and $\Gamma, A \Rightarrow \gamma$, then $\Gamma \Rightarrow \gamma$.
2. If $\Gamma \Rightarrow K \text{ affirms } A$ and $\Gamma, A \Rightarrow K \text{ affirms } B$, then $\Gamma \Rightarrow K \text{ affirms } B$.

3 Translation to First-Order Intuitionistic Logic

Now we present the translation from INLL to first-order intuitionistic logic (FOIL). The syntax and proof theory of intuitionistic first-order logic are standard. A cut free sequent calculus is summarized in appendix B. We write $\Sigma; \Gamma \Rightarrow A$ to mean that from assumptions Γ , A is provable in FOIL. The set Σ records all first-order constants occurring in Γ and A .

Our translation $(\ulcorner \cdot \urcorner)$ is described in Figure 1. It maps all intuitionistic connectives of INLL to themselves. The core of our work is the translation of $\langle K \rangle A$. We assume the existence of a binary predicate $\mathbf{af}(K, x)$, which does not occur in INLL formulas. Its first argument is a principal. The second is assumed to have an arbitrary fixed type. We often call the second argument a *nonce*. We define

$$\ulcorner \langle K \rangle A \urcorner = \forall x. (\ulcorner A \urcorner \supset \mathbf{af}(K, x)) \supset \mathbf{af}(K, x)$$

This resembles a CPS transformation of the lax modality. The formula $\ulcorner A \urcorner \supset \mathbf{af}(K, x)$ is the “type” of the continuation, and $\mathbf{af}(K, x)$ is type of the result. It is necessary to universally quantify over the nonce x in order to preserve provability. Figure 1 also shows the translation of hypotheses Γ and sequents. The non-trivial part is the translation of the sequent $\Gamma \Rightarrow K \text{ affirms } A$, which is defined as $\Sigma, a; \ulcorner \Gamma \urcorner, (\ulcorner A \urcorner \supset \mathbf{af}(K, a)) \Rightarrow \mathbf{af}(K, a)$ where a is a fresh constant.

We prove two complementary correctness theorems for the translation. *Completeness* states that whenever a formula is provable in INLL, its translation is provable in FOIL. The dual theorem, *soundness*, states the converse. Completeness is easy to establish. We only need to show that each

$$\begin{aligned}
\lceil P \rceil &= P \\
\lceil A_1 \wedge A_2 \rceil &= \lceil A_1 \rceil \wedge \lceil A_2 \rceil \\
\lceil A_1 \vee A_2 \rceil &= \lceil A_1 \rceil \vee \lceil A_2 \rceil \\
\lceil A_1 \supset A_2 \rceil &= \lceil A_1 \rceil \supset \lceil A_2 \rceil \\
\lceil \top \rceil &= \top \\
\lceil \perp \rceil &= \perp \\
\lceil \langle K \rangle A \rceil &= \forall x. (\lceil A \rceil \supset \mathbf{af}(K, x)) \supset \mathbf{af}(K, x) \\
\lceil \Gamma = \{A_1, \dots, A_n\} \rceil &= \{\lceil A_1 \rceil, \dots, \lceil A_n \rceil\} \\
\lceil \Gamma \Rightarrow A \rceil &= \Sigma; \lceil \Gamma \rceil \Rightarrow \lceil A \rceil \\
\lceil \Gamma \Rightarrow K \text{ affirms } A \rceil &= \Sigma, a; \lceil \Gamma \rceil, (\lceil A \rceil \supset \mathbf{af}(K, a)) \Rightarrow \mathbf{af}(K, a) \quad (a \text{ fresh}) \\
&\Sigma \text{ contains all constants mentioned in } \Gamma, A \text{ and } K.
\end{aligned}$$

Figure 1: First-Order Translation

inference rule in the sequent calculus for INLL can be simulated in FOIL after translation. The formal proof is a straightforward induction on a given INLL proof.

Theorem 3.1 (Completeness). *Suppose Σ contains all first-order constants mentioned in Γ , A and K .*

1. *If $\Gamma \Rightarrow A$ in INLL, then $\Sigma; \lceil \Gamma \rceil \Rightarrow \lceil A \rceil$ in FOIL.*
2. *If $\Gamma \Rightarrow K$ affirms A in INLL, then $\Sigma, a; \lceil \Gamma \rceil, (\lceil A \rceil \supset \mathbf{af}(K, a)) \Rightarrow \mathbf{af}(K, a)$ in FOIL for every fresh constant a .*

Proof. See Appendix D. □

Soundness states that if $\lceil \Gamma \rceil \Rightarrow \lceil A \rceil$ in FOIL, then $\Gamma \Rightarrow A$ in INLL. Establishing this theorem is non-trivial. Our approach is to identify a syntactic class of FOIL sequents which can occur in proofs of translated INLL sequents. Then we define an inverse translation ($\lfloor \cdot \rfloor$) from this class of sequents to INLL, such that $\lfloor \lceil \cdot \rceil \rfloor$ is the identity. Finally we induct on proofs of sequents in this class to show that their inverse translation is provable in INLL. The formal soundness theorem is shown below.

Theorem 3.2 (Soundness). *Suppose Σ contains all first-order constants mentioned in Γ , A and K .*

1. *If $\Sigma; \lceil \Gamma \rceil \Rightarrow \lceil A \rceil$ in FOIL, then $\Gamma \Rightarrow A$ in INLL.*
2. *If $\Sigma, a; \lceil \Gamma \rceil, (\lceil A \rceil \supset \mathbf{af}(K, a)) \Rightarrow \mathbf{af}(K, a)$ and $a \notin \Sigma$, then $\Gamma \Rightarrow K$ affirms A .*

Proof. See Appendix E. □

Importance of Nonces. The universally quantified nonce x in the translated formula $\forall x. (\lceil A \rceil \supset \mathbf{af}(K, x)) \supset \mathbf{af}(K, x)$ is essential for the proof of soundness. A translation without the nonce is

unsound. We show this by means of a counterexample. Suppose that we omit the nonce, so that \mathbf{af} is a unary predicate expecting only one principal as argument and define

$$\ulcorner \langle K \rangle A \urcorner = (\ulcorner A \urcorner \supset \mathbf{af}(K)) \supset \mathbf{af}(K)$$

Consider the INLL formula $((A \supset \langle K \rangle B) \supset A) \supset \langle K \rangle A$. It is quite easy to verify that this formula is not provable in general in INLL. However its translation is provable in FOIL for any A , B and K , as the following derivation shows.

$$\frac{\frac{\frac{\ulcorner A \urcorner \Rightarrow \ulcorner A \urcorner \text{ init}}{\ulcorner A \urcorner \supset \mathbf{af}(K)} \supset L^* \quad \frac{\ulcorner \mathbf{af}(K) \Rightarrow \mathbf{af}(K) \urcorner \text{ init}}{\ulcorner A \urcorner, \ulcorner B \urcorner \supset \mathbf{af}(K) \Rightarrow \mathbf{af}(K)} \supset R^+}{\ulcorner A \urcorner \supset \mathbf{af}(K), \ulcorner A \urcorner \Rightarrow \ulcorner \langle K \rangle B \urcorner} \supset R}{\ulcorner A \urcorner \supset \mathbf{af}(K) \Rightarrow \ulcorner A \supset \langle K \rangle B \urcorner} \supset R \quad \frac{\ulcorner A \urcorner \Rightarrow \ulcorner A \urcorner \text{ init}}{\ulcorner \mathbf{af}(K) \Rightarrow \mathbf{af}(K) \urcorner} \supset L}{\ulcorner ((A \supset \langle K \rangle B) \supset A) \urcorner, \ulcorner A \urcorner \supset \mathbf{af}(K) \Rightarrow \ulcorner A \urcorner} \supset L^*}{\ulcorner ((A \supset \langle K \rangle B) \supset A) \urcorner, \ulcorner \mathbf{af}(K) \Rightarrow \mathbf{af}(K) \urcorner} \supset L^*} \supset R$$

$$\frac{\ulcorner ((A \supset \langle K \rangle B) \supset A) \urcorner, \ulcorner \mathbf{af}(K) \Rightarrow \mathbf{af}(K) \urcorner}{\ulcorner ((A \supset \langle K \rangle B) \supset A) \urcorner \Rightarrow \ulcorner \langle K \rangle A \urcorner} \supset R}{\ulcorner ((A \supset \langle K \rangle B) \supset A) \urcorner \Rightarrow \ulcorner \langle K \rangle A \urcorner} \supset R} \supset R$$

In each application of the $\supset L$ rule, we have put the principal formula in a box. This proof uses the continuation $\ulcorner A \urcorner \supset \mathbf{af}(K)$ twice: once in the rule marked $*$ and then in the rule marked $**$. If we used a universally quantified nonce in the predicate $\mathbf{af}(K, x)$, this proof would be invalid because the goal $\mathbf{af}(K)$ generated from $\ulcorner \langle K \rangle B \urcorner$ (rule marked $+$) would contain a fresh nonce that would not match the nonce in the continuation.

4 Translation to Intuitionistic Linear Logic

The counterexample at the end of section 3 demonstrates that the nonce x is essential in the first-order translation. We now describe an alternate possibility. Instead of adding the nonce, we could make the continuation $\ulcorner A \urcorner \supset \mathbf{af}(K)$ linear forcing it to be used *exactly once* in the proof. The rule marked $*$ would consume the continuation, making it unavailable in the rule marked $**$. This would invalidate the proof and eliminate the need for a first-order quantifier. Formally, we translate INLL to propositional intuitionistic linear logic (ILL) instead of first-order intuitionistic logic.

There are several presentations of intuitionistic linear logic [dPH93, CCP03, Wad93, Bar96]. We use a two-context presentation [CCP03, Bar96]. Appendix C summarizes the syntax and semantics of ILL. The judgment $\Gamma; \Delta \Rightarrow A$ means that under the linear assumptions Δ and unrestricted assumptions Γ , A can be established. The assumptions in Δ must each be used exactly once. Those in Γ may be used zero or more times. We use the symbol \multimap for linear implication, and \supset for non-linear implication. One may think of $A \supset B$ as being $(!A) \multimap B$. The other connectives we need are $\&$ (additive conjunction), \oplus (additive disjunction), \top and $\mathbf{0}$.

Our linear translation $(\ulcorner \cdot \urcorner^\top)$ is described in Figure 2. For intuitionistic connectives, our translation mirrors Girard's translation from intuitionistic logic to linear logic [Gir87]. For translating $\langle K \rangle B$, we assume a *unary* predicate $\mathbf{af}(K)$ whose argument is a principal and define

$$\ulcorner \langle K \rangle B \urcorner^\top = (\ulcorner B \urcorner^\top \supset \mathbf{af}(K)) \multimap \mathbf{af}(K)$$

$$\begin{aligned}
\ulcorner P \urcorner &= P \\
\ulcorner B_1 \wedge B_2 \urcorner &= \ulcorner B_1 \urcorner \& \ulcorner B_2 \urcorner \\
\ulcorner B_1 \vee B_2 \urcorner &= !(\ulcorner B_1 \urcorner) \oplus !(\ulcorner B_2 \urcorner) \\
\ulcorner B_1 \supset B_2 \urcorner &= \ulcorner B_1 \urcorner \supset \ulcorner B_2 \urcorner \\
\ulcorner \top \urcorner &= \top \\
\ulcorner \perp \urcorner &= \mathbf{0} \\
\ulcorner \langle K \rangle B \urcorner &= (\ulcorner B \urcorner \supset \mathbf{af}(K)) \multimap \mathbf{af}(K) \\
\ulcorner \Gamma = \{A_1, \dots, A_n\} \urcorner &= \{\ulcorner A_1 \urcorner, \dots, \ulcorner A_n \urcorner\} \\
\ulcorner \Gamma \Rightarrow A \urcorner &= \ulcorner \Gamma \urcorner; \cdot \Rightarrow \ulcorner A \urcorner \\
\ulcorner \Gamma \Rightarrow K \text{ affirms } A \urcorner &= \ulcorner \Gamma \urcorner; \ulcorner A \urcorner \supset \mathbf{af}(K) \Rightarrow \mathbf{af}(K)
\end{aligned}$$

Figure 2: Linear Translation

Observe the use of \multimap in the translation. For sequents, the interesting part is the translation of $\Gamma \Rightarrow K \text{ affirms } A$, where the continuation $(\ulcorner A \urcorner \supset \mathbf{af}(K))$ is a linear assumption. It is instructive to check that by making the translation linear in this manner, the counterexample at the end of section 3 no longer holds.

Correctness of the translation is established by proving soundness and completeness. It is straightforward to establish completeness by showing that each proof in INLL can be simulated in ILL.

Theorem 4.1 (Completeness).

1. If $\Gamma \Rightarrow A$ in INLL, then $\ulcorner \Gamma \urcorner; \cdot \Rightarrow \ulcorner A \urcorner$ in ILL.
2. If $\Gamma \Rightarrow K \text{ affirms } A$ in INLL, then $\ulcorner \Gamma \urcorner; \ulcorner A \urcorner \supset \mathbf{af}(K) \Rightarrow \mathbf{af}(K)$ in ILL.

Proof. See Appendix F. □

Soundness is harder, but can be established using methods similar to section 3.

Theorem 4.2 (Soundness).

1. If $\ulcorner \Gamma \urcorner; \cdot \Rightarrow \ulcorner A \urcorner$ in ILL, then $\Gamma \Rightarrow A$ in INLL
2. If $\ulcorner \Gamma \urcorner; \ulcorner A \urcorner \supset \mathbf{af}(K) \Rightarrow \mathbf{af}(K)$ in ILL, then $\Gamma \Rightarrow K \text{ affirms } A$ in INLL

Proof. See Appendix G. □

5 Conclusion

We have presented translations of propositional indexed lax logic to first-order intuitionistic logic and intuitionistic linear logic, and showed that they preserve provability. The essence of our translations is a CPS encoding of lax modalities. We conclude this report with a discussion of extensions

and future work.

First-order and linear extensions. INLL is a propositional logic. Our translations can be extended to extensions of INLL with first-order universal and existential quantifiers, including those over principals, by mapping these quantifiers to themselves. In the case of the linear translation this requires corresponding connectives in the target linear logic. For the first-order case, one must also assume that the type of nonces is fresh, i.e., nonces do not appear in INLL formulas.

It is also possible to translate a linear logic with indexed lax modalities to linear logic without any modalities. In this case, every linear connective is mapped to itself, and $\langle K \rangle A$ is mapped to $(\ulcorner A \urcorner \multimap \mathbf{af}(K)) \multimap \mathbf{af}(K)$. This is interesting because applications of linear logic in access control have been studied recently [GBB⁺06, BBG⁺07].

Future Work. An immediate subject of future work is to actually use our translations for theorem proving in access control systems. We would like to see if this idea scales to large access control policies that are used in practice.

On a more theoretical note, we would like to use our translation to explore Kripke semantics for lax logic. Since Kripke semantics of first-order logic are well understood, we should be able to derive semantics for lax logic using the translation. It would be interesting to explore how these relate to existing Kripke semantics [FM97, AMdPR01, GA08], and whether these derived semantics have some practical application in the context of access control.

In a related direction, it is possible to obtain translations from lax logic into first-order intuitionistic logic by taking existing Kripke semantics and encoding their accessibility relations as explicit predicates. It would be interesting to see if these translations relate to ours in a meaningful way.

Acknowledgments

We are grateful to Frank Pfenning for discussions and feedback on an earlier draft of this work, and to Martín Abadi for feedback on related work.

References

- [Aba03] Martín Abadi. Logic in access control. In *Proceedings of the 18th Annual Symposium on Logic in Computer Science (LICS'03)*, pages 228–233. IEEE Computer Society Press, June 2003.
- [Aba06] Martín Abadi. Access control in a core calculus of dependency. In *ICFP '06: Proceedings of the eleventh ACM SIGPLAN international conference on Functional programming*, pages 263–273, New York, NY, USA, 2006. ACM Press.
- [ABLP93] Martín Abadi, Michael Burrows, Butler Lampson, and Gordon Plotkin. A calculus for access control in distributed systems. *ACM Trans. Program. Lang. Syst.*, 15(4):706–734, 1993.

