Noninterference for Intuitionist Necessity

Radha Jagadeesan, Corin Pitcher, and James Riely

DePaul University

Abstract. We study indexed necessity modalities in intuitionist S4. These provide the logical foundation required by a variety of applications, such as capability-based policy languages for access control and type theories for exceptional computation. We establish noninterference properties capturing the limitations on information flow between formulas under the scope of necessity modalities with different indices.

1 Introduction

Classical S4 is standard textbook material [11]. The intuitionist versions of S4 are also well explored [6, 14, 5, 10]. We recall briefly. For any formula α, $\Box\alpha$ is also a formula. The necessity modality[1] satisfies the following three axioms and rule of inference.

$$\Box(\alpha \Rightarrow \beta) \Rightarrow \Box\alpha \Rightarrow \Box\beta \qquad \text{(K: distribution)}$$
$$\Box\alpha \Rightarrow \alpha \qquad \text{(T: reflexivity)}$$
$$\Box\alpha \Rightarrow \Box\Box\alpha \qquad \text{(4: transitivity)}$$
$$\text{If } \alpha \text{ is a theorem, so is } \Box\alpha \qquad \text{(N: necessitation)}$$

In this paper, we investigate the metatheory of indexed intuitionist S4 necessity modalities. Let $(\mathscr{L}, \preceq)$ be a preorder and let a, b range over elements of $\mathscr{L}$. We consider a family of modalities, indexed by elements of $\mathscr{L}$, such that:

For each a, the modality $\Box_a$ satisfies [K,T,4,N] above (Necessity modality)
If $b \preceq a$, then $\Box_b\alpha \Rightarrow \Box_a\alpha$ (Principal naturality)

Such indexed necessity operators arise naturally in a variety of settings. We consider two examples from the literature below.

Security policies. In this example, $(\mathscr{L}, \preceq)$ is a lattice whose elements are security principals. In different applications, principals might represent users, roles, locations, or processes, etc. The ordering in the lattice is the security order: if $b \preceq a$, then b is less secure than a.

The indexed necessitation operator is used to capture the possession of capabilities [8, 7]. Let object references, o, be atomic formulas. Then, $\Box_a o$ is intended to specify that a is permitted to possess object reference o. The formula $\Box_b(o \Rightarrow o')$ specifies a guarded object, such as a ciphertext. By distribution (K), b gets the capability to the plaintext, written $\Box_b o'$, whenever it gets the key, written $\Box_b o$.

In this application, principal naturality captures the idea that more secure principals have access to more capabilities.

[1] The modality has highest precedence; eg. $\Box\alpha \Rightarrow \beta$ stands for $(\Box\alpha) \Rightarrow \beta$

Exceptional computations. The elements of the lattice are sets of exceptions. The ordering in the lattice is the subset order, i.e., $b \preceq a$ if $b \subseteq a$.

The necessity operator is used in the type theory to capture the names of the exceptions that can be raised in evaluating an expression [13, 12]. For example, consider $\Box_a \alpha$ for a modality-free intuitionist formula α. An expression has this type if the following conditions hold: if its evaluation terminates normally, it results in a value of type α; and, any exception that it raises during an abnormal evaluation is contained in the set a. Thus, a is an upper bound on the exceptions that can be raised in evaluating an expression of this type; e.g., a pure functional program of type α that does not raise any exceptions is given the type $\Box_\emptyset \alpha$. Since all types are (at least implicitly) under the scope of an indexed modality, axiom (T) plays a limited role in this treatment.

Principal naturality is a conservative coercion that permits us to increase the upper bound on the set of exceptions that could be raised in evaluating an expression.

Noninterference. Noninterference is the idea that there is no information flow between differently indexed modalities. Let α be a modality free formula. The intuitive idea behind noninterference is that if $\Box_a \alpha$ is derivable from some deductively closed set of hypotheses, then it is derivable from a subset of those hypotheses that are in the scope of the modality indexed by a, i.e. the formulas of the form $\Box_a$. Thus, computations of values of a types are isolated from types that are not in the scope of an a indexed modality.

Noninterference implies the non-provability of some simple formulas. Let p be a proposition, and $b \not\preceq a$. Then, the following formulas are not provable.

$$\not\vdash \Box_b p \Rightarrow \Box_a p$$
$$\not\vdash ((\Box_a p \Rightarrow q) \;\&\; \Box_b p) \Rightarrow \Box_a q$$

Noninterference is essential to justify the use of indexed necessity modalities in the modeling of both motivating examples.