- [AF99] Andrew W. Appel and Edward W. Felten. Proof-carrying authentication. In *CCS '99: Proceedings of the 6th ACM conference on Computer and communications security*, pages 52–62, New York, NY, USA, 1999. ACM Press.
- [AMdPR01] 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.
- [Bar96] Andrew Barber. Dual intuitionistic linear logic. Technical Report ECS-LFCS-96-347, University of Edinburgh, 1996.
- [Bau03] Lujo Bauer. *Access Control for the Web via Proof-Carrying Authorization*. PhD thesis, Princeton University, November 2003.
- [BBdP98] P. N. Benton, Gavin Bierman, and Valeria de Paiva. Computational types from a logical perspective. *Journal of Functional Programming*, 8(2):177–193, 1998.
- [BBG⁺07] Kevin D. Bowers, Lujo Bauer, Deepak Garg, Frank Pfenning, and Michael K. Reiter. Consumable credentials in logic-based access-control systems. In *In Proceedings of the 14th Annual Network and Distributed System Security Symposium (NDSS 2007)*, 2007.
- [Ber04] Josh Berdine. *Linear and Affine Typing of Continuation-Passing Style*. PhD thesis, Queen Mary, University of London, 2004.
- [BORT02] Josh Berdine, Peter O’Hearn, Uday Reddy, and Hayo Thielecke. Linear continuation-passing. *Higher Order Symbol. Comput.*, 15(2-3):181–208, 2002.
- [CCD⁺07] J. G. Cederquist, R. Corin, M. A. C. Dekker, S. Etalle, J. I. den Hartog, and G. Lenzini. Audit-based compliance control. *Int. J. Inf. Secur.*, 6(2):133–151, 2007.
- [CCP03] Bor-Yuh Evan Chang, Kaustuv Chaudhuri, and Frank Pfenning. A judgmental analysis of linear logic. Technical Report CMU-CS-03-131R, December 2003.
- [DDP99] Olivier Danvy, Belmina Dzafic, and Frank Pfenning. On proving syntactic properties of CPS programs. In Andrew Gordon and Andrew Pitts, editors, *HOOTS '99, Higher Order Operational Techniques in Semantics*, volume 26 of *Electronic Notes in Theoretical Computer Science*, pages 21–33. Elsevier, 1999.
- [dPH93] Valeria de Paiva and Martin Hayland. Full intuitionistic linear logic. *Annals of Pure and Applied Logic*, 64(3):273–291, 1993.
- [Fil89] Andrzej Filinski. Declarative continuations and categorical duality. Technical Report 89/11, University of Copenhagen, 1989.
- [Fil94] Andrzej Filinski. Representing monads. In *POPL '94: Proceedings of the 21st ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, pages 446–457, New York, NY, USA, 1994. ACM.

- [FM97] Matt Fairtlough and Michael Mendler. Propositional lax logic. *Information and Computation*, 137(1):1–33, 1997.
- [FMW97] Matt Fairtlough, Michael Mendler, and Matt Walton. First order lax logic as a framework for constraint logic programming. Technical Report MIPS-9714, University of Passau, 1997.
- [FW97] Matt Fairtlough and Matt Walton. Quantified lax logic. Technical Report CS-97-11, University of Sheffield, 1997.
- [GA08] Deepak Garg and Martín Abadi. A modal deconstruction of access control logics. In *Proceedings of the 11th International Conference on Foundations of Software Science and Computation Structures (FoSSaCS 2008)*, 2008. To appear.
- [GBB⁺06] Deepak Garg, Lujo Bauer, Kevin D. Bowers, Frank Pfenning, and Michael K. Reiter. A linear logic of authorization and knowledge. In *Computer Security—ESORICS 2006: 11th European Symposium on Research in Computer Security*, volume 4189 of *Lecture Notes in Computer Science*, pages 297–312, September 2006.
- [Gir87] Jean-Yves Girard. Linear logic. *Theoretical Computer Science*, 50(1):1–102, 1987.
- [GP06] Deepak Garg and Frank Pfenning. Non-interference in constructive authorization logic. In *CSFW '06: Proceedings of the 19th IEEE Workshop on Computer Security Foundations*, pages 283–296, Washington, DC, USA, 2006. IEEE Computer Society.
- [How01] Jacob M. Howe. Proof search in lax logic. *Mathematical Structures in Computer Science*, 11(4):573–588, 2001.
- [LABW92] Butler Lampson, Martín Abadi, Michael Burrows, and Edward Wobber. Authentication in distributed systems: theory and practice. *ACM Trans. Comput. Syst.*, 10(4):265–310, 1992.
- [LLFS⁺07] Chris Lesniewski-Laas, Bryan Ford, Jacob Strauss, Robert Morris, and M. Frans Kaashoek. Alpaca: Extensible authorization for distributed services. In *Proceedings of the 14th ACM Conference on Computer and Communications Security (CCS-2007)*, Alexandria, VA, October 2007. To appear.
- [PD01] Frank Pfenning and Rowan Davies. A judgmental reconstruction of modal logic. *Mathematical Structures in Computer Science*, 11:511–540, 2001. Notes to an invited talk at the *Workshop on Intuitionistic Modal Logics and Applications (IMLA'99)*, Trento, Italy, July 1999.
- [Wad93] Philip Wadler. A taste of linear logic. In *MFCS '93: Proceedings of the 18th International Symposium on Mathematical Foundations of Computer Science*, pages 185–210, London, UK, 1993. Springer-Verlag.

A INLL

INLL has all the inference rules of intuitionistic propositional logic:

$$\begin{array}{c}
\frac{}{\Gamma, P \Rightarrow P} \text{INIT} \quad \frac{\Gamma, A, A \wedge B \Rightarrow C}{\Gamma, A \wedge B \Rightarrow C} \wedge L_1 \quad \frac{\Gamma, B, A \wedge B \Rightarrow C}{\Gamma, A \wedge B \Rightarrow C} \wedge L_2 \quad \frac{\Gamma \Rightarrow A \quad \Gamma \Rightarrow B}{\Gamma \Rightarrow A \wedge B} \wedge R \\
\\
\frac{\Gamma \Rightarrow A}{\Gamma \Rightarrow A \vee B} \vee R_1 \quad \frac{\Gamma \Rightarrow B}{\Gamma \Rightarrow A \vee B} \vee R_2 \quad \frac{\Gamma, A \Rightarrow C \quad \Gamma, B \Rightarrow C}{\Gamma, A \vee B \Rightarrow C} \vee L \\
\\
\frac{\Gamma, A \supset B \Rightarrow A \quad \Gamma, A \supset B, B \Rightarrow C}{\Gamma, A \supset B \Rightarrow C} \supset L \quad \frac{\Gamma, A \Rightarrow B}{\Gamma \Rightarrow A \supset B} \supset R \quad \frac{}{\Gamma, \perp \Rightarrow A} \perp L \quad \frac{}{\Gamma \Rightarrow \top} \top R
\end{array}$$

To these we add inference rules mirroring the left rules of intuitionistic propositional logic:

$$\begin{array}{c}
\frac{\Gamma, A, A \wedge B \Rightarrow K \text{ affirms } C}{\Gamma, A \wedge B \Rightarrow K \text{ affirms } C} \wedge L'_1 \quad \frac{\Gamma, B, A \wedge B \Rightarrow K \text{ affirms } C}{\Gamma, A \wedge B \Rightarrow K \text{ affirms } C} \wedge L'_2 \\
\\
\frac{\Gamma, A \Rightarrow C \quad \Gamma, B \Rightarrow K \text{ affirms } C}{\Gamma, A \vee B \Rightarrow K \text{ affirms } C} \vee L' \quad \frac{\Gamma, A \supset B \Rightarrow A \quad \Gamma, A \supset B, B \Rightarrow K \text{ affirms } C}{\Gamma, A \supset B \Rightarrow K \text{ affirms } C} \supset L' \\
\\
\frac{}{\Gamma, \perp \Rightarrow K \text{ affirms } C} \perp L'
\end{array}$$

Finally, we add rules connecting the two judgment forms:

$$\frac{\Gamma \Rightarrow A}{\Gamma \Rightarrow K \text{ affirms } A} \text{affirms} \quad \frac{\Gamma \Rightarrow K \text{ affirms } A}{\Gamma \Rightarrow \langle K \rangle A} \langle \rangle R \quad \frac{\Gamma, \langle K \rangle A, A \Rightarrow K \text{ affirms } C}{\Gamma, \langle K \rangle A \Rightarrow K \text{ affirms } C} \langle \rangle L$$

B Intuitionistic First-Order Logic

$$\begin{array}{c}
\frac{}{\Sigma; \Gamma, P \Rightarrow P} \text{INIT} \quad \frac{\Sigma; \Gamma, A \Rightarrow C}{\Sigma; \Gamma, A \wedge B \Rightarrow C} \wedge L_1 \quad \frac{\Sigma; \Gamma, B \Rightarrow C}{\Sigma; \Gamma, A \wedge B \Rightarrow C} \wedge L_2 \\
\\
\frac{\Sigma; \Gamma \Rightarrow A \quad \Sigma; \Gamma \Rightarrow B}{\Sigma; \Gamma \Rightarrow A \wedge B} \wedge R \quad \frac{\Sigma; \Gamma \Rightarrow A}{\Sigma; \Gamma \Rightarrow A \vee B} \vee R_1 \quad \frac{\Sigma; \Gamma \Rightarrow B}{\Sigma; \Gamma \Rightarrow A \vee B} \vee R_2 \\
\\
\frac{\Sigma; \Gamma, A \Rightarrow C \quad \Sigma; \Gamma, B \Rightarrow C}{\Sigma; \Gamma, A \vee B \Rightarrow C} \vee L \quad \frac{\Sigma; \Gamma, A \supset B \Rightarrow A \quad \Sigma; \Gamma, A \supset B, B \Rightarrow C}{\Sigma; \Gamma, A \supset B \Rightarrow C} \supset L \\
\\
\frac{\Sigma; \Gamma, A \Rightarrow B}{\Sigma; \Gamma \Rightarrow A \supset B} \supset R \quad \frac{}{\Sigma; \Gamma, \perp \Rightarrow A} \perp L \quad \frac{}{\Sigma; \Gamma \Rightarrow \top} \top R \quad \frac{\Sigma; \Gamma, \forall x.A, [t/x]A \Rightarrow C}{\Sigma; \Gamma, \forall x.A \Rightarrow C} \forall L \\
\\
\frac{\Sigma, a; \Gamma \Rightarrow [a/x]A \quad a \notin \Sigma}{\Sigma; \Gamma \Rightarrow \forall x.A} \forall R \quad \frac{\Sigma, a; \Gamma, \exists x.A, [a/x]A \Rightarrow C \quad a \notin \Sigma}{\Sigma; \Gamma, \exists x.A \Rightarrow C} \exists L \quad \frac{\Sigma; \Gamma \Rightarrow [t/x]A}{\Sigma; \Gamma \Rightarrow \exists x.A} \exists R
\end{array}$$

C Linear Logic

The syntax of intuitionistic propositional linear logic follows:

$$A, B ::= P \mid B \multimap B \mid B \supset B \mid B \otimes B \mid B \oplus B \mid B \& B \mid \mathbf{0} \mid \mathbf{1} \mid \top \mid !B$$

where ranges P over atomic propositions.

To express truth, the judgment form $B \text{ true}$ is needed. The sequent form $\Gamma; \Delta \Rightarrow B \text{ true}$ expresses hypothetical judgments. It means that under the unrestricted assumptions Γ and the restricted (linear) assumptions Δ , B is true. The two contexts have the following form:

$$\begin{aligned} \Gamma &::= \cdot \mid \Gamma, B && \text{Unrestricted Context} \\ \Delta &::= \cdot \mid \Delta, B && \text{Linear Context} \end{aligned}$$

The inference rules of the logic are as follows.

Judgmental Rules

$$\frac{}{\Gamma; P \Rightarrow P \text{ true}} \text{init} \qquad \frac{\Gamma, A; \Delta, A \Rightarrow C \text{ true}}{\Gamma, A; \Delta \Rightarrow C \text{ true}} \text{copy}$$

Multiplicative Connectives

$$\begin{aligned} &\frac{\Gamma; \Delta_1 \Rightarrow A \text{ true} \quad \Gamma; \Delta_2 \Rightarrow B \text{ true}}{\Gamma; \Delta_1, \Delta_2 \Rightarrow A \otimes B \text{ true}} \otimes R && \frac{\Gamma; \Delta, A, B \Rightarrow C \text{ true}}{\Gamma; \Delta, A \otimes B \Rightarrow C \text{ true}} \otimes L && \frac{}{\Gamma; \cdot \Rightarrow \mathbf{1} \text{ true}} \mathbf{1}R \\ &\frac{\Gamma; \Delta \Rightarrow C \text{ true}}{\Gamma; \Delta, \mathbf{1} \Rightarrow C \text{ true}} \mathbf{1}L && \frac{\Gamma; \Delta, A \Rightarrow B \text{ true}}{\Gamma; \Delta \Rightarrow A \multimap B \text{ true}} \multimap R && \frac{\Gamma; \Delta_1 \Rightarrow A \text{ true} \quad \Gamma; \Delta_2, B \Rightarrow C \text{ true}}{\Gamma; \Delta_1, \Delta_2, A \multimap B \Rightarrow C \text{ true}} \multimap L \\ &\frac{\Gamma, A; \Delta \Rightarrow B \text{ true}}{\Gamma; \Delta \Rightarrow A \supset B \text{ true}} \supset R && \frac{\Gamma; \cdot \Rightarrow A \text{ true} \quad \Gamma; \Delta, B \Rightarrow C \text{ true}}{\Gamma; \Delta, A \supset B \Rightarrow C \text{ true}} \supset L \end{aligned}$$

Additive Connectives

$$\begin{aligned} &\frac{\Gamma; \Delta \Rightarrow A \text{ true} \quad \Gamma; \Delta \Rightarrow B \text{ true}}{\Gamma; \Delta \Rightarrow A \& B \text{ true}} \& R && \frac{\Gamma; \Delta, A \Rightarrow C \text{ true}}{\Gamma; \Delta, A \& B \Rightarrow C \text{ true}} \& L_1 \\ &\frac{\Gamma; \Delta, B \Rightarrow C \text{ true}}{\Gamma; \Delta, A \& B \Rightarrow C \text{ true}} \& L_2 && \frac{}{\Gamma; \Delta \Rightarrow \top \text{ true}} \top R && \text{no } \top L \text{ rule} && \frac{\Gamma; \Delta \Rightarrow A \text{ true}}{\Gamma; \Delta \Rightarrow A \oplus B \text{ true}} \oplus R_1 \\ &\frac{\Gamma; \Delta \Rightarrow B \text{ true}}{\Gamma; \Delta \Rightarrow A \oplus B \text{ true}} \oplus R_2 && \frac{\Gamma; \Delta, A \Rightarrow C \text{ true} \quad \Gamma; \Delta, B \Rightarrow C \text{ true}}{\Gamma; \Delta, A \oplus B \Rightarrow C \text{ true}} \oplus L && \frac{}{\Gamma; \Delta, \mathbf{0} \Rightarrow C \text{ true}} \mathbf{0}L \end{aligned}$$

Exponential Connective

$$\frac{\Gamma; \cdot \Rightarrow A \text{ true}}{\Gamma; \cdot \Rightarrow !A \text{ true}} !R \qquad \frac{\Gamma, A; \Delta \Rightarrow C \text{ true}}{\Gamma; \Delta, !A \Rightarrow C \text{ true}} !L$$

D Proof of Completeness for First-Order Translation

Before proving completeness, we must prove a lemma.

Lemma D.1. $\lceil [t/x]A \rceil = [t/x]\lceil A \rceil$ where t ranges over terms.

Proof. By induction on the structure of A . □

Now we prove completeness. By the definition of $\lceil \Sigma, \Gamma \Rightarrow \gamma \rceil$, this may be shown by proving

1. if $\Sigma; \Gamma \Rightarrow C$, then $\Sigma; \lceil \Gamma \rceil \Rightarrow \lceil C \rceil$; and
2. if $\Sigma; \Gamma \Rightarrow K$ affirms C , then for any fresh a , $\Sigma, a; \lceil \Gamma \rceil, \lceil C \rceil \supset \mathbf{af}(K, a) \Rightarrow \mathbf{af}(K, a)$.

We prove these statements by simultaneous induction over the derivations \mathcal{D} of $\Sigma; \Gamma \Rightarrow A$ or $\Sigma; \Gamma \Rightarrow K$ affirms C :

Case: $\mathcal{D} = \frac{}{\Sigma; \Gamma, P \Rightarrow \bar{P}} \text{INIT}$

1. $\Sigma; \Gamma, P \Rightarrow \bar{P}$ by INIT
2. $\Sigma; \lceil \Gamma, P \rceil \Rightarrow \lceil \bar{P} \rceil$ by definition of $\lceil \cdot \rceil$

Case: $\mathcal{D} = \frac{}{\Sigma; \Gamma, \perp \Rightarrow C} \perp \text{L}$

1. $\Sigma; \lceil \Gamma \rceil, \perp \Rightarrow \lceil C \rceil$ by $\perp \text{L}$
2. $\Sigma; \lceil \Gamma, \perp \rceil \Rightarrow \lceil C \rceil$ by definition of $\lceil \cdot \rceil$

Case: $\mathcal{D} = \frac{}{\Sigma; \Gamma, \perp \Rightarrow K \text{ affirms } C} \perp \text{L}'$

1. $\Sigma, a; \lceil \Gamma \rceil, \perp, \lceil C \rceil \supset \mathbf{af}(K, a) \Rightarrow \mathbf{af}(K, a)$ by $\perp \text{L}$
2. $\Sigma, a; \lceil \Gamma, \perp \rceil, \lceil C \rceil \supset \mathbf{af}(K, a) \Rightarrow \mathbf{af}(K, a)$ by definition of $\lceil \cdot \rceil$

Case: $\mathcal{D} = \frac{\Sigma; \Gamma, A \supset B \Rightarrow A \quad \Sigma; \Gamma, A \supset \bar{B}, B \Rightarrow C}{\Sigma; \Gamma, A \supset B \Rightarrow C} \supset \text{L}$

1. $\Sigma; \lceil \Gamma, A \supset B \rceil \Rightarrow \lceil A \rceil$ by i.h. on \mathcal{D}_1
2. $\Sigma; \lceil \Gamma \rceil, \lceil A \rceil \supset \lceil B \rceil \Rightarrow \lceil A \rceil$ by definition of $\lceil \cdot \rceil$
3. $\Sigma; \lceil \Gamma, A \supset B, B \rceil \Rightarrow \lceil C \rceil$ by i.h. on \mathcal{D}_2
4. $\Sigma; \lceil \Gamma \rceil, \lceil A \rceil \supset \lceil B \rceil, \lceil B \rceil \Rightarrow \lceil C \rceil$ by definition of $\lceil \cdot \rceil$
5. $\Sigma; \lceil \Gamma \rceil, \lceil A \rceil \supset \lceil B \rceil \Rightarrow \lceil C \rceil$ by $\supset \text{L}$
6. $\Sigma; \lceil \Gamma, A \supset B \rceil \Rightarrow \lceil C \rceil$ by definition of $\lceil \cdot \rceil$

Case: $\mathcal{D} = \frac{\Sigma; \Gamma, A \supset B \Rightarrow A \quad \Sigma; \Gamma, A \supset B, B \Rightarrow K \text{ affirms } C}{\Sigma; \Gamma, A \supset B \Rightarrow K \text{ affirms } C} \supset \text{L}'$

1. $\Sigma; \lceil \Gamma, A \supset B \rceil \Rightarrow \lceil A \rceil$ by i.h. on \mathcal{D}_1
2. $\Sigma; \lceil \Gamma \rceil, \lceil A \rceil \supset \lceil B \rceil \Rightarrow \lceil A \rceil$ by definition of $\lceil \cdot \rceil$
3. $\Sigma, a; \lceil \Gamma \rceil, \lceil A \rceil \supset \lceil B \rceil, \lceil C \rceil \supset \mathbf{af}(K, a) \Rightarrow \lceil A \rceil$ by weakening
4. $\Sigma, a; \lceil \Gamma, A \supset B, B \rceil, \lceil C \rceil \supset \mathbf{af}(K, a) \Rightarrow \mathbf{af}(K, a)$ by i.h. on \mathcal{D}_2
5. $\Sigma, a; \lceil \Gamma \rceil, \lceil A \rceil \supset \lceil B \rceil, \lceil B \rceil, \lceil C \rceil \supset \mathbf{af}(K, a) \Rightarrow \mathbf{af}(K, a)$ by definition of $\lceil \cdot \rceil$
6. $\Sigma, a; \lceil \Gamma \rceil, \lceil A \rceil \supset \lceil B \rceil, \lceil C \rceil \supset \mathbf{af}(K, a) \Rightarrow \mathbf{af}(K, a)$ by $\supset \text{L}$
7. $\Sigma, a; \lceil \Gamma, A \supset B \rceil, \lceil C \rceil \supset \mathbf{af}(K, a) \Rightarrow \mathbf{af}(K, a)$ by definition of $\lceil \cdot \rceil$

$$\text{Case: } \mathcal{D} = \frac{\mathcal{D}_1}{\Sigma; \Gamma \Rightarrow A \supset B} \supset R$$

1. $\Sigma; \ulcorner \Gamma, A \urcorner \Rightarrow \ulcorner B \urcorner$ by i.h. on \mathcal{D}_1
2. $\Sigma; \ulcorner \Gamma \urcorner, \ulcorner A \urcorner \Rightarrow \ulcorner B \urcorner$ by definition of $\ulcorner \cdot \urcorner$
3. $\Sigma; \ulcorner \Gamma \urcorner \Rightarrow \ulcorner A \urcorner \supset \ulcorner B \urcorner$ by $\supset R$
4. $\Sigma; \ulcorner \Gamma \urcorner \Rightarrow \ulcorner A \supset B \urcorner$ by definition of $\ulcorner \cdot \urcorner$

$$\text{Case: } \mathcal{D} = \frac{\mathcal{D}_1}{\Sigma; \Gamma \Rightarrow K \text{ affirms } C} \text{ affirms}$$

1. $\Sigma; \ulcorner \Gamma \urcorner \Rightarrow \ulcorner C \urcorner$ by i.h. on \mathcal{D}_1
2. $\Sigma, a; \ulcorner \Gamma \urcorner, \ulcorner C \urcorner \supset \mathbf{af}(K, a) \Rightarrow \ulcorner C \urcorner$ by weakening
3. $\Sigma, a; \mathbf{af}(K, a) \Rightarrow \mathbf{af}(K, a)$ by INIT
4. $\Sigma, a; \ulcorner \Gamma \urcorner, \ulcorner C \urcorner \supset \mathbf{af}(K, a), \mathbf{af}(K, a) \Rightarrow \mathbf{af}(K, a)$ by weakening
5. $\Sigma, a; \ulcorner \Gamma \urcorner, \ulcorner C \urcorner \supset \mathbf{af}(K, a) \Rightarrow \mathbf{af}(K, a)$ by $\supset L$

$$\text{Case: } \mathcal{D} = \frac{\mathcal{D}_1}{\Sigma; \Gamma \Rightarrow \langle K \rangle C} \langle \rangle R$$

1. $\Sigma, a; \ulcorner \Gamma \urcorner, \ulcorner C \urcorner \supset \mathbf{af}(K, a) \Rightarrow \mathbf{af}(K, a)$ where a is fresh by i.h. on \mathcal{D}_1
2. $\Sigma, a; \ulcorner \Gamma \urcorner \Rightarrow (\ulcorner C \urcorner \supset \mathbf{af}(K, a)) \supset \mathbf{af}(K, a)$ by $\supset R$
3. $\Sigma; \ulcorner \Gamma \urcorner \Rightarrow \forall x. (\ulcorner C \urcorner \supset \mathbf{af}(K, x)) \supset \mathbf{af}(K, x)$ by $\forall R$ (a is fresh)
4. $\Sigma; \ulcorner \Gamma \urcorner \Rightarrow \ulcorner \langle K \rangle C \urcorner$ by definition of $\ulcorner \cdot \urcorner$

$$\text{Case: } \mathcal{D} = \frac{\mathcal{D}_1}{\Sigma; \Gamma, \langle K \rangle A, A \Rightarrow K \text{ affirms } C} \langle \rangle L$$

1. $\Sigma, a; \ulcorner \Gamma, \langle K \rangle A, A \urcorner, \ulcorner C \urcorner \supset \mathbf{af}(K, a) \Rightarrow \mathbf{af}(K, a)$ by i.h. on \mathcal{D}_1
2. $\Sigma, a; \ulcorner \Gamma \urcorner, \ulcorner \langle K \rangle A \urcorner, \ulcorner A \urcorner, \ulcorner C \urcorner \supset \mathbf{af}(K, a) \Rightarrow \mathbf{af}(K, a)$ by definition of $\ulcorner \cdot \urcorner$
3. $\Sigma, a; \ulcorner \Gamma \urcorner, \ulcorner \langle K \rangle A \urcorner, \ulcorner C \urcorner \supset \mathbf{af}(K, a) \Rightarrow \ulcorner A \urcorner \supset \mathbf{af}(K, a)$ by $\supset R$
4. $\Sigma, a; \ulcorner \Gamma \urcorner, \ulcorner \langle K \rangle A \urcorner, (\ulcorner A \urcorner \supset \mathbf{af}(K, a)) \supset \mathbf{af}(K, a), \ulcorner C \urcorner \supset \mathbf{af}(K, a) \Rightarrow \ulcorner A \urcorner \supset \mathbf{af}(K, a)$ by weakening
5. $\Sigma, a; \mathbf{af}(K, a) \Rightarrow \mathbf{af}(K, a)$ by INIT
6. $\Sigma, a; \ulcorner \Gamma \urcorner, \ulcorner \langle K \rangle A \urcorner, (\ulcorner A \urcorner \supset \mathbf{af}(K, a)) \supset \mathbf{af}(K, a), \ulcorner C \urcorner \supset \mathbf{af}(K, a), \mathbf{af}(K, a) \Rightarrow \mathbf{af}(K, a)$ by weakening
7. $\Sigma, a; \ulcorner \Gamma \urcorner, \ulcorner \langle K \rangle A \urcorner, (\ulcorner A \urcorner \supset \mathbf{af}(K, a)) \supset \mathbf{af}(K, a), \ulcorner C \urcorner \supset \mathbf{af}(K, a) \Rightarrow \mathbf{af}(K, a)$ by $\supset L$
8. $\Sigma, a; \ulcorner \Gamma \urcorner, \forall x. (\ulcorner A \urcorner \supset \mathbf{af}(K, x)) \supset \mathbf{af}(K, x), (\ulcorner A \urcorner \supset \mathbf{af}(K, a)) \supset \mathbf{af}(K, a), \ulcorner C \urcorner \supset \mathbf{af}(K, a) \Rightarrow \mathbf{af}(K, a)$ by definition of $\ulcorner \cdot \urcorner$
9. $\Sigma, a; \ulcorner \Gamma \urcorner, \forall x. (\ulcorner A \urcorner \supset \mathbf{af}(K, x)) \supset \mathbf{af}(K, x), \ulcorner C \urcorner \supset \mathbf{af}(K, a) \Rightarrow \mathbf{af}(K, a)$

· pleasant	$\frac{\Gamma \text{ pleasant}}{\Gamma, \ulcorner C \urcorner \text{ pleasant}}$	$\frac{\Gamma \text{ pleasant}}{\Gamma, \mathbf{af}(K, t) \text{ pleasant}}$	$\frac{\Gamma \text{ pleasant}}{\Gamma, \ulcorner C \urcorner \supset \mathbf{af}(K, t) \text{ pleasant}}$
$\frac{\Gamma \text{ pleasant}}{\Gamma, (\ulcorner C \urcorner \supset \mathbf{af}(K, t)) \supset \mathbf{af}(K, t) \text{ pleasant}}$			

Table 1: The formal definition of *pleasant*.

- | | |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------|
| | by $\forall L$ |
| 10. $\Sigma, a; \ulcorner \Gamma \urcorner, \ulcorner \langle K \rangle A \urcorner, \ulcorner C \urcorner \supset \mathbf{af}(K, a) \Rightarrow \mathbf{af}(K, a)$ | by definition of $\ulcorner \cdot \urcorner$ |
| 11. $\Sigma, a; \ulcorner \Gamma \urcorner, \langle K \rangle A \urcorner, \ulcorner C \urcorner \supset \mathbf{af}(K, a) \Rightarrow \mathbf{af}(K, a)$ | by definition of $\ulcorner \cdot \urcorner$ |

E Proof of Soundness for First-Order Translation

E.1 A Lemma

Before we can prove soundness, we need to define a few forms in which various terms may be found. We define these forms to focus our attention on only those formulas that can arise from proving a the translated sequent.

- Let the proposition D be called (K, t) -*nice* if it has the form $\ulcorner C \urcorner, \mathbf{af}(K, t), \ulcorner C \urcorner \supset \mathbf{af}(K, t)$, or $(\ulcorner C \urcorner \supset \mathbf{af}(K, t)) \supset \mathbf{af}(K, t)$.
- Let the proposition A be called (K, t) -*mean* if it has the form $\mathbf{af}(K'', t''), \ulcorner B \urcorner \supset \mathbf{af}(K'', t'')$, or $(\ulcorner B \urcorner \supset \mathbf{af}(K'', t'')) \supset \mathbf{af}(K'', t'')$ where $K'' \neq K$ or $t'' \neq t$.
- Let a hypothesis context Γ be called *pleasant* if Γ is empty or Γ has the form Γ', E for some proposition E where Γ' is pleasant and E has the form $\ulcorner C \urcorner, \mathbf{af}(K, t), \ulcorner C \urcorner \supset \mathbf{af}(K, t)$, or $(\ulcorner C \urcorner \supset \mathbf{af}(K, t)) \supset \mathbf{af}(K, t)$.

Pleasant is more formally defined in Table 1.

Lemma E.1. *Let \mathcal{D} be a derivation of $\Sigma; \Gamma, A \Rightarrow D$ where D is (K, t) -nice, Γ is pleasant, and A is (K, t) -mean. There exists a derivation \mathcal{D}' of $\Sigma; \Gamma \Rightarrow D$ that is a shorter or equal in length to \mathcal{D} .*

Proof. Now we simultaneously induct on the given derivation \mathcal{D} for all values of K and t .

Case: $\mathcal{D} = \frac{}{\Sigma; \Gamma, A \Rightarrow D} \text{INIT}$

Since D is (K, t) -nice, it ranges over $\ulcorner C \urcorner, \mathbf{af}(K, t), \ulcorner C \urcorner \supset \mathbf{af}(K, t)$, and $(\ulcorner C \urcorner \supset \mathbf{af}(K, t)) \supset \mathbf{af}(K, t)$. Since A is (K, t) -mean, A cannot be equal to D . Thus, D is in Γ and $\Sigma; \Gamma \Rightarrow D$ by INIT.

Case: $\mathcal{D} = \frac{}{\Sigma; \Gamma, A \Rightarrow D} \perp R$

A cannot be \perp since A is (K, t) -mean. Thus, \perp must be in Γ and $\Sigma; \Gamma \Rightarrow D$ follows in one step by $\perp R$.

Case: $\supset R$

Subcase: $\mathcal{D} = \frac{\mathcal{D}_1 \quad \Sigma; \Gamma, A, \ulcorner C \urcorner \supset \mathbf{af}(K, t) \Rightarrow \mathbf{af}(K, t)}{\Sigma; \Gamma, A \Rightarrow (\ulcorner C \urcorner \supset \mathbf{af}(K, t)) \supset \mathbf{af}(K, t)} \supset R$

$\Gamma, \ulcorner C \urcorner \supset \mathbf{af}(K, t)$ is pleasant, $\mathbf{af}(K, t)$ is (K, t) -nice, and A is (K, t) -mean. Thus, the i.h. applies to \mathcal{D}_1 . By the i.h. on \mathcal{D}_1 , $\Sigma; \Gamma, \ulcorner C \urcorner \supset \mathbf{af}(K, t) \Rightarrow \mathbf{af}(K, t)$ has a derivation \mathcal{D}'_1 with a length less than or equal to that of \mathcal{D}_1 . Make \mathcal{D}' by extending \mathcal{D}'_1 with $\supset R$ to prove $\Sigma; \Gamma \Rightarrow (\ulcorner C \urcorner \supset \mathbf{af}(K, t)) \supset \mathbf{af}(K, t)$. Since \mathcal{D} is one step longer than \mathcal{D}_1 , \mathcal{D}'_1 is equal to or less than \mathcal{D}_1 in length, and \mathcal{D}' is one step longer than \mathcal{D}'_1 , \mathcal{D}' is equal to or less than \mathcal{D} in length.

Subcase: $\mathcal{D} = \frac{\mathcal{D}_1 \quad \Sigma; \Gamma, A, \ulcorner C \urcorner \Rightarrow \mathbf{af}(K, t)}{\Sigma; \Gamma, A \Rightarrow \ulcorner C \urcorner \supset \mathbf{af}(K, t)} \supset R$

By the i.h. on \mathcal{D}_1 , $\Sigma; \Gamma, \ulcorner C \urcorner \Rightarrow \mathbf{af}(K, t)$ has a derivation \mathcal{D}'_1 with a length no greater than that of \mathcal{D}_1 . Make \mathcal{D}' by extending \mathcal{D}'_1 with $\supset R$ to prove $\Sigma; \Gamma \Rightarrow \ulcorner C \urcorner \supset \mathbf{af}(K, t)$ in no more steps than \mathcal{D} .

Subcase: $\mathcal{D} = \frac{\mathcal{D}_1 \quad \Sigma; \Gamma, A, \ulcorner E \urcorner \Rightarrow \ulcorner F \urcorner}{\Sigma; \Gamma, A \Rightarrow \ulcorner E \urcorner \supset \ulcorner F \urcorner} \supset R$

By the i.h. on \mathcal{D}_1 , $\Sigma; \Gamma, \ulcorner E \urcorner \Rightarrow \ulcorner F \urcorner$ has a derivation \mathcal{D}'_1 with a length no greater than that of \mathcal{D}_1 . Make \mathcal{D}' by extending \mathcal{D}'_1 with $\supset R$ to prove $\Sigma; \Gamma \Rightarrow \ulcorner E \urcorner \supset \ulcorner F \urcorner$ in no more steps than \mathcal{D} .