- The policies for capabilities are used in access control in a distributed system. The unprovability of $\Box_b p \Rightarrow \Box_a p$ ensures that the logical reasoning does not permit capabilities to be transferred unrestrictedly between principals. The unprovability of $((\Box_a p \Rightarrow q) \;\&\; \Box_b p) \Rightarrow \Box_a q$ ensures that the acquisition of new capabilities (p) by another principal (b) does not create new capabilities for a principal (a) by purely logical reasoning.
- In the modeling of exceptions, the consequences of noninterference are best seen in computational terms using the Curry-Howard isomorphism. The unprovability of the two formulas above captures the intuitive idea that there are no pure terms that can catch and handle the exceptions in $b \setminus a$. More generally, noninterference identifies the computations that can be queried during the evaluation of a pure expression in the scope of a $\Box_a$; clearly, any computation of a type $\Box_b$ cannot be queried if $a \not\subseteq b$.

Results. We describe an intuitionist logic with indexed necessity operators. Our sequent calculus is a multi-principal variant of the sequent calculus for intuitionist S4 described by Bierman and de Paiva [6]. Our particular design is guided by Abadi's formalization of the "says" monad [1] and games models of this monad [4] .

Our statement of noninterference follows Abadi's statement for monadic logics [1]. We describe a translation of logical formulas into intuitionist propositional logic. The main technical result is that the translation preserve provability, i.e., if the source formula is a theorem in our logic (with indexed modalities), the target formula is provable in standard intuitionist propositional logic. This preservation validates the intuitive idea that the proof of a formula $\Box_a \alpha$ does not essentially use formulas that are *not* in the scope of $\Box_a$.

As simple illustrations of the power of this approach, we show how this result is used to establish the non provability of formulas, including the two unprovable formulas considered earlier in this introduction.

Our noninterference theorem has the form, "for all valid proofs, there exists a translated proof that is valid in intuitionist propositional logic." Consequently, our results hold for any stricter logic that supports fewer proofs. In particular, our results hold for the canonical presentation of the Intuitionist S4 necessity modality. Thus, our noninterference theorem is robust: it is independent of our particular modeling of indexed intuitionist necessity.

Related work. Intuitionist S4 is well explored. For example, Bierman and de Paiva [6] and Alechina, Mendler, de Paiva and Ritter [5] study categorical models of proof and provability. Pfenning and Wong [14] study the proof theory. We do not present a natural deduction system; the above papers discuss the subtle accommodations needed to facilitate the commutative conversions. Goubault-Larrecq and Goubault [10] study the geometry of the proofs of intuitionist S4 using tools from algebraic topology. None of this prior work studies principal-indexed modalities, nor does it address noninterference.

Our exploration of noninterference results is inspired by the modeling of access control using "says" monads and the study of the meta theory of these logics [2, 3, 9, 1, 15]. Our proof of noninterference builds on the translation-based proof pioneered in this research [1, 15]. Our adaptation of these methods uses normal forms inspired by game semantics of monads [4]. This adaptation perforce has some new ingredients because the necessity modality is not "dual" to monads. The dual of the necessity modality in classical S4 is the possibility modality and not the says modality; the says modalities distributes over conjunction and the possibility modality does not.

Rest of the paper. In section 2 we describe a sequent calculus for the logic. The following section 3 describes our treatment of non interference. We conclude in section 4. In appendix A, we explicate the internal structure of our translation by a factorization result.

2 Logic

Let p, q range over a set of atomic propositions. Let $(\mathscr{L}, \preceq)$ be a preorder, and let a, b, c range over elements of $\mathscr{L}$.

We consider intuitionist propositional logic with necessity modalities indexed by elements of $\mathscr{L}$. We include conjunction and implication but not disjunction. Formulas

are defined inductively as follows.

$$\alpha, \beta, \gamma ::= \mathtt{tt} \mid p \mid \alpha \,\&\, \beta \mid \alpha \Rightarrow \beta \mid \Box_a \alpha$$

2.1 a-available

The following definition impacts the modality introduction rule on the right. Formally, the format of the definition shadows Abadi's treatment in logics for monads [1].

Definition 1. a-available formulas are inductively defined as follows.