Case: When $\supset L$ is the last rule in \mathcal{D} , either A can be principal or not.

Subcase: A is principal. In this case, A has the form $\ulcorner B \urcorner \supset \mathbf{af}(K'', t'')$ or $(\ulcorner B \urcorner \supset \mathbf{af}(K'', t'')) \supset \mathbf{af}(K'', t'')$ where $K'' \neq K$ or $t'' \neq t$ since A is (K, t) -mean. That is A is of the form $E \supset \mathbf{af}(K'', t'')$ where E is either $\ulcorner B \urcorner$ or $\ulcorner B \urcorner \supset \mathbf{af}(K'', t'')$. Either way,

$$\mathcal{D} = \frac{\Sigma; \Gamma, E \supset \mathbf{af}(K'', t'') \Rightarrow E \quad \Sigma; \Gamma, E \supset \mathbf{af}(K'', t''), \mathbf{af}(K'', t'') \Rightarrow D}{\Sigma; \Gamma, E \supset \mathbf{af}(K'', t'') \Rightarrow D} \supset L$$

$\Gamma, \mathbf{af}(K'', t'')$ is pleasant. By the i.h. on \mathcal{D}_2 , $\Sigma; \Gamma, \mathbf{af}(K'', t'') \Rightarrow D$ has a derivation \mathcal{D}'_2 with a length no greater than that of \mathcal{D}_1 . Since \mathcal{D}'_2 is no greater in size than \mathcal{D}_2 and $\mathbf{af}(K'', t'')$ is (K, t) -mean, we may select $\mathbf{af}(K'', t'')$ as A and again apply the i.h. This yields that $\Sigma; \Gamma \Rightarrow D$ has a derivation of \mathcal{D}'_2 with a size no greater than that of \mathcal{D}'_2 . Since \mathcal{D}'_2 must also be no larger than \mathcal{D}_2 , which is smaller than \mathcal{D} , we are done.

Subcase: A is not principal. In this case the principal formula must be in Γ . Since Γ is pleasant and the principal formula is an implication, it must have one of the following forms: $\ulcorner E \urcorner \supset \ulcorner F \urcorner$, $\ulcorner E \urcorner \supset \mathbf{af}(K', t')$, or $(\ulcorner E \urcorner \supset \mathbf{af}(K', t')) \supset \mathbf{af}(K', t')$. First, we consider when the principal formula has one of the first two forms. Second, we consider when it has the last form.

Subsubcase: Let B range over $\ulcorner F \urcorner$ and $\mathbf{af}(K', t')$.

$$\mathcal{D} = \frac{\frac{\mathcal{D}_1}{\Sigma; \Gamma, \ulcorner E \urcorner \supset B, A \Rightarrow \ulcorner E \urcorner} \quad \frac{\mathcal{D}_2}{\Sigma; \Gamma, \ulcorner E \urcorner \supset B, B, A \Rightarrow D}}{\Sigma; \Gamma, \ulcorner E \urcorner \supset B, A \Rightarrow D} \supset \text{L}$$

$\ulcorner E \urcorner$ is (K, t) -nice and $\Gamma, \ulcorner E \urcorner \supset B$ is pleasant. By the i.h. on \mathcal{D}_1 , $\Sigma; \Gamma, \ulcorner E \urcorner \supset B \Rightarrow \ulcorner E \urcorner$ has a derivation \mathcal{D}'_1 with a length no greater than that of \mathcal{D}_1 . $\Gamma, \ulcorner E \urcorner \supset B, B$ is pleasant. By the i.h. on \mathcal{D}_2 , $\Sigma; \Gamma, \ulcorner E \urcorner \supset B, B \Rightarrow D$ has a derivation \mathcal{D}'_2 with a length no greater than that of \mathcal{D}_2 . Make \mathcal{D}' by combining \mathcal{D}'_1 and \mathcal{D}'_2 with $\supset \text{L}$ to prove $\Sigma; \Gamma, \ulcorner E \urcorner \supset B \Rightarrow D$ in no more steps than \mathcal{D} .

Subsubcase: The only remaining case is when principal formula has the form $(\ulcorner E \urcorner \supset \mathbf{af}(K', t')) \supset \mathbf{af}(K', t')$. This means that \mathcal{D} has the form

$$\frac{\mathcal{F}_1 \quad \mathcal{F}_2}{\Sigma; \Gamma, (\ulcorner E \urcorner \supset \mathbf{af}(K', t')) \supset \mathbf{af}(K', t'), A \Rightarrow D} \supset \text{L}$$

where $\mathcal{F}_1 = \frac{\mathcal{D}_1}{\Sigma; \Gamma, (\ulcorner E \urcorner \supset \mathbf{af}(K', t')) \supset \mathbf{af}(K', t'), A \Rightarrow \ulcorner E \urcorner \supset \mathbf{af}(K', t')}$

and $\mathcal{F}_2 = \frac{\mathcal{D}_2}{\Sigma; \Gamma, (\ulcorner E \urcorner \supset \mathbf{af}(K', t')) \supset \mathbf{af}(K', t'), \mathbf{af}(K', t'), A \Rightarrow D}$

Since A is (K, t) -mean, A must have one of the following forms $\mathbf{af}(K'', t'')$, $\ulcorner B \urcorner \supset \mathbf{af}(K'', t'')$, or $(\ulcorner B \urcorner \supset \mathbf{af}(K'', t'')) \supset \mathbf{af}(K'', t'')$ where $K'' \neq K$ or $t'' \neq t$. We now consider two cases:

Subsubsubcase: $K'' = K'$ and $t'' = t'$. Since $K' \neq K$ or $t' \neq t$, $\mathbf{af}(K', t')$ is (K, t) -mean. We may use the i.h. on \mathcal{D}_2 to delete A and produce a derivation \mathcal{D}'_2 of $\Sigma; \Gamma, (\ulcorner E \urcorner \supset \mathbf{af}(K', t')) \supset \mathbf{af}(K', t'), \mathbf{af}(K', t') \Rightarrow D$ that is no longer than \mathcal{D}_2 . Since $\mathbf{af}(K', t')$ is also (K, t) -mean, the i.h. may be used again on \mathcal{D}'_2 to produce a derivation \mathcal{D}''_2 of $\Sigma; \Gamma, (\ulcorner E \urcorner \supset \mathbf{af}(K', t')) \supset \mathbf{af}(K', t') \Rightarrow D$ that is no longer than \mathcal{D}'_2 or \mathcal{D}_2 . \mathcal{D}''_2 is the needed derivation \mathcal{D}' in the required length.

Subsubsubcase: $K'' \neq K'$ or $t'' \neq t'$. A is (K', t') -mean. Furthermore, $\ulcorner E \urcorner \supset \mathbf{af}(K', t')$ is (K', t') -nice and $\Gamma, (\ulcorner E \urcorner \supset \mathbf{af}(K', t')) \supset \mathbf{af}(K', t')$ is pleasant. Thus, we may use the i.h. with K' and t' instead of K and t on \mathcal{D}_1 to produce a derivation \mathcal{D}'_1 of $\Sigma; \Gamma, (\ulcorner E \urcorner \supset \mathbf{af}(K', t')) \supset \mathbf{af}(K', t') \Rightarrow \ulcorner E \urcorner \supset \mathbf{af}(K', t')$ with a length no greater than that of \mathcal{D}_1 .

We may use the i.h. with K and t on \mathcal{D}_2 to produce a derivation \mathcal{D}'_2 of $\Sigma; \Gamma, (\ulcorner E \urcorner \supset \mathbf{af}(K', t')) \supset \mathbf{af}(K', t'), \mathbf{af}(K', t') \Rightarrow D$ with a length no greater than that of \mathcal{D}_2 .

To make \mathcal{D}' of the required length combine \mathcal{D}'_1 and \mathcal{D}'_2 with $\supset \text{L}$.

Case: When $\forall \text{L}$ is the last rule applied in \mathcal{D} , the principal formula cannot be A since A is (K, t) -mean. Thus, it must be in Γ . Since Γ is pleasant, the principal formula must have one of the following forms: $\ulcorner \langle K' \rangle E \urcorner = \forall x. (\ulcorner E \urcorner \supset \mathbf{af}(K', x)) \supset \mathbf{af}(K', x)$ or $\ulcorner \forall x. E \urcorner = \forall x. \ulcorner E \urcorner$.

$$\text{Subcase: } \mathcal{D} = \frac{\frac{\mathcal{D}_1}{\Sigma; \Gamma, \ulcorner \langle K' \rangle E \urcorner, (\ulcorner E \urcorner \supset \mathbf{af}(K', t')) \supset \mathbf{af}(K', t'), A \Rightarrow D}}{\Sigma; \Gamma, \ulcorner \langle K' \rangle E \urcorner, A \Rightarrow D} \forall \text{L}$$

$\Gamma, \ulcorner \langle K' \rangle E \urcorner, (\ulcorner E \urcorner \supset \mathbf{af}(K', t')) \supset \mathbf{af}(K', t')$ is pleasant. By the i.h. on \mathcal{D}_1 , we know that $\Sigma; \Gamma, \ulcorner \langle K' \rangle E \urcorner, (\ulcorner E \urcorner \supset \mathbf{af}(K', t')) \supset \mathbf{af}(K', t') \Rightarrow D$ has a derivation \mathcal{D}'_1 with a length no greater than that of \mathcal{D}_1 . Make \mathcal{D}' by extending \mathcal{D}'_1 with $\forall \text{L}$ to prove $\Sigma; \Gamma, \ulcorner \langle K' \rangle E \urcorner \Rightarrow D$ in no more steps than \mathcal{D} .

$$\text{Subcase: } \mathcal{D} = \frac{\mathcal{D}_1}{\Sigma; \Gamma, \forall x. \ulcorner E \urcorner, [t'/x] \ulcorner E \urcorner, A \Rightarrow D} \forall L$$

By Lemma D.1, $[t'/x] \ulcorner E \urcorner$ is equal to $\ulcorner [t'/x] E \urcorner$. Thus, $\Gamma, \forall x. \ulcorner E \urcorner, [t'/x] \ulcorner E \urcorner$ is pleasant. By the i.h. on \mathcal{D}_1 , $\Sigma; \Gamma, \forall x. \ulcorner E \urcorner, [t'/x] \ulcorner E \urcorner \Rightarrow D$ has a derivation \mathcal{D}'_1 with a length no greater than that of \mathcal{D}_1 . Make \mathcal{D}' by extending \mathcal{D}'_1 with $\forall L$ to prove $\Sigma; \Gamma, \forall x. \ulcorner E \urcorner \Rightarrow D$ in no more steps than \mathcal{D} .

Case: $\forall R$ is the last rule in \mathcal{D} . In this case D must have the form $\ulcorner \langle K \rangle C \urcorner$ or $\forall x. \ulcorner C \urcorner$ since D is (K, t) -nice.

$$\text{Subcase: } \mathcal{D} = \frac{\mathcal{D}_1}{\Sigma; \Gamma, A \Rightarrow (\ulcorner C \urcorner \supset \mathbf{af}(K, a)) \supset \mathbf{af}(K, a)} \forall R$$

Note that a is fresh and does not equal t , and that $\ulcorner \langle K \rangle C \urcorner$ is $\forall x. (\ulcorner C \urcorner \supset \mathbf{af}(K, x)) \supset \mathbf{af}(K, x)$. Since A is (K, t) -mean and a is fresh and not in A , A is (K, a) -mean. $(\ulcorner C \urcorner \supset \mathbf{af}(K, a)) \supset \mathbf{af}(K, a)$ is (K, a) -nice. By i.h. on \mathcal{D}_1 , $\Sigma, a; \Gamma \Rightarrow (\ulcorner C \urcorner \supset \mathbf{af}(K, a)) \supset \mathbf{af}(K, a)$ has a derivation \mathcal{D}'_1 with a length no greater than that of \mathcal{D}_1 . Make \mathcal{D}' by extending \mathcal{D}'_1 with $\forall R$ to prove $\Sigma; \Gamma \Rightarrow \forall x. (\ulcorner C \urcorner \supset \mathbf{af}(K, x)) \supset \mathbf{af}(K, x)$, which is $\Sigma; \Gamma \Rightarrow \ulcorner \langle K \rangle C \urcorner$, in no more steps than \mathcal{D} .

$$\text{Subcase: } \mathcal{D} = \frac{\mathcal{D}_1}{\Sigma; \Gamma, A \Rightarrow [a/x] \ulcorner C \urcorner} \forall R$$

Note that $[a/x] \ulcorner C \urcorner$ is equal to $\ulcorner [a/x] C \urcorner$ by Lemma D.1. Thus, $[a/x] \ulcorner C \urcorner$ is (K, t) -nice. So we may use the i.h. on \mathcal{D}_1 to conclude that $\Sigma, a; \Gamma \Rightarrow \ulcorner [a/x] C \urcorner$ has a derivation \mathcal{D}'_1 with a length no greater than that of \mathcal{D}_1 . Make \mathcal{D}' by extending \mathcal{D}'_1 with $\forall R$ to prove $\Sigma; \Gamma \Rightarrow \forall x. \ulcorner C \urcorner$ in no more steps than \mathcal{D} .

□

E.2 More Definitions

To prove soundness, we will prove a stronger statement of formulas of a certain form. A sequent $\Sigma; \Gamma \Rightarrow \gamma$ is *regular* iff one of the following sets of conditions hold:

1. (a) $\gamma = \ulcorner A \urcorner$ and
(b) All assumptions in Γ have the form $\ulcorner B \urcorner$
2. (a) $\gamma = \mathbf{af}(K, a)$ for a parameter a ,
(b) all assumptions in Γ have the form $\ulcorner B \urcorner$ or $(\ulcorner C \urcorner \supset \mathbf{af}(K, a)) \supset \mathbf{af}(K, a)$, and
(c) a occurs only inside assumptions of 2nd form.

Let the inverse translation $\lfloor A \rfloor$ be defined by Table 2 and $\lfloor \Gamma, A \rfloor = \lfloor \Gamma \rfloor, \lfloor A \rfloor$ and $\lfloor \cdot \rfloor = \cdot$. Note that $A = \lfloor \ulcorner A \urcorner \rfloor$ for all propositions A of INLL.

If the hypothesis context Γ is pleasant, then every formula in Γ has the form $\ulcorner C \urcorner$, $\mathbf{af}(K, t)$, $\ulcorner C \urcorner \supset \mathbf{af}(K, t)$, or $(\ulcorner C \urcorner \supset \mathbf{af}(K, t)) \supset \mathbf{af}(K, t)$. Let $\Gamma \downarrow$ denote Γ restricted to only those formulas of the form $\ulcorner C \urcorner$. Let $\Gamma \uparrow$ denote those formulas of the remaining three forms. So $\Gamma = \Gamma \downarrow, \Gamma \uparrow$.

$$\begin{aligned}
& \llbracket P \rrbracket = P \\
& \llbracket A_1 \wedge A_2 \rrbracket = \llbracket A_1 \rrbracket \wedge \llbracket A_2 \rrbracket \\
& \llbracket A_1 \vee A_2 \rrbracket = \llbracket A_1 \rrbracket \vee \llbracket A_2 \rrbracket \\
& \llbracket A_1 \supset A_2 \rrbracket = \llbracket A_1 \rrbracket \supset \llbracket A_2 \rrbracket \\
& \llbracket \top \rrbracket = \top \\
& \llbracket \perp \rrbracket = \perp \\
& \llbracket \forall x.(A \supset \mathbf{af}(K, x)) \supset \mathbf{af}(K, x) \rrbracket = \langle K \rangle \llbracket A \rrbracket \\
& \llbracket (A \supset \mathbf{af}(K, a)) \supset \mathbf{af}(K, a) \rrbracket = \langle K \rangle \llbracket A \rrbracket
\end{aligned}$$

Table 2: Inverse Translation Rules

E.3 The Theorem

Soundness is corollary to the following theorem.

Theorem E.2.

1. if $\Sigma; \ulcorner \Gamma \urcorner \Rightarrow \ulcorner A \urcorner$, then $\Gamma \Rightarrow A$.
2. if $\Sigma, a; \Gamma, \ulcorner D \urcorner \supset \mathbf{af}(K, a) \Rightarrow \mathbf{af}(K, a)$ and $\Sigma, a; \Gamma \Rightarrow \mathbf{af}(K, a)$ is regular, then $\ulcorner \Gamma \urcorner \Rightarrow K$ affirms D .

Note that since $\Sigma; \Gamma \Rightarrow A$ and $\Sigma, a; \Gamma \Rightarrow \mathbf{af}(K, a)$ is regular, $\ulcorner \Gamma \urcorner$ and $\ulcorner A \urcorner$ are defined.

Since $\ulcorner \ulcorner A \urcorner \urcorner = A$, the statement (i) is equivalent to

(i') if $\Sigma; \Gamma \Rightarrow A$ and $\Sigma; \Gamma \Rightarrow A$ is regular, then $\ulcorner \Gamma \urcorner \Rightarrow \ulcorner A \urcorner$.

Proof. Now we prove (i) and (ii) by simultaneous induction on the derivation \mathcal{D} of $\Sigma; \Gamma \Rightarrow A$ and \mathcal{E} of $\Sigma, a; \Gamma, \ulcorner D \urcorner \supset \mathbf{af}(K, a) \Rightarrow \mathbf{af}(K, a)$.

Case: $\mathcal{D} = \frac{}{\Sigma; \ulcorner \Gamma \urcorner, \ulcorner P \urcorner \Rightarrow \ulcorner P \urcorner}$ INIT

1. $\Gamma, P \Rightarrow P$ by INIT

Case: $\mathcal{E} = \frac{}{\Sigma, a; \Gamma, \ulcorner D \urcorner \supset \mathbf{af}(K, a) \Rightarrow \mathbf{af}(K, a)}$ INIT

Since Γ is regular, it will not contain $\mathbf{af}(K, a)$ as an assumption. Thus, INIT cannot be applied and need not further consider this case.

Case: $\mathcal{D} = \frac{}{\Sigma; \ulcorner \Gamma \urcorner, \ulcorner \perp \urcorner \Rightarrow \ulcorner A \urcorner}$ \perp L

1. $\Gamma, \perp \Rightarrow A$ by \perp L

Case: $\mathcal{E} = \frac{}{\Sigma, a; \Gamma, \ulcorner \perp \urcorner, \ulcorner D \urcorner \supset \mathbf{af}(K, a) \Rightarrow \mathbf{af}(K, a)}$ \perp L

1. $\ulcorner \Gamma \urcorner, \perp \Rightarrow K$ affirms D by \perp L'

Case: \mathcal{D} ends with \forall R.

Subcase: $\mathcal{D} = \frac{\mathcal{D}_1}{\Sigma, a; \ulcorner \Gamma \urcorner \Rightarrow [a/x] \ulcorner C \urcorner}$ \forall R

No B exists such that $\ulcorner B \urcorner$ is equal to $\forall x. \ulcorner C \urcorner = \ulcorner \forall x. C \urcorner$. Thus, we need not further consider this case.

Subcase: $\mathcal{D} = \frac{\mathcal{D}_1}{\Sigma, a; \ulcorner \Gamma \urcorner \Rightarrow (\ulcorner C \urcorner \supset \mathbf{af}(K, a)) \supset \mathbf{af}(K, a)}$ \forall R

Note that $\ulcorner \langle K \rangle C \urcorner = \forall x. (\ulcorner C \urcorner \supset \mathbf{af}(K, x)) \supset \mathbf{af}(K, x)$. We know that $\Sigma, a; \ulcorner \Gamma \urcorner, \ulcorner C \urcorner \supset \mathbf{af}(K, a) \Rightarrow \mathbf{af}(K, a)$ has a derivation \mathcal{E}_1 by inversion on premise. Thus, $\Gamma \Rightarrow K$ affirms C by i.h. (ii) on \mathcal{E}_1 . This yields $\Gamma \Rightarrow \langle K \rangle C$ by $\langle \rangle$ R and since $\ulcorner \ulcorner \Gamma \urcorner \urcorner = \Gamma$.

Case: \mathcal{E} ends with \forall R. This cannot happen since $\mathbf{af}(K, a)$ does not have the form $\forall x. C$. We need not further consider this case.

Case: \mathcal{D} ends with \forall L.

$$\text{Subcase: } \mathcal{D} = \frac{\mathcal{D}_1}{\Sigma; \ulcorner \Gamma \urcorner, \forall x. \ulcorner C \urcorner, \ulcorner [t/x]C \urcorner \Rightarrow \ulcorner A \urcorner} \forall L$$

No B exists such that $\ulcorner B \urcorner$ is equal to $\forall x. \ulcorner C \urcorner = \ulcorner \forall x. C \urcorner$. Thus, we need not further consider this case.

$$\text{Subcase: } \mathcal{D} = \frac{\mathcal{D}_1}{\Sigma; \ulcorner \Gamma \urcorner, \ulcorner \langle K \rangle C \urcorner, (\ulcorner C \urcorner \supset \mathbf{af}(K, a)) \supset \mathbf{af}(K, a) \Rightarrow \ulcorner A \urcorner} \forall L$$

$\ulcorner \Gamma \urcorner, \ulcorner \langle K \rangle C \urcorner$ is pleasant. $(\ulcorner C \urcorner \supset \mathbf{af}(K, a)) \supset \mathbf{af}(K, a)$ is (K', t') -mean and $\ulcorner A \urcorner$ is (K', t') -nice for any $K' \neq K$ and $t' \neq a$. Thus, $\Sigma; \ulcorner \Gamma \urcorner, \ulcorner \langle K \rangle C \urcorner \Rightarrow \ulcorner A \urcorner$ has a derivation \mathcal{D}'_1 that is shorter than or equal to \mathcal{D}_1 in length by Lemma E.1. We may use i.h. (i) on \mathcal{D}'_1 to yield $\Gamma, \langle K \rangle C \Rightarrow A$.

Case: \mathcal{E} ends with $\forall L$.

$$\text{Subcase: } \mathcal{E} = \frac{\mathcal{E}_1}{\Sigma, a; \Gamma, \forall x. \ulcorner C \urcorner, \ulcorner [t/x]C \urcorner, \ulcorner D \urcorner \supset \mathbf{af}(K, a) \Rightarrow \mathbf{af}(K, a)} \forall L$$

$\forall x. \ulcorner C \urcorner$ cannot be in Γ since Γ is regular and no B exists such that $\ulcorner B \urcorner$ is equal to $\forall x. \ulcorner C \urcorner$. Thus, we need not further consider this case.

Subcase: \mathcal{E} is

$$\frac{\Sigma, a; \Gamma, \ulcorner \langle K' \rangle C \urcorner, (\ulcorner C \urcorner \supset \mathbf{af}(K', t')) \supset \mathbf{af}(K', t'), \ulcorner D \urcorner \supset \mathbf{af}(K, a) \Rightarrow \mathbf{af}(K, a)}{\Sigma, a; \Gamma, \ulcorner \langle K' \rangle C \urcorner, \ulcorner D \urcorner \supset \mathbf{af}(K, a) \Rightarrow \mathbf{af}(K, a)} \forall L$$

Now we consider the following cases:

Subsubcase $K' \neq K$ or $t' \neq a$.

$\Gamma, \ulcorner \langle K' \rangle C \urcorner, \ulcorner D \urcorner \supset \mathbf{af}(K, a)$ is pleasant since Γ is regular, $\mathbf{af}(K, a)$ is (K, a) -nice, and $(\ulcorner C \urcorner \supset \mathbf{af}(K', t')) \supset \mathbf{af}(K', t')$ is (K, a) -mean. Thus, $\Sigma, a; \Gamma, \ulcorner \langle K' \rangle C \urcorner, \ulcorner D \urcorner \supset \mathbf{af}(K, a) \Rightarrow \mathbf{af}(K, a)$ has a derivation \mathcal{E}'_1 that is shorter than or equal to \mathcal{E}_1 in length by Lemma E.1. By h.i. (ii) on \mathcal{E}'_1 , we prove $\ulcorner \Gamma, \ulcorner \langle K' \rangle C \urcorner \urcorner \Rightarrow K$ affirms D .

Subsubcase $K' = K$ and $t' = a$.

1. $\ulcorner \Gamma, \ulcorner \langle K \rangle C \urcorner, (\ulcorner C \urcorner \supset \mathbf{af}(K, a)) \supset \mathbf{af}(K, a) \urcorner \Rightarrow K$ affirms D

by i.h. (ii) on \mathcal{E}_1

2. $\ulcorner \Gamma \urcorner, \langle K \rangle C, \langle K \rangle C \Rightarrow K$ affirms D

by definitions of $\ulcorner \cdot \urcorner$ and $\ulcorner \cdot \urcorner$

3. $\ulcorner \Gamma \urcorner, \langle K \rangle C \Rightarrow K$ affirms D

by strengthening

$$\text{Case: } \mathcal{D} = \frac{\mathcal{D}_1}{\Sigma; \ulcorner \Gamma \urcorner, \ulcorner A \urcorner \Rightarrow \ulcorner B \urcorner} \supset R$$

1. $\Gamma, A \Rightarrow B$ by i.h. (i) on \mathcal{D}_1

2. $\Gamma \Rightarrow A \supset B$ by $\supset R$

Case: \mathcal{E} ends with $\supset R$. This cannot happen since $\mathbf{af}(K, a)$ is not an implication. We need not further consider this case.

$$\mathbf{Case: } \mathcal{D} = \frac{\Sigma; \ulcorner \Gamma \urcorner, \ulcorner B \urcorner \supset \ulcorner C \urcorner \Rightarrow \ulcorner B \urcorner \quad \Sigma; \ulcorner \Gamma \urcorner, \ulcorner B \urcorner \supset \ulcorner C \urcorner, \ulcorner C \urcorner \Rightarrow \ulcorner A \urcorner}{\Sigma; \ulcorner \Gamma \urcorner, \ulcorner B \urcorner \supset \ulcorner C \urcorner \Rightarrow \ulcorner A \urcorner} \supset L$$

1. $\Gamma, B \supset C \Rightarrow B$ by i.h. (i) on \mathcal{D}_1
2. $\Gamma, B \supset C, C \Rightarrow A$ by i.h. (i) on \mathcal{D}_2
3. $\Gamma, B \supset C \Rightarrow A$ by $\supset L$

Case: \mathcal{E} ends with $\supset L$.

$$\mathbf{Subcase: } \mathcal{E} = \frac{\mathcal{F}_1 \quad \mathcal{F}_2}{\Sigma, a; \Gamma, \ulcorner B \urcorner \supset \ulcorner C \urcorner, \ulcorner D \urcorner \supset \mathbf{af}(K, a) \Rightarrow \mathbf{af}(K, a)} \supset L$$

$$\text{where } \mathcal{F}_1 = \frac{\mathcal{D}_1}{\Sigma, a; \Gamma, \ulcorner B \urcorner \supset \ulcorner C \urcorner, \ulcorner D \urcorner \supset \mathbf{af}(K, a) \Rightarrow \ulcorner B \urcorner}$$

$$\text{and } \mathcal{F}_2 = \frac{\mathcal{E}_2}{\Sigma, a; \Gamma, \ulcorner B \urcorner \supset \ulcorner C \urcorner, \ulcorner C \urcorner, \ulcorner D \urcorner \supset \mathbf{af}(K, a) \Rightarrow \mathbf{af}(K, a)}$$

$\Gamma, \ulcorner B \urcorner \supset \ulcorner C \urcorner$ is pleasant since Γ is regular. For all $t \neq a$, $\ulcorner D \urcorner \supset \mathbf{af}(K, a)$ is (K, t) -mean and $\ulcorner B \urcorner$ is (K, t) -nice. By Lemma E.1 on \mathcal{D}_1 , there exists a derivation \mathcal{D}'_1 of $\Sigma, a; \Gamma, \ulcorner B \urcorner \supset \ulcorner C \urcorner \Rightarrow \ulcorner B \urcorner$ that has a length no greater than that of \mathcal{D}_1 .

Since no formula can contain every term t , every formula in $\Gamma \uparrow$ is (K, t) -mean for some t . Furthermore, $\ulcorner B \urcorner$ is (K, t) -nice for all t . Removing formulas from Γ will never result in Γ no longer being pleasant. Thus, we may use Lemma E.1 over and over again to remove every formula in $\Gamma \uparrow$ from the hypothesis context starting on \mathcal{D}'_1 . This results in a derivation \mathcal{D}''_1 of $\Sigma, a; \Gamma \downarrow, \ulcorner B \urcorner \supset \ulcorner C \urcorner \Rightarrow \ulcorner B \urcorner$ with a length no greater than that of \mathcal{D}'_1 . Since $\Gamma \downarrow$ has only formula of the form $\ulcorner E \urcorner$, we can use i.h. (i) on \mathcal{D}''_1 to prove that $\ulcorner \Gamma \downarrow \urcorner, B \supset C \Rightarrow B$.

By i.h. (ii) on \mathcal{E}_2 , $\ulcorner \Gamma \downarrow \urcorner, B \supset C, C \Rightarrow K$ affirms D . Combining $\ulcorner \Gamma \downarrow \urcorner, B \supset C \Rightarrow B$ and $\ulcorner \Gamma \downarrow \urcorner, B \supset C, C \Rightarrow K$ affirms D with $\supset L$ and weakening produces a proof of $\ulcorner \Gamma \downarrow \urcorner, B \supset C \Rightarrow K$ affirms D as needed.

Subcase: \mathcal{E} is

$$\frac{\Sigma, a; \Gamma, \ulcorner D \urcorner \supset \mathbf{af}(K, a) \Rightarrow \ulcorner D \urcorner \quad \Sigma, a; \Gamma, \ulcorner D \urcorner \supset \mathbf{af}(K, a), \mathbf{af}(K, a) \Rightarrow \mathbf{af}(K, a)}{\Sigma, a; \Gamma, \ulcorner D \urcorner \supset \mathbf{af}(K, a) \Rightarrow \mathbf{af}(K, a)} \supset L$$

Γ is pleasant since Γ is regular. For all $t \neq a$, $\ulcorner D \urcorner \supset \mathbf{af}(K, a)$ is (K, t) -mean and $\ulcorner B \urcorner$ is (K, t) -nice. By Lemma E.1 on \mathcal{D}_1 , there is a derivation \mathcal{D}'_1 of $\Sigma, a; \Gamma \Rightarrow \ulcorner D \urcorner$ with a length no greater than that of \mathcal{D}_1 . As above, we may apply Lemma E.1 over and over again to remove every formula of $\Gamma \uparrow$. This yields the derivation \mathcal{D}''_1 of $\Sigma, a; \Gamma \downarrow \Rightarrow \ulcorner D \urcorner$. By i.h. (i) on \mathcal{D}''_1 , $\ulcorner \Gamma \downarrow \urcorner \Rightarrow D$. Using the inference rule affirms and weakening yields $\ulcorner \Gamma \downarrow \urcorner \Rightarrow K$ affirms D as needed.

Subcase: $\mathcal{E} = \frac{\mathcal{F}_1 \quad \mathcal{F}_2}{\Sigma, a; \Gamma, (\ulcorner C \urcorner \supset \mathbf{af}(K, a)) \supset \mathbf{af}(K, a), \ulcorner D \urcorner \supset \mathbf{af}(K, a) \Rightarrow \mathbf{af}(K, a)} \supset L$ where \mathcal{F}_1 is the derivation

$$\Sigma, a; \Gamma, (\ulcorner C \urcorner \supset \mathbf{af}(K, a)) \supset \mathbf{af}(K, a), \ulcorner D \urcorner \supset \mathbf{af}(K, a) \Rightarrow \ulcorner C \urcorner \supset \mathbf{af}(K, a)$$

$$\begin{array}{c}
\frac{}{\Gamma, A \vdash A} \text{hyp} \qquad \frac{\Gamma, A \vdash B}{\Gamma \vdash A \supset B} \supset I \qquad \frac{\Gamma \vdash A \supset B \quad \Gamma \vdash A}{\Gamma \vdash B} \supset E \\
\\
\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B} \wedge I \qquad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A} \wedge E_1 \qquad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B} \wedge E_2 \\
\\
\frac{\Gamma \vdash A}{\Gamma \vdash A \vee B} \vee I_1 \qquad \frac{\Gamma \vdash B}{\Gamma \vdash A \vee B} \vee I_2 \qquad \frac{\Gamma \vdash A \vee B \quad \Gamma, A \vdash \gamma \quad \Gamma, B \vdash \gamma}{\Gamma \vdash \gamma} \vee E \\
\\
\frac{}{\Gamma \vdash \top} \top R \qquad \frac{}{\Gamma, \perp \vdash \gamma} \perp L \\
\\
\frac{\Gamma \vdash A}{\Gamma \vdash K \text{ affirms } A} \text{affirms} \qquad \frac{\Gamma \vdash K \text{ affirms } A}{\Gamma \vdash \langle K \rangle A} \langle \rangle I \qquad \frac{\Gamma \vdash \langle K \rangle A \quad \Gamma, A \vdash K \text{ affirms } C}{\Gamma \vdash K \text{ affirms } C} \langle \rangle E
\end{array}$$

Figure 3: Natural Deduction for INLL

and \mathcal{F}_2 is the derivation

$$\Sigma, a; \Gamma, (\ulcorner C \urcorner \supset \mathbf{af}(K, a)) \supset \mathbf{af}(K, a), \ulcorner D \urcorner \supset \mathbf{af}(K, a), \mathbf{af}(K, a) \Rightarrow \mathbf{af}(K, a) \quad \mathcal{E}_2$$

$\Sigma, a; \Gamma, (\ulcorner C \urcorner \supset \mathbf{af}(K, a)) \supset \mathbf{af}(K, a), \ulcorner D \urcorner \supset \mathbf{af}(K, a), \ulcorner C \urcorner \Rightarrow \mathbf{af}(K, a)$ has a derivation \mathcal{D}'_1 by inversion of the first premise. From i.h. (ii) on \mathcal{D}'_1 , we can prove that $\llcorner \Gamma, (\ulcorner C \urcorner \supset \mathbf{af}(K, a)) \supset \mathbf{af}(K, a), \ulcorner C \urcorner \llcorner \Rightarrow K \text{ affirms } D$. By the definitions of $\ulcorner \cdot \urcorner$ and $\llcorner \cdot \llcorner$, we get $\llcorner \Gamma \llcorner, \langle K \rangle C, C \Rightarrow K \text{ affirms } D$. $\langle \rangle L$ produces $\llcorner \Gamma \llcorner, \langle K \rangle C \Rightarrow K \text{ affirms } D$ as needed. □

F Proof of Completeness for Linear Translation

We first construct a natural deduction system for INLL. This is provably equivalent to the sequent calculus of Section A. The proof is relatively straightforward and we omit it here. The basic hypothetical judgments has the form $\Gamma \vdash \gamma$ where $\gamma = A$ or $\gamma = K \text{ affirms } A$. The system is shown in Figure 3.