- $\mathtt{tt}$ is a-available.
- $(\alpha \,\&\, \beta)$ is a-available if both α and β are a-available.
- $\Box_b \alpha$ is a-available if $b \preceq a$
- $\Box_b \alpha$ is a-available if α is a-available
- $(\beta \Rightarrow \alpha)$ is a-available if α is a-available.

This definition extends to sets, multisets, and sequences of formulas $\Gamma = \alpha_1 \ldots \alpha_n$ pointwise. $\Gamma = \alpha_1, \ldots, \alpha_n$ is a-available if all $\alpha_1, \ldots, \alpha_n$ are a-available. □

It will turn out that an a-available formula α is one that satisfies $\alpha \Rightarrow \Box_a \alpha$. In standard presentations, these are the formulas of form $\Box_a$. We motivate our more liberal presentation using game semantics[2] [4]: a formula is a-available if the first move in the game happens in the context of a principal lower in $\preceq$ than a. Thus, $\Box_b \alpha$ is a-available if $b \preceq a$ or α is a-available. The first move in $(\beta \Rightarrow \alpha)$ comes from α, so it is a-available if α is. The first moves of $(\alpha \,\&\, \beta)$ comes from either α or β, so it is a-available if both α, β are. $\mathtt{tt}$ is trivially a-available since it has no moves.

Lemma 2. If $b \preceq a$ and α is b-available, then α is a-available. □

2.2 Sequent calculus

The sequent calculus for the logic is given in Figure 1. Our sequent calculus is a multiprincipal variant of the necessity fragment of the sequent calculus of Bierman and De Paiva [6]. The only modification is in the PROMOTE rule that uses our more generous variation of a-available.

Remark 3. Weakening is admissible [6]. This is the motivation for the weakening built into AXIOM and PROMOTE. We do not present a natural deduction system; subtle accommodations are needed to facilitate the commutative conversions [6, 14]. □

Remark 4 (Standard theorems). The standard ingredients for intuitionist necessity are derivable standardly. None of the following derivations use the third or fourth cases of the Definition 1.

$$\frac{}{\Box_a \alpha \vdash \Box_a \Box_a \alpha} \qquad \text{(Comultiplication)}$$

[2] Abramsky and Jagadeesan [4] describe game semantics for monads in a form that is easily adapted to the current setting. Merely invert the inequality in the definition of condition (p6) in that paper.

$$\frac{}{\Gamma,\alpha\vdash\alpha}\ (\text{AXIOM}) \qquad \frac{\Gamma\vdash\alpha \quad \Delta,\alpha\vdash\beta}{\Gamma,\Delta\vdash\beta}\ (\text{CUT}) \qquad \frac{\Gamma,\gamma,\beta,\Delta\vdash\alpha}{\Gamma,\beta,\gamma,\Delta\vdash\alpha}\ (\text{EXCHANGE}) \qquad \frac{\Gamma\vdash\alpha}{\Gamma,\beta\vdash\alpha}\ (\text{WEAKENING}) \qquad \frac{\Gamma,\beta,\beta,\Delta\vdash\alpha}{\Gamma,\beta,\Delta\vdash\alpha}\ (\text{CONTRACTION})$$

$$\frac{\Gamma,\beta,\gamma,\Delta\vdash\alpha}{\Gamma,\beta\,\&\,\gamma,\Delta\vdash\alpha}\ (\&\text{-L}) \qquad \frac{\Gamma\vdash\alpha \quad \Gamma\vdash\beta}{\Gamma\vdash\alpha\,\&\,\beta}\ (\&\text{-R}) \qquad \frac{\Gamma\vdash\alpha}{\Gamma,\mathtt{tt}\vdash\alpha}\ (\mathtt{tt}\text{-L}) \qquad \frac{}{\Gamma\vdash\mathtt{tt}}\ (\mathtt{tt}\text{-R})$$

$$\frac{\Gamma,\beta\vdash\gamma}{\Gamma\vdash\beta\Rightarrow\gamma}\ (\Rightarrow\text{-R}) \qquad \frac{\Gamma\vdash\beta \quad \Gamma,\gamma\vdash\alpha}{\Gamma,\beta\Rightarrow\gamma\vdash\alpha}\ (\Rightarrow\text{-L}) \qquad \frac{\Gamma,\beta\vdash\alpha}{\Gamma,\Box_a\beta\vdash\alpha}\ (\text{COUNIT}) \qquad \frac{\Gamma\vdash\alpha}{\Gamma,\Delta\vdash\Box_a\alpha}\ (\text{PROMOTE})\ \ \Gamma\ a\text{-available}$$