Theorem F.1 (Equivalence). $\Gamma \vdash \gamma$ if and only if $\Gamma \Rightarrow \gamma$.

Proof. Straightforward extension of standard proofs. See for instance [How01]. □

Theorem F.2 (Completeness).

1. If $\Gamma \vdash A$ in INLL, then $\ulcorner \Gamma \urcorner; \cdot \Rightarrow \ulcorner A \urcorner$ in ILL.
2. If $\Gamma \vdash K \text{ affirms } A$ in INLL, then $\ulcorner \Gamma \urcorner; \ulcorner A \urcorner \supset \mathbf{af}(K) \Rightarrow \mathbf{af}(K)$ in ILL.

Proof. We perform a simultaneous induction on the given derivations, and analyze cases on the last rule.

Case: $\frac{}{\Gamma, A \vdash A} \text{hyp}$

To show: $\ulcorner \Gamma \urcorner, \ulcorner A \urcorner; \cdot \Rightarrow \ulcorner A \urcorner$.

1. $\ulcorner \Gamma \urcorner, \ulcorner A \urcorner; \ulcorner A \urcorner \Rightarrow \ulcorner A \urcorner$ by init
2. $\ulcorner \Gamma \urcorner, \ulcorner A \urcorner; \cdot \Rightarrow \ulcorner A \urcorner$ by copy on 1

Case: $\frac{\Gamma, A \vdash B}{\Gamma \vdash A \supset B} \supset I$

To show: $\ulcorner \Gamma \urcorner; \cdot \Rightarrow \ulcorner A \urcorner \supset \ulcorner B \urcorner$.

1. $\ulcorner \Gamma \urcorner, \ulcorner A \urcorner; \cdot \Rightarrow \ulcorner B \urcorner$ by i.h.
2. $\ulcorner \Gamma \urcorner; \cdot \Rightarrow \ulcorner A \urcorner \supset \ulcorner B \urcorner$ by Rule $\supset R$ on 1

Case: $\frac{\Gamma \vdash A \supset B \quad \Gamma \vdash A}{\Gamma \vdash B} \supset E$

To show: $\ulcorner \Gamma \urcorner; \cdot \Rightarrow \ulcorner B \urcorner$.

1. $\ulcorner \Gamma \urcorner; \cdot \Rightarrow \ulcorner A \urcorner \supset \ulcorner B \urcorner$ by i.h. premise 1
2. $\ulcorner \Gamma \urcorner; \cdot \Rightarrow \ulcorner A \urcorner$ by i.h. premise 2
3. $\ulcorner \Gamma \urcorner; \ulcorner B \urcorner \Rightarrow \ulcorner B \urcorner$ by Rule init
4. $\ulcorner \Gamma \urcorner; \ulcorner A \urcorner \supset \ulcorner B \urcorner \Rightarrow \ulcorner B \urcorner$ by Rule $\supset L$ on 2,3
5. $\ulcorner \Gamma \urcorner; \cdot \Rightarrow \ulcorner B \urcorner$ by Cut 1,4

Case: $\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B} \wedge I$

To show: $\ulcorner \Gamma \urcorner; \cdot \Rightarrow \ulcorner A \urcorner \& \ulcorner B \urcorner$.

1. $\ulcorner \Gamma \urcorner; \cdot \Rightarrow \ulcorner A \urcorner$ by i.h. premise 1
2. $\ulcorner \Gamma \urcorner; \cdot \Rightarrow \ulcorner B \urcorner$ by i.h. premise 2
3. $\ulcorner \Gamma \urcorner; \cdot \Rightarrow \ulcorner A \urcorner \& \ulcorner B \urcorner$ by Rule $\&R$ on 1,2

Case: $\frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A} \wedge E_1$

To show: $\ulcorner \Gamma \urcorner; \cdot \Rightarrow \ulcorner A \urcorner$.

1. $\ulcorner \Gamma \urcorner; \cdot \Rightarrow \ulcorner A \urcorner \& \ulcorner B \urcorner$ by i.h.
2. $\ulcorner \Gamma \urcorner; \ulcorner A \urcorner \Rightarrow \ulcorner A \urcorner$ by Rule init
3. $\ulcorner \Gamma \urcorner; \ulcorner A \urcorner \& \ulcorner B \urcorner \Rightarrow \ulcorner A \urcorner$ by Rule $\&L_1$ on 2
4. $\ulcorner \Gamma \urcorner; \cdot \Rightarrow \ulcorner A \urcorner$ by Cut 1,3

Case: $\frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B} \wedge E_2$

To show: $\ulcorner \Gamma \urcorner; \cdot \Rightarrow \ulcorner B \urcorner$.

Similar to previous case.

$$\text{Case: } \frac{\Gamma \vdash A}{\Gamma \vdash A \vee B} \vee I_1$$

To show: $\ulcorner \Gamma \urcorner; \cdot \Rightarrow (!\ulcorner A \urcorner) \oplus (!\ulcorner B \urcorner)$.

1. $\ulcorner \Gamma \urcorner; \cdot \Rightarrow \ulcorner A \urcorner$ by i.h.
2. $\ulcorner \Gamma \urcorner; \cdot \Rightarrow !\ulcorner A \urcorner$ by Rule $!R$ on 1
3. $\ulcorner \Gamma \urcorner; \cdot \Rightarrow (!\ulcorner A \urcorner) \oplus (!\ulcorner B \urcorner)$ by Rule $\oplus R_1$ on 2

$$\text{Case: } \frac{\Gamma \vdash B}{\Gamma \vdash A \vee B} \vee I_2$$

To show: $\ulcorner \Gamma \urcorner; \cdot \Rightarrow (!\ulcorner A \urcorner) \oplus (!\ulcorner B \urcorner)$.

Similar to previous case.

$$\text{Case: } \frac{\Gamma \vdash A \vee B \quad \Gamma, A \vdash C \quad \Gamma, B \vdash C}{\Gamma \vdash C} \vee E$$

To show: $\ulcorner \Gamma \urcorner; \cdot \Rightarrow \ulcorner C \urcorner$.

1. $\ulcorner \Gamma \urcorner, \ulcorner A \urcorner; \cdot \Rightarrow \ulcorner C \urcorner$ by i.h. premise 2
2. $\ulcorner \Gamma \urcorner; !\ulcorner A \urcorner \Rightarrow \ulcorner C \urcorner$ by Rule $!L$ on 1
3. $\ulcorner \Gamma \urcorner, \ulcorner B \urcorner; \cdot \Rightarrow \ulcorner C \urcorner$ by i.h. premise 3
4. $\ulcorner \Gamma \urcorner; !\ulcorner B \urcorner \Rightarrow \ulcorner C \urcorner$ by Rule $!L$ on 3
5. $\ulcorner \Gamma \urcorner; (!\ulcorner A \urcorner) \oplus (!\ulcorner B \urcorner) \Rightarrow \ulcorner C \urcorner$ by Rule $\oplus L$ on 2,4
6. $\ulcorner \Gamma \urcorner; \cdot \Rightarrow (!\ulcorner A \urcorner) \oplus (!\ulcorner B \urcorner)$ by i.h. premise 1
7. $\ulcorner \Gamma \urcorner; \cdot \Rightarrow \ulcorner C \urcorner$ by Cut 6,5

$$\text{Case: } \frac{\Gamma \vdash A \vee B \quad \Gamma, A \vdash K \text{ affirms } C \quad \Gamma, B \vdash K \text{ affirms } C}{\Gamma \vdash K \text{ affirms } C} \vee E$$

To show: $\ulcorner \Gamma \urcorner; \ulcorner C \urcorner \supset \mathbf{af}(K) \Rightarrow \mathbf{af}(K)$.

1. $\ulcorner \Gamma \urcorner, \ulcorner A \urcorner; \ulcorner C \urcorner \supset \mathbf{af}(K) \Rightarrow \mathbf{af}(K)$ by i.h. premise 2
2. $\ulcorner \Gamma \urcorner; !\ulcorner A \urcorner, \ulcorner C \urcorner \supset \mathbf{af}(K) \Rightarrow \mathbf{af}(K)$ by Rule $!L$ on 1
3. $\ulcorner \Gamma \urcorner, \ulcorner B \urcorner; \ulcorner C \urcorner \supset \mathbf{af}(K) \Rightarrow \mathbf{af}(K)$ by i.h. premise 3
4. $\ulcorner \Gamma \urcorner; !\ulcorner B \urcorner, \ulcorner C \urcorner \supset \mathbf{af}(K) \Rightarrow \mathbf{af}(K)$ by Rule $!L$ on 3
5. $\ulcorner \Gamma \urcorner; (!\ulcorner A \urcorner) \oplus (!\ulcorner B \urcorner), \ulcorner C \urcorner \supset \mathbf{af}(K) \Rightarrow \mathbf{af}(K)$ by Rule $\oplus L$ on 2,4
6. $\ulcorner \Gamma \urcorner; \cdot \Rightarrow (!\ulcorner A \urcorner) \oplus (!\ulcorner B \urcorner)$ by i.h. premise 1
7. $\ulcorner \Gamma \urcorner; \ulcorner C \urcorner \supset \mathbf{af}(K) \Rightarrow \mathbf{af}(K)$ by Cut 6,5

$$\text{Case: } \frac{}{\Gamma \vdash \top} \top R$$

To show: $\ulcorner \Gamma \urcorner; \cdot \Rightarrow \top$.

Follows immediately by rule $\top R$.

$$\text{Case: } \frac{}{\Gamma, \perp \vdash C} \perp L$$

To show: $\ulcorner \Gamma \urcorner, \mathbf{0}; \cdot \Rightarrow \ulcorner C \urcorner$.

1. $\ulcorner \Gamma \urcorner, \mathbf{0}; \cdot \Rightarrow \ulcorner C \urcorner$ by Rule $\mathbf{0}L$
2. $\ulcorner \Gamma \urcorner, \mathbf{0}; \cdot \Rightarrow \ulcorner C \urcorner$ by Rule copy on 1

Case: $\frac{}{\Gamma, \perp \vdash K \text{ affirms } C} \perp L$

To show: $\ulcorner \Gamma \urcorner, \mathbf{0}; \ulcorner C \urcorner \supset \mathbf{af}(K) \Rightarrow \mathbf{af}(K)$.

1. $\ulcorner \Gamma \urcorner, \mathbf{0}; \mathbf{0}, \ulcorner C \urcorner \supset \mathbf{af}(K) \Rightarrow \mathbf{af}(K)$ by Rule $\mathbf{0}L$
2. $\ulcorner \Gamma \urcorner, \mathbf{0}; \ulcorner C \urcorner \supset \mathbf{af}(K) \Rightarrow \mathbf{af}(K)$ by Rule copy on 1

Case: $\frac{\Gamma \vdash A}{\Gamma \vdash K \text{ affirms } A} \text{affirms}$

To show: $\ulcorner \Gamma \urcorner; \ulcorner A \urcorner \supset \mathbf{af}(K) \Rightarrow \mathbf{af}(K)$.

1. $\ulcorner \Gamma \urcorner; \cdot \Rightarrow \ulcorner A \urcorner$ by i.h.
2. $\ulcorner \Gamma \urcorner; \mathbf{af}(K) \Rightarrow \mathbf{af}(K)$ by Rule init
3. $\ulcorner \Gamma \urcorner; \ulcorner A \urcorner \supset \mathbf{af}(K) \Rightarrow \mathbf{af}(K)$ by Rule $\supset L$

Case: $\frac{\Gamma \vdash K \text{ affirms } A}{\Gamma \vdash \langle K \rangle A} \langle \rangle I$

To show: $\ulcorner \Gamma \urcorner; \cdot \Rightarrow (\ulcorner A \urcorner \supset \mathbf{af}(K)) \multimap \mathbf{af}(K)$.

1. $\ulcorner \Gamma \urcorner; \ulcorner A \urcorner \supset \mathbf{af}(K) \Rightarrow \mathbf{af}(K)$ by i.h.
2. $\ulcorner \Gamma \urcorner; \cdot \Rightarrow (\ulcorner A \urcorner \supset \mathbf{af}(K)) \multimap \mathbf{af}(K)$ by Rule $\multimap R$ on 1

Case: $\frac{\Gamma \vdash \langle K \rangle A \quad \Gamma, A \vdash K \text{ affirms } C}{\Gamma \vdash K \text{ affirms } C} \langle \rangle E$

To show: $\ulcorner \Gamma \urcorner; \ulcorner C \urcorner \supset \mathbf{af}(K) \Rightarrow \mathbf{af}(K)$.

1. $\ulcorner \Gamma \urcorner, \ulcorner A \urcorner; \ulcorner C \urcorner \supset \mathbf{af}(K) \Rightarrow \mathbf{af}(K)$ by i.h. premise 2
2. $\ulcorner \Gamma \urcorner; \ulcorner C \urcorner \supset \mathbf{af}(K) \Rightarrow \ulcorner A \urcorner \supset \mathbf{af}(K)$ by Rule $\supset R$ on 1
3. $\ulcorner \Gamma \urcorner; \mathbf{af}(K) \Rightarrow \mathbf{af}(K)$ by Rule init
4. $\ulcorner \Gamma \urcorner; (\ulcorner A \urcorner \supset \mathbf{af}(K)) \multimap \mathbf{af}(K), \ulcorner C \urcorner \supset \mathbf{af}(K) \Rightarrow \mathbf{af}(K)$ by Rule $\multimap L$ on 2,3
5. $\ulcorner \Gamma \urcorner; \cdot \Rightarrow (\ulcorner A \urcorner \supset \mathbf{af}(K)) \multimap \mathbf{af}(K)$ by i.h. premise 1
6. $\ulcorner \Gamma \urcorner; \ulcorner C \urcorner \supset \mathbf{af}(K) \Rightarrow \mathbf{af}(K)$ by Cut 5,4

□

Proof of theorem 4.1.

1. Suppose $\Gamma \Rightarrow A$. By theorem F.1, $\Gamma \vdash A$. Hence by theorem F.2, $\ulcorner \Gamma \urcorner; \cdot \Rightarrow \ulcorner A \urcorner$.
2. Suppose $\Gamma \Rightarrow K \text{ affirms } A$. By theorem F.1, $\Gamma \vdash K \text{ affirms } A$. Hence by theorem F.2, $\ulcorner \Gamma \urcorner; \ulcorner A \urcorner \supset \mathbf{af}(K) \Rightarrow \mathbf{af}(K)$.

□

G Proof of Soundness for Linear Translation

To prove soundness, we need some basic properties of proofs in INLL and ILL. We mention these properties below. The proofs of these properties are straightforward.

Lemma G.1 (Structural Properties of INLL Proofs). *The following hold in INLL.*

1. (Weakening) If $\Gamma \Rightarrow \gamma$, then $\Gamma, A \Rightarrow \gamma$.
2. (Strengthening) If $\Gamma, A, A \Rightarrow \gamma$, then $\Gamma, A \Rightarrow \gamma$.

Proof. Both properties follow by a straightforward induction on the given derivations. \square

Lemma G.2 (Inversion in ILL). *The following hold in ILL.*

1. If $\Gamma; \Delta, !A \Rightarrow B$, then $\Gamma, A; \Delta \Rightarrow B$ by a shorter or equal derivation.
2. If $\Gamma; \Delta \Rightarrow A \supset B$, then $\Gamma, A; \Delta \Rightarrow B$ by a shorter or equal derivation.