Fig. 1. Sequent calculus

$$\frac{\beta\vdash\alpha}{\Box_a\beta\vdash\Box_a\alpha}\ (\text{Functoriality})$$

$$\frac{}{\Box_b\alpha\vdash\Box_a\alpha}\ b\preceq a\ (\text{Principal naturality})$$

Comultiplication is derived using AXIOM on $\Box_a\alpha$ followed by PROMOTE. Functoriality is derived using cut against COUNIT followed byPROMOTE. Principal naturality is derivable starting with AXIOM on α, using cut against COUNIT (on b) followed by PROMOTE. □

Remark 5 (Non-standard theorems). Sequences of nested modalities without intervening connectives can be exchanged, providing commutativity of principals.

$$\frac{}{\Box_b\Box_a\alpha\vdash\Box_a\Box_b\alpha}$$

COUNIT yields $\Box_a\Box_b\alpha\vdash\alpha$. The second case of definition 1 ensures that $\Box_a\Box_b\alpha$ is a-available, so use of PROMOTE yields $\Box_a\Box_b\alpha\vdash\Box_a\alpha$. The *third* case of definition 1 ensures that $\Box_a\Box_b\alpha$ is b-available, so use of PROMOTE yields the required result.

Let $A=\{a_0,a_1,\ldots,a_n\}$ be a set of principals. Using commutativity of principals, we can define, without ambiguity, $\Box_A\alpha\triangleq\Box_{a_0}\Box_{a_1}\cdots\Box_{a_n}\alpha$.

Another nonstandard new theorem is:

$$\frac{}{\alpha\Rightarrow\Box_a\beta\vdash\Box_a(\alpha\Rightarrow\Box_a\beta)}$$

Start with AXIOM on $\alpha\Rightarrow\Box_a\beta$. The *third* case of definition 1 ensures that $\alpha\Rightarrow\Box_a\beta$ is a-available since $\Box_a\beta$ is, so use of PROMOTE yields the required result. □

3 Noninterference

We prove noninterference in this section. Our proofs rely on normal forms for formulas. These normal forms are inspired by game semantics. A *unique result formula* is one whose game has a unique starting move. A *multiple result formula* may have multiple

starting moves. In syntactic terms, a unique result formula does not have any conjunction at the ultimate result type.

$$\delta ::= \mathtt{tt} \mid p, q \mid \mu \Rightarrow \delta \mid \Box_a \delta \qquad \text{(Unique result formulas)}$$
$$\mu ::= \delta \mid \mu \,\&\, \delta \mid \delta \,\&\, \mu \qquad \text{(Multiple result formulas)}$$

Any formula α is equivalent to a multiple result formula. This is proved by using the following distributivity laws:

$$\begin{array}{lcl} \Box_a(\alpha \,\&\, \beta) & \Leftrightarrow & \Box_a\alpha \,\&\, \Box_a\beta \\ \alpha \Rightarrow (\beta \,\&\, \gamma) & \Leftrightarrow & (\alpha \Rightarrow \beta) \,\&\, (\alpha \Rightarrow \gamma) \end{array}$$

Remark 6. Moving to multiple result formulas does not affect a-availability. Thus, $\Box_b(\alpha \,\&\, \beta)$ is a-available if and only if $\Box_b\alpha \,\&\, \Box_a\beta$ is a-available. Similarly, $\alpha \Rightarrow (\beta \,\&\, \gamma)$ is a-available if and only if $(\alpha \Rightarrow \beta) \,\&\, (a \Rightarrow \gamma)$ is a-available.

Moving to multiple result formulas does not affect provability if axioms are used only on propositions. We use the following basic facts. An induction on the length of the proofs shows that if $\Gamma, \beta \,\&\, \gamma \vdash \alpha$ is provable, then so is $\Gamma, \beta, \gamma \vdash \alpha$ by a proof of smaller length. Similarly, if $\Gamma \vdash \beta \,\&\, \gamma$ is provable, then so are $\Gamma \vdash \beta$ and $\Gamma \vdash \gamma$ by proofs of smaller length.

For any formula α, let $(\alpha)^{\mathtt{mr}}$ be the equivalent multiple result formulas. Similarly, for any multiset of formulas Γ, let $(\Gamma)^{\mathtt{mr}}$ be the equivalent multiset of multiple result formulas. A simple induction on the length of the proof shows that if $\Gamma \vdash \alpha$ is provable, then there is a proof $(\Gamma)^{\mathtt{mr}} \vdash (\alpha)^{\mathtt{mr}}$ containing only multiple result formulas. As a sample case, consider the case when the last rule is $\Rightarrow$-R, so we have the following.

$$\dfrac{\Gamma, \beta \vdash \gamma_1 \,\&\, \gamma_2}{\Gamma \vdash \beta \Rightarrow (\gamma_1 \,\&\, \gamma_2)}\,{\scriptstyle (\Rightarrow\text{-R})}$$

In this case, we also have proofs of $\Gamma, \beta \vdash \gamma_1$ and $\Gamma, \beta \vdash \gamma_2$ of smaller length. So, by induction hypothesis, we have proofs of $(\Gamma, \beta)^{\mathtt{mr}} \vdash (\gamma_1)^{\mathtt{mr}}$ and $(\Gamma, \beta)^{\mathtt{mr}} \vdash (\gamma_2)^{\mathtt{mr}}$. Using $\Rightarrow$-R on each of these proofs followed by an application of &-R yields the required proof of $(\Gamma)^{\mathtt{mr}} \vdash (\beta \Rightarrow \gamma_1)^{\mathtt{mr}} \,\&\, (\beta \Rightarrow \gamma_2)^{\mathtt{mr}}$. □

In the rest of this section, without loss of generality, we will assume that all the formulas are multiple result formulas and axioms are used only on propositions.

3.1 Translations of formulas

We describe two translations $\langle\alpha\rangle_a^+$ and $\langle\alpha\rangle_a^-$ on multiple-result formulas by mutual recursion. Both translations yield pure IPL formulas without any modalities. The translation $\langle\cdot\rangle_a^-$ is closest in spirit to the extant treatment of the says monad [1], albeit with modifications designed to accommodate the differences arising from the necessity modality.

The translations share some common features: Both are structural and remove all modalities. Both "delete" information by replacing some chosen subformulas by $\mathtt{tt}$.

The intuition is that both translations try to ensure that results of a-available formulas are not influenced by formulas that are not a-available. This is illustrated by considering the translation of $\alpha \Rightarrow \beta$ when β is a-available. In this case, the translations ensure that all the subformulas of α that are not a-available are replaced by $\mathtt{tt}$. Viewing via the lens of game semantics, the translations replace the non a-available formulas by the empty game that interprets $\mathtt{tt}$. Thus, the Opponent cannot move in these subformula occurrences. The upcoming preservation theorem (Theorem 13) shows that the proof also does not need to make moves in this proposition instance, i.e. this subformula instance is expendable to the proof.

$\langle\cdot\rangle_a^-$ enforces more constraints: it also replaces the results that are not a-available by $\mathtt{tt}$.

Definition 7. For a formula α in multiple result normal form, define $\langle\alpha\rangle_a^+, \langle\alpha\rangle_a^-$ in IPL as follows.

$$\begin{array}{ll|ll}
\langle\mathtt{tt}\rangle_a^+ & = \mathtt{tt} & \langle\mathtt{tt}\rangle_a^- & = \mathtt{tt} \\
\langle p\rangle_a^+ & = p & \langle p\rangle_a^- & = \mathtt{tt} \\
\langle\alpha \,\&\, \beta\rangle_a^+ & = \langle\alpha\rangle_a^+ \,\&\, \langle\beta\rangle_a^+ & \langle\alpha \,\&\, \beta\rangle_a^- & = \langle\alpha\rangle_a^- \,\&\, \langle\beta\rangle_a^- \\
\langle\Box_b\alpha\rangle_a^+ & = \langle\alpha\rangle_a^+ & \langle\Box_b\alpha\rangle_a^- & = \begin{cases} \langle\alpha\rangle_a^-, & b \not\preceq a \\ \langle\alpha\rangle_a^+, & b \preceq a \end{cases} \\
\langle\alpha \Rightarrow \beta\rangle_a^+ & = \begin{cases} \langle\alpha\rangle_a^- \Rightarrow \langle\beta\rangle_a^+, & \beta\ a-\text{available} \\ \langle\alpha\rangle_a^+ \Rightarrow \langle\beta\rangle_a^+, & \text{otherwise} \end{cases} & \langle\alpha \Rightarrow \beta\rangle_a^- & = \langle\alpha\rangle_a^- \Rightarrow \langle\beta\rangle_a^-
\end{array}$$