Proof. Both properties follow by a straightforward induction on the given derivations. \square

Finally, we prove soundness. We have to generalize the statement of the theorem to facilitate induction.

Theorem G.3 (Soundness). *Let $\psi = \{\mathbf{af}(K_1), \dots, \mathbf{af}(K_n)\}$ be a multi-set of assumptions for some $n \geq 0$. The following hold:*

1. If $\ulcorner \Gamma \urcorner; \ulcorner \Delta \urcorner, \psi \Rightarrow \ulcorner A \urcorner$, then $\Gamma, \Delta \Rightarrow A$.
2. If $\ulcorner \Gamma \urcorner; \ulcorner \Delta \urcorner, \psi \Rightarrow \ulcorner !A \urcorner$, then $\Gamma, \Delta \Rightarrow A$.
3. If $\ulcorner \Gamma \urcorner; \ulcorner \Delta \urcorner, \ulcorner A \urcorner \supset \mathbf{af}(K), \psi \Rightarrow \mathbf{af}(K)$ and $\mathbf{af}(K) \notin \psi$, then $\Gamma, \Delta \Rightarrow K$ affirms A .
4. If $\ulcorner \Gamma \urcorner; \ulcorner \Delta \urcorner, \psi \Rightarrow \mathbf{af}(K)$ and $\mathbf{af}(K) \notin \psi$, then $\Gamma, \Delta \Rightarrow K$ affirms \perp .

Proof. We prove this theorem by a simultaneous induction on the *depth* of the given derivations.

Proof of statement (1)

Case: $\frac{}{\ulcorner \Gamma \urcorner, \ulcorner P \urcorner \Rightarrow \ulcorner P \urcorner}$ init

To show: $\Gamma, P \Rightarrow P$.

This follows immediately by rule init.

Case: $\frac{\ulcorner \Gamma \urcorner, \ulcorner A \urcorner; \ulcorner \Delta \urcorner, \ulcorner A \urcorner, \psi \Rightarrow \ulcorner B \urcorner}{\ulcorner \Gamma \urcorner, \ulcorner A \urcorner; \ulcorner \Delta \urcorner, \psi \Rightarrow \ulcorner B \urcorner}$ copy

To show: $\Gamma, A, \Delta \Rightarrow B$.

1. $\Gamma, A, \Delta, A \Rightarrow B$ by i.h.
2. $\Gamma, A, \Delta \Rightarrow B$ by Strengthening on 1

Case: $\frac{\ulcorner \Gamma \urcorner; \ulcorner \Delta \urcorner, \psi \Rightarrow \ulcorner A \urcorner \quad \ulcorner \Gamma \urcorner; \ulcorner \Delta \urcorner, \psi \Rightarrow \ulcorner B \urcorner}{\ulcorner \Gamma \urcorner; \ulcorner \Delta \urcorner, \psi \Rightarrow \ulcorner A \urcorner \& \ulcorner B \urcorner}$ &R

To show: $\Gamma, \Delta \Rightarrow A \wedge B$.

1. $\Gamma, \Delta \Rightarrow A$ by i.h. premise 1
2. $\Gamma, \Delta \Rightarrow B$ by i.h. premise 2
3. $\Gamma, \Delta \Rightarrow A \wedge B$ by Rule $\wedge R$ on 1,2

$$\text{Case: } \frac{\ulcorner \Gamma^\neg; \ulcorner \Delta^\neg, \ulcorner A^\neg, \psi \Rightarrow \ulcorner C^\neg}{\ulcorner \Gamma^\neg; \ulcorner \Delta^\neg, \ulcorner A^\neg \& \ulcorner B^\neg, \psi \Rightarrow \ulcorner C^\neg} \&L_1$$

To show: $\Gamma, \Delta, A \wedge B \Rightarrow C$.

1. $\Gamma, \Delta, A \Rightarrow C$ by i.h.
2. $\Gamma, \Delta, A \wedge B \Rightarrow C$ by Rule $\wedge L_1$ on 1

$$\text{Case: } \frac{\ulcorner \Gamma^\neg; \ulcorner \Delta^\neg, \ulcorner B^\neg, \psi \Rightarrow \ulcorner C^\neg}{\ulcorner \Gamma^\neg; \ulcorner \Delta^\neg, \ulcorner A^\neg \& \ulcorner B^\neg, \psi \Rightarrow \ulcorner C^\neg} \&L_2$$

To show: $\Gamma, \Delta, A \wedge B \Rightarrow C$.

Similar to previous case.

$$\text{Case: } \frac{\ulcorner \Gamma^\neg; \ulcorner \Delta^\neg, \psi \Rightarrow !\ulcorner A^\neg}{\ulcorner \Gamma^\neg; \ulcorner \Delta^\neg, \psi \Rightarrow (!\ulcorner A^\neg) \oplus (!\ulcorner B^\neg)} \oplus R_1$$

To show: $\Gamma, \Delta \Rightarrow A \vee B$.

1. $\Gamma, \Delta \Rightarrow A$ by i.h.
2. $\Gamma, \Delta \Rightarrow A \vee B$ by Rule $\vee R_1$

$$\text{Case: } \frac{\ulcorner \Gamma^\neg; \ulcorner \Delta^\neg, \psi \Rightarrow !\ulcorner B^\neg}{\ulcorner \Gamma^\neg; \ulcorner \Delta^\neg, \psi \Rightarrow (!\ulcorner A^\neg) \oplus (!\ulcorner B^\neg)} \oplus R_2$$

To show: $\Gamma, \Delta \Rightarrow A \vee B$.

Similar to previous case.

$$\text{Case: } \frac{\ulcorner \Gamma^\neg; !\ulcorner A^\neg, \ulcorner \Delta^\neg, \psi \Rightarrow \ulcorner C^\neg \quad \ulcorner \Gamma^\neg; !\ulcorner B^\neg, \ulcorner \Delta^\neg, \psi \Rightarrow \ulcorner C^\neg}{\ulcorner \Gamma^\neg; (!\ulcorner A^\neg) \oplus (!\ulcorner B^\neg), \ulcorner \Delta^\neg, \psi \Rightarrow \ulcorner C^\neg} \oplus L$$

To show: $\Gamma, A \vee B, \Delta \Rightarrow C$.

1. $\ulcorner \Gamma^\neg, \ulcorner A^\neg; \ulcorner \Delta^\neg, \psi \Rightarrow \ulcorner C^\neg$ by Inversion premise 1
2. $\ulcorner \Gamma^\neg, \ulcorner B^\neg; \ulcorner \Delta^\neg, \psi \Rightarrow \ulcorner C^\neg$ by Inversion premise 2
3. $\Gamma, A, \Delta \Rightarrow C$ by i.h. on 1
4. $\Gamma, B, \Delta \Rightarrow C$ by i.h. on 2
5. $\Gamma, A \vee B, \Delta \Rightarrow C$ by Rule $\vee L$ on 3,4

$$\text{Case: } \frac{}{\ulcorner \Gamma^\neg; \ulcorner \Delta^\neg, \psi \Rightarrow \top} \top R$$

To show: $\Gamma, \Delta \Rightarrow \top$.

Follows immediately by rule $\top R$.

$$\text{Case: } \frac{}{\ulcorner \Gamma^\neg; \ulcorner \Delta^\neg, \mathbf{0}, \psi \Rightarrow \ulcorner A^\neg} \mathbf{0}L$$

To show: $\Gamma, \Delta, \perp \Rightarrow A$.

Follows immediately by rule $\perp L$.

$$\text{Case: } \frac{\ulcorner \Gamma^\neg; \ulcorner \Delta^\neg, \psi, \ulcorner A^\neg \supset \mathbf{af}(K) \Rightarrow \mathbf{af}(K)}{\ulcorner \Gamma^\neg; \ulcorner \Delta^\neg, \psi \Rightarrow (\ulcorner A^\neg \supset \mathbf{af}(K)) \multimap \mathbf{af}(K)} \multimap R$$

To show: $\Gamma, \Delta \Rightarrow \langle K \rangle A$.

1. $\Gamma, \Delta \Rightarrow K$ *affirms* A by i.h.
2. $\Gamma, \Delta \Rightarrow \langle K \rangle A$ by Rule $\langle \rangle R$ on 1

$$\text{Case: } \frac{\frac{\ulcorner \Gamma \urcorner; \ulcorner \Delta_1 \urcorner, \psi_1 \Rightarrow \ulcorner A \urcorner \supset \mathbf{af}(K) \quad \ulcorner \Gamma \urcorner; \ulcorner \Delta_2 \urcorner, \psi_2, \mathbf{af}(K) \Rightarrow \ulcorner C \urcorner}{\ulcorner \Gamma \urcorner; \ulcorner \Delta_1 \urcorner, \ulcorner \Delta_2 \urcorner, \psi_1, \psi_2, (\ulcorner A \urcorner \supset \mathbf{af}(K)) \multimap \mathbf{af}(K) \Rightarrow \ulcorner C \urcorner} \multimap L}{\ulcorner \Gamma \urcorner; \ulcorner \Delta \urcorner, \psi \Rightarrow \ulcorner B \urcorner} \supset R$$

To show: $\Gamma, \Delta_1, \Delta_2, \langle K \rangle A \Rightarrow C$.

1. $\Gamma, \Delta_2 \Rightarrow C$ by i.h. premise 2
2. $\Gamma, \Delta_1, \Delta_2, \langle K \rangle A \Rightarrow C$ by Weakening on 1

$$\text{Case: } \frac{\ulcorner \Gamma \urcorner, \ulcorner A \urcorner; \ulcorner \Delta \urcorner, \psi \Rightarrow \ulcorner B \urcorner}{\ulcorner \Gamma \urcorner; \ulcorner \Delta \urcorner, \psi \Rightarrow \ulcorner A \urcorner \supset \ulcorner B \urcorner} \supset R$$

To show: $\Gamma, \Delta \Rightarrow A \supset B$.

1. $\Gamma, A, \Delta \Rightarrow B$ by i.h.
2. $\Gamma, \Delta \Rightarrow A \supset B$ by Rule $\supset R$ on 1

$$\text{Case: } \frac{\ulcorner \Gamma \urcorner; \cdot \Rightarrow \ulcorner A \urcorner \quad \ulcorner \Gamma \urcorner; \ulcorner \Delta \urcorner, \ulcorner B \urcorner, \psi \Rightarrow \ulcorner C \urcorner}{\ulcorner \Gamma \urcorner; \ulcorner \Delta \urcorner, \ulcorner A \urcorner \supset \ulcorner B \urcorner, \psi \Rightarrow \ulcorner C \urcorner} \supset L$$

To show: $\Gamma, \Delta, A \supset B \Rightarrow C$.

1. $\Gamma \Rightarrow A$ by i.h. premise 1
2. $\Gamma, \Delta, B \Rightarrow C$ by i.h. premise 2
3. $\Gamma, \Delta, A \supset B \Rightarrow C$ by Rule $\supset L$ on 1,2

Other cases do not apply.

Proof of statement (2)

$$\text{Case: } \frac{\ulcorner \Gamma \urcorner, \ulcorner A \urcorner; \ulcorner \Delta \urcorner, \ulcorner A \urcorner, \psi \Rightarrow \ulcorner B \urcorner}{\ulcorner \Gamma \urcorner, \ulcorner A \urcorner; \ulcorner \Delta \urcorner, \psi \Rightarrow \ulcorner B \urcorner} \text{copy}$$

To show: $\Gamma, A, \Delta \Rightarrow B$.

1. $\Gamma, A, \Delta, A \Rightarrow B$ by i.h.
2. $\Gamma, A, \Delta \Rightarrow B$ by Strengthening on 1

$$\text{Case: } \frac{\ulcorner \Gamma \urcorner; \ulcorner \Delta \urcorner, \ulcorner A \urcorner, \psi \Rightarrow \ulcorner C \urcorner}{\ulcorner \Gamma \urcorner; \ulcorner \Delta \urcorner, \ulcorner A \urcorner \& \ulcorner B \urcorner, \psi \Rightarrow \ulcorner C \urcorner} \&L_1$$

To show: $\Gamma, \Delta, A \wedge B \Rightarrow C$.

1. $\Gamma, \Delta, A \Rightarrow C$ by i.h.
2. $\Gamma, \Delta, A \wedge B \Rightarrow C$ by Rule $\wedge L_1$ on 1

$$\text{Case: } \frac{\ulcorner \Gamma \urcorner; \ulcorner \Delta \urcorner, \ulcorner B \urcorner, \psi \Rightarrow \ulcorner C \urcorner}{\ulcorner \Gamma \urcorner; \ulcorner \Delta \urcorner, \ulcorner A \urcorner \& \ulcorner B \urcorner, \psi \Rightarrow \ulcorner C \urcorner} \&L_2$$

To show: $\Gamma, \Delta, A \wedge B \Rightarrow C$.

Similar to previous case.

$$\text{Case: } \frac{\frac{\frac{\Gamma; !A, \Delta, \psi \Rightarrow !C}{\Gamma; (!A), \Delta, \psi \Rightarrow !C} \oplus L \quad \Gamma; !B, \Delta, \psi \Rightarrow !C}{\Gamma; (!A) \oplus (!B), \Delta, \psi \Rightarrow !C} \oplus L$$

To show: $\Gamma, A \vee B, \Delta \Rightarrow C$.

1. $\Gamma, A, \Delta, \psi \Rightarrow !C$ by Inversion premise 1
2. $\Gamma, B, \Delta, \psi \Rightarrow !C$ by Inversion premise 2
3. $\Gamma, A, \Delta \Rightarrow C$ by i.h. on 1
4. $\Gamma, B, \Delta \Rightarrow C$ by i.h. on 2
5. $\Gamma, A \vee B, \Delta \Rightarrow C$ by Rule $\vee L$ on 3,4

$$\text{Case: } \frac{}{\Gamma, \Delta, \perp, \psi \Rightarrow !A} \mathbf{0}L$$

To show: $\Gamma, \Delta, \perp \Rightarrow A$.

Follows immediately by rule $\perp L$.

$$\text{Case: } \frac{\frac{\frac{\Gamma; \Delta_1, \psi_1 \Rightarrow A \supset \mathbf{af}(K) \quad \Gamma; \Delta_2, \psi_2, \mathbf{af}(K) \Rightarrow !C}{\Gamma; \Delta_1, \Delta_2, \psi_1, \psi_2, (A \supset \mathbf{af}(K)) \multimap \mathbf{af}(K) \Rightarrow !C} \multimap L \quad \Gamma; \Delta_1, \psi_1 \Rightarrow A \supset \mathbf{af}(K)}}{\Gamma; \Delta_1, \Delta_2, \langle K \rangle A \Rightarrow C} \multimap L$$

To show: $\Gamma, \Delta_1, \Delta_2, \langle K \rangle A \Rightarrow C$.

1. $\Gamma, \Delta_2 \Rightarrow C$ by i.h. premise 2
2. $\Gamma, \Delta_1, \Delta_2, \langle K \rangle A \Rightarrow C$ by Weakening on 1

$$\text{Case: } \frac{\frac{\Gamma; \cdot \Rightarrow A \quad \Gamma; \Delta, B, \psi \Rightarrow !C}{\Gamma; \Delta, A \supset B \Rightarrow !C} \supset L \quad \Gamma; \Delta, A \supset B \Rightarrow !C}{\Gamma, \Delta, A \supset B \Rightarrow C} \supset L$$

To show: $\Gamma, \Delta, A \supset B \Rightarrow C$.

1. $\Gamma \Rightarrow A$ by i.h. premise 1
2. $\Gamma, \Delta, B \Rightarrow C$ by i.h. premise 2
3. $\Gamma, \Delta, A \supset B \Rightarrow C$ by Rule $\supset L$ on 1,2

$$\text{Case: } \frac{\Gamma; \cdot \Rightarrow A}{\Gamma; \cdot \Rightarrow !A} !R$$

To show: $\Gamma \Rightarrow A$.

Follows immediately by i.h. on premise.

Other cases do not apply.

Proof of statement (3)

Case: Rule *init* does not apply since the consequent $\mathbf{af}(K)$ cannot occur in Γ, Δ (by definition) or ψ (by assumption).

$$\text{Case: } \frac{\frac{\Gamma, A, \Delta, A \Rightarrow K \text{ affirms } B \quad \Gamma, \Delta, A \Rightarrow K \text{ affirms } B}{\Gamma, A, \Delta \Rightarrow K \text{ affirms } B} \text{copy} \quad \Gamma, A, \Delta, A \Rightarrow K \text{ affirms } B}{\Gamma, A, \Delta \Rightarrow K \text{ affirms } B} \text{copy}$$

To show: $\Gamma, A, \Delta \Rightarrow K \text{ affirms } B$.

1. $\Gamma, A, \Delta, A \Rightarrow K \text{ affirms } B$ by i.h.
2. $\Gamma, A, \Delta \Rightarrow K \text{ affirms } B$ by Strengthening on 1

$$\text{Case: } \frac{\ulcorner \Gamma^\top; \ulcorner \Delta^\top, \ulcorner A^\top, \ulcorner C^\top \supset \mathbf{af}(K), \psi \Rightarrow \mathbf{af}(K)}{\ulcorner \Gamma^\top; \ulcorner \Delta^\top, \ulcorner A^\top \& \ulcorner B^\top, \ulcorner C^\top \supset \mathbf{af}(K), \psi \Rightarrow \mathbf{af}(K)} \&L_1$$

To show: $\Gamma, \Delta, A \wedge B \Rightarrow K$ affirms C .

1. $\Gamma, \Delta, A \Rightarrow K$ affirms C by i.h.
2. $\Gamma, \Delta, A \wedge B \Rightarrow K$ affirms C by Rule $\wedge L'_1$ on 1

$$\text{Case: } \frac{\ulcorner \Gamma^\top; \ulcorner \Delta^\top, \ulcorner B^\top, \ulcorner C^\top \supset \mathbf{af}(K), \psi \Rightarrow \mathbf{af}(K)}{\ulcorner \Gamma^\top; \ulcorner \Delta^\top, \ulcorner A^\top \& \ulcorner B^\top, \ulcorner C^\top \supset \mathbf{af}(K), \psi \Rightarrow \mathbf{af}(K)} \&L_2$$

To show: $\Gamma, \Delta, A \wedge B \Rightarrow K$ affirms C .

Similar to previous case.

$$\text{Case: } \frac{\ulcorner \Gamma^\top; !\ulcorner A^\top, \ulcorner \Delta^\top, \ulcorner C^\top \supset \mathbf{af}(K), \psi \Rightarrow \mathbf{af}(K) \quad \ulcorner \Gamma^\top; !\ulcorner B^\top, \ulcorner \Delta^\top, \ulcorner C^\top \supset \mathbf{af}(K), \psi \Rightarrow \mathbf{af}(K)}{\ulcorner \Gamma^\top; (!\ulcorner A^\top) \oplus (!\ulcorner B^\top), \ulcorner \Delta^\top, \ulcorner C^\top \supset \mathbf{af}(K), \psi \Rightarrow \mathbf{af}(K)} \oplus L$$

To show: $\Gamma, A \vee B, \Delta \Rightarrow K$ affirms C .

1. $\ulcorner \Gamma^\top, \ulcorner A^\top; \ulcorner \Delta^\top, \ulcorner C^\top \supset \mathbf{af}(K), \psi \Rightarrow \mathbf{af}(K)$ by Inversion premise 1
2. $\ulcorner \Gamma^\top, \ulcorner B^\top; \ulcorner \Delta^\top, \ulcorner C^\top \supset \mathbf{af}(K), \psi \Rightarrow \mathbf{af}(K)$ by Inversion premise 2
3. $\Gamma, A, \Delta \Rightarrow K$ affirms C by i.h. on 1
4. $\Gamma, B, \Delta \Rightarrow K$ affirms C by i.h. on 2
5. $\Gamma, A \vee B, \Delta \Rightarrow K$ affirms C by Rule $\vee L'$ on 3,4

$$\text{Case: } \frac{}{\ulcorner \Gamma^\top; \ulcorner \Delta^\top, \mathbf{0}, \ulcorner A^\top \supset \mathbf{af}(K), \psi \Rightarrow \mathbf{af}(K)} \mathbf{0}L$$

To show: $\Gamma, \Delta, \perp \Rightarrow K$ affirms A .

Follows immediately by rule $\perp L'$.

$$\text{Case: } \frac{\ulcorner \Gamma^\top; \ulcorner \Delta_1^\top, \psi_1 \Rightarrow \ulcorner C^\top \supset \mathbf{af}(K') \quad \ulcorner \Gamma^\top; \ulcorner \Delta_2^\top, \ulcorner A^\top \supset \mathbf{af}(K), \psi_2, \mathbf{af}(K') \Rightarrow \mathbf{af}(K)}{\ulcorner \Gamma^\top; \ulcorner \Delta_1^\top, \ulcorner \Delta_2^\top, \psi_1, \psi_2, \ulcorner \langle K' \rangle C^\top, \ulcorner A^\top \supset \mathbf{af}(K) \Rightarrow \mathbf{af}(K)} \multimap L$$

To show: $\Gamma, \Delta_1, \Delta_2, \langle K' \rangle C \Rightarrow K$ affirms A .

We have two possibilities: either $K = K'$ or $K \neq K'$.

Subcase: $K = K'$

1. $\ulcorner \Gamma^\top, \ulcorner C^\top; \ulcorner \Delta_1^\top, \psi_1 \Rightarrow \mathbf{af}(K)$ by Inversion premise 1
2. $\Gamma, \Delta_1, C \Rightarrow K$ affirms \perp by i.h. on 1
3. $\Gamma, \Delta_1, \Delta_2, \langle K \rangle C \Rightarrow K$ affirms C by Reasoning in INLL
4. $\Gamma, \Delta_1, \Delta_2, \langle K \rangle C \Rightarrow K$ affirms \perp by Theorem 2.1 on 3,2
5. $\perp \Rightarrow K$ affirms A by Rule $\perp L'$
6. $\Gamma, \Delta_1, \Delta_2, \langle K \rangle C \Rightarrow K$ affirms A by Theorem 2.1 on 4,5

Subcase: $K \neq K'$

1. $\Gamma, \Delta_2 \Rightarrow K$ affirms A by i.h. premise 2
2. $\Gamma, \Delta_1, \Delta_2, \langle K' \rangle C \Rightarrow K$ affirms A by Weakening on 1

$$\text{Case: } \frac{\ulcorner \Gamma^\top; \ulcorner \Delta_1^\top, \psi_1, \ulcorner A^\top \supset \mathbf{af}(K) \Rightarrow \ulcorner C^\top \supset \mathbf{af}(K') \quad \ulcorner \Gamma^\top; \ulcorner \Delta_2^\top, \psi_2, \mathbf{af}(K') \Rightarrow \mathbf{af}(K)}{\ulcorner \Gamma^\top; \ulcorner \Delta_1^\top, \ulcorner \Delta_2^\top, \psi_1, \psi_2, \ulcorner \langle K' \rangle C^\top, \ulcorner A^\top \supset \mathbf{af}(K) \Rightarrow \mathbf{af}(K)} \multimap L$$

To show: $\Gamma, \Delta_1, \Delta_2, \langle K' \rangle C \Rightarrow K$ affirms A .

We have two possibilities: either $K = K'$ or $K \neq K'$.

Subcase: $K = K'$

1. $\ulcorner \Gamma \urcorner, \ulcorner C \urcorner; \ulcorner \Delta_1 \urcorner, \psi_1, \ulcorner A \urcorner \supset \mathbf{af}(K) \Rightarrow \mathbf{af}(K)$ by Inversion premise 1
2. $\Gamma, \Delta_1, C \Rightarrow K$ affirms A by i.h. on 1
3. $\Gamma, \Delta_1, \Delta_2, \langle K \rangle C \Rightarrow K$ affirms C by Reasoning in INLL
4. $\Gamma, \Delta_1, \Delta_2, \langle K \rangle C \Rightarrow K$ affirms A by Theorem 2.1 on 3,2

Subcase: $K \neq K'$

1. $\Gamma, \Delta_2 \Rightarrow K$ affirms \perp by i.h. premise 2
2. $\perp \Rightarrow K$ affirms A by Rule $\perp L'$
3. $\Gamma, \Delta_2 \Rightarrow K$ affirms A by Theorem 2.1 on 1,2
4. $\Gamma, \Delta_1, \Delta_2, \langle K' \rangle C \Rightarrow K$ affirms A by Weakening on 3

$$\text{Case: } \frac{\ulcorner \Gamma \urcorner; \cdot \Rightarrow \ulcorner A \urcorner \quad \ulcorner \Gamma \urcorner; \ulcorner \Delta \urcorner, \psi, \mathbf{af}(K) \Rightarrow \mathbf{af}(K)}{\ulcorner \Gamma \urcorner; \ulcorner \Delta \urcorner, \psi, \ulcorner A \urcorner \supset \mathbf{af}(K) \Rightarrow \mathbf{af}(K)} \supset L$$

To show: $\Gamma, \Delta \Rightarrow K$ affirms A .

1. $\Gamma \Rightarrow A$ by i.h. premise 1
2. $\Gamma \Rightarrow K$ affirms A by Rule affirms on 1
3. $\Gamma, \Delta \Rightarrow K$ affirms A by Weakening on 2

$$\text{Case: } \frac{\ulcorner \Gamma \urcorner; \cdot \Rightarrow \ulcorner B \urcorner \quad \ulcorner \Gamma \urcorner; \ulcorner \Delta \urcorner, \psi, \ulcorner C \urcorner, \ulcorner A \urcorner \supset \mathbf{af}(K) \Rightarrow \mathbf{af}(K)}{\ulcorner \Gamma \urcorner; \ulcorner \Delta \urcorner, \ulcorner B \urcorner \supset \ulcorner C \urcorner, \ulcorner A \urcorner \supset \mathbf{af}(K), \psi \Rightarrow \mathbf{af}(K)} \supset L$$

To show: $\Gamma, \Delta, B \supset C \Rightarrow K$ affirms A .

1. $\Gamma \Rightarrow B$ by i.h. premise 1
2. $\Gamma, \Delta, C \Rightarrow K$ affirms A by i.h. premise 2
3. $\Gamma, \Delta, B \supset C \Rightarrow K$ affirms A by Rule $\supset L'$ on 1,2

No other case applies.

Proof of statement (4)

Case: Rule init does not apply since the consequent $\mathbf{af}(K)$ cannot occur in $\ulcorner \Delta \urcorner$ (by definition) or ψ (by assumption).

$$\text{Case: } \frac{\ulcorner \Gamma \urcorner, \ulcorner A \urcorner; \ulcorner \Delta \urcorner, \ulcorner A \urcorner, \psi \Rightarrow \mathbf{af}(K)}{\ulcorner \Gamma \urcorner, \ulcorner A \urcorner; \ulcorner \Delta \urcorner, \psi \Rightarrow \mathbf{af}(K)} \text{copy}$$

To show: $\Gamma, A, \Delta \Rightarrow K$ affirms \perp .

1. $\Gamma, A, \Delta, A \Rightarrow K$ affirms \perp by i.h.
2. $\Gamma, A, \Delta \Rightarrow K$ affirms \perp by Strengthening on 1

$$\text{Case: } \frac{\ulcorner \Gamma \urcorner; \ulcorner \Delta \urcorner, \ulcorner A \urcorner, \psi \Rightarrow \mathbf{af}(K)}{\ulcorner \Gamma \urcorner; \ulcorner \Delta \urcorner, \ulcorner A \urcorner \& \ulcorner B \urcorner, \psi \Rightarrow \mathbf{af}(K)} \&L_1$$

To show: $\Gamma, \Delta, A \wedge B \Rightarrow K$ affirms \perp .

1. $\Gamma, \Delta, A \Rightarrow K$ affirms \perp by i.h.
2. $\Gamma, \Delta, A \wedge B \Rightarrow K$ affirms \perp by Rule $\wedge L'_1$ on 1

$$\text{Case: } \frac{\ulcorner \Gamma \urcorner; \ulcorner \Delta \urcorner, \ulcorner B \urcorner, \psi \Rightarrow \mathbf{af}(K)}{\ulcorner \Gamma \urcorner; \ulcorner \Delta \urcorner, \ulcorner A \urcorner \& \ulcorner B \urcorner, \psi \Rightarrow \mathbf{af}(K)} \&L_2$$

To show: $\Gamma, \Delta, A \wedge B \Rightarrow K \text{ affirms } \perp$.

Similar to previous case.

$$\text{Case: } \frac{\ulcorner \Gamma \urcorner; \ulcorner !\ulcorner A \urcorner \urcorner, \ulcorner \Delta \urcorner, \psi \Rightarrow \mathbf{af}(K) \quad \ulcorner \Gamma \urcorner; \ulcorner !\ulcorner B \urcorner \urcorner, \ulcorner \Delta \urcorner, \psi \Rightarrow \mathbf{af}(K)}{\ulcorner \Gamma \urcorner; (\ulcorner !\ulcorner A \urcorner \urcorner) \oplus (\ulcorner !\ulcorner B \urcorner \urcorner), \ulcorner \Delta \urcorner, \psi \Rightarrow \mathbf{af}(K)} \oplus L$$

To show: $\Gamma, A \vee B, \Delta \Rightarrow K \text{ affirms } C$.

1. $\ulcorner \Gamma \urcorner, \ulcorner A \urcorner; \ulcorner \Delta \urcorner, \psi \Rightarrow \mathbf{af}(K)$ by Inversion premise 1
2. $\ulcorner \Gamma \urcorner, \ulcorner B \urcorner; \ulcorner \Delta \urcorner, \psi \Rightarrow \mathbf{af}(K)$ by Inversion premise 2
3. $\Gamma, A, \Delta \Rightarrow K \text{ affirms } \perp$ by i.h. on 1
4. $\Gamma, B, \Delta \Rightarrow K \text{ affirms } \perp$ by i.h. on 2
5. $\Gamma, A \vee B, \Delta \Rightarrow K \text{ affirms } \perp$ by Rule $\vee L'$ on 3,4

$$\text{Case: } \frac{}{\ulcorner \Gamma \urcorner; \ulcorner \Delta \urcorner, \mathbf{0}, \psi \Rightarrow \mathbf{af}(K)} \mathbf{0}L$$

To show: $\Gamma, \Delta, \perp \Rightarrow K \text{ affirms } \perp$.

Follows immediately by rule $\perp L'$.

$$\text{Case: } \frac{\ulcorner \Gamma \urcorner; \ulcorner \Delta_1 \urcorner, \psi_1 \Rightarrow \ulcorner C \urcorner \supset \mathbf{af}(K') \quad \ulcorner \Gamma \urcorner; \ulcorner \Delta_2 \urcorner, \psi_2, \mathbf{af}(K') \Rightarrow \mathbf{af}(K)}{\ulcorner \Gamma \urcorner; \ulcorner \Delta_1 \urcorner, \ulcorner \Delta_2 \urcorner, \psi_1, \psi_2, \ulcorner \langle K' \rangle C \urcorner \Rightarrow \mathbf{af}(K)} \multimap L$$

To show: $\Gamma, \Delta_1, \Delta_2, \langle K' \rangle C \Rightarrow K \text{ affirms } \perp$.

We have two possibilities: $K = K'$ or $K \neq K'$.

Subcase: $K = K'$.

1. $\ulcorner \Gamma \urcorner, \ulcorner C \urcorner; \ulcorner \Delta_1 \urcorner, \psi_1 \Rightarrow \mathbf{af}(K)$ by Inversion premise 1
2. $\Gamma, C, \Delta_1 \Rightarrow K \text{ affirms } \perp$ by i.h. on 1
3. $\Gamma, \Delta_1, \Delta_2, \langle K \rangle C \Rightarrow K \text{ affirms } C$ by Reasoning in INLL
4. $\Gamma, \Delta_1, \Delta_2, \langle K \rangle C \Rightarrow K \text{ affirms } \perp$ by Theorem 2.1 on 3,2

Subcase: $K \neq K'$.

1. $\Gamma, \Delta_2 \Rightarrow K \text{ affirms } \perp$ by i.h. premise 2
2. $\Gamma, \Delta_1, \Delta_2, \langle K' \rangle C \Rightarrow K \text{ affirms } \perp$ by Weakening on 1

$$\text{Case: } \frac{\ulcorner \Gamma \urcorner; \cdot \Rightarrow \ulcorner B \urcorner \quad \ulcorner \Gamma \urcorner; \ulcorner \Delta \urcorner, \psi, \ulcorner C \urcorner \Rightarrow \mathbf{af}(K)}{\ulcorner \Gamma \urcorner; \ulcorner \Delta \urcorner, \ulcorner B \urcorner \supset \ulcorner C \urcorner, \psi \Rightarrow \mathbf{af}(K)} \supset L$$

To show: $\Gamma, \Delta, B \supset C \Rightarrow K \text{ affirms } \perp$.

1. $\Gamma \Rightarrow B$ by i.h. premise 1
2. $\Gamma, \Delta, C \Rightarrow K \text{ affirms } \perp$ by i.h. premise 2
3. $\Gamma, \Delta, B \supset C \Rightarrow K \text{ affirms } \perp$ by Rule $\supset L'$ on 1,2

No other cases apply.

□

Proof of theorem 4.2.

1. Suppose that $\ulcorner \Gamma \urcorner; \cdot \Rightarrow \ulcorner A \urcorner$. Then by theorem G.3(1), $\Gamma \Rightarrow A$.
2. Suppose that $\ulcorner \Gamma \urcorner; \ulcorner A \urcorner \supset \mathbf{af}(K) \Rightarrow \mathbf{af}(K)$. By theorem G.3(3), $\Gamma \Rightarrow K$ affirms A .

□