These definitions extend pointwise to sets/multisets/sequences of formulas.

$$\langle\alpha_1,\ldots,\alpha_n\rangle_a^+ = \langle\alpha_1\rangle_a^+,\ldots,\langle\alpha_n\rangle_a^+$$
$$\langle\alpha_1,\ldots,\alpha_n\rangle_a^- = \langle\alpha_1\rangle_a^-,\ldots,\langle\alpha_n\rangle_a^+$$

Consider propositions p. $\langle p\rangle_a^+$ is p since there are no constraints that need to be enforced. However, since p is not a-available, $\langle p\rangle_a^-$ is $\mathtt{tt}$.

$\langle\cdot\rangle_a^+$ is fully compositional for all cases except implication $\alpha \Rightarrow \beta$ when β is a-available. In this case, we switch to $\langle\alpha\rangle_a^-$to ensure that only a-available formulas influence a-available results.

$\langle\cdot\rangle_a^-$ is fully compositional for all cases except $\Box_b\alpha$ when $b \preceq a$. In this case, we switch to $\langle\alpha\rangle_a^+$ because the enclosing modality $\Box_b$ intuitively has satisfied the constraint of making the formula available to a, so we only need to enforce the constraints of $\langle\cdot\rangle_a^+$.

Example 8. (a) $\langle p \Rightarrow q\rangle_a^+ = (p \Rightarrow q)$. (b) $\langle p \Rightarrow q\rangle_a^- = \mathtt{tt}$. (c) $\langle p \Rightarrow \Box_a q\rangle_a^+ = \langle p \Rightarrow \Box_a q\rangle_a^- = (\mathtt{tt} \Rightarrow q)$ □

Remark 9. The translations $\langle\cdot\rangle_a^+$ and $\langle\cdot\rangle_a^-$ are not semantically robust. They do not respect equivalence of formulas. They have the desired properties explicated below only on formulas in multiple result normal form. □

The translations coincide on a-available formulas. This confirms the intuition that they differ only in the availability of the top-level formula.

Lemma 10. If α is a-available, then $\langle\alpha\rangle_a^+ = \langle\alpha\rangle_a^-$. □

PROOF. By structural induction on α. The base cases for the induction are when α is of the form $\mathtt{tt}$ and $\Box_b\beta$ with $b \preceq a$. In these cases, $\langle\alpha\rangle_a^+ = \langle\alpha\rangle_a^-$ by definition.
If β, γ are a-available: $\langle\beta \,\&\, \gamma\rangle_a^+ = \langle\beta\rangle_a^+ \,\&\, \langle\gamma\rangle_a^+ = \langle\beta\rangle_a^- \,\&\, \langle\gamma\rangle_a^- = \langle\beta \,\&\, \gamma\rangle_a^-$
If γ is a-available: $\langle\beta \Rightarrow \gamma\rangle_a^+ = \langle\beta\rangle_a^- \Rightarrow \langle\gamma\rangle_a^+ = \langle\beta\rangle_a^- \Rightarrow \langle\gamma\rangle_a^- = \langle\beta \Rightarrow \gamma\rangle_a^-$
If $b \not\preceq a$ and β is a-available: $\langle\Box_b\beta\rangle_a^+ = \langle\beta\rangle_a^+ = \langle\beta\rangle_a^- = \langle\Box_b\beta\rangle_a^-$ □

The next two lemmas are the key technical drivers that motivate the consideration of normal forms for formulas in this proof. If the sole result of a single result formula is not a-available, the $\langle\cdot\rangle_a^-$ translation removes all non trivial information from it.

Lemma 11. If a unique result formula δ is not a-available, then $\langle\delta\rangle_a^- \Leftrightarrow \mathtt{tt}$. □

PROOF. By structural induction on δ. If δ is of the form $\mathtt{tt}$ or p, $\langle\delta\rangle_a^- = \mathtt{tt}$ by definition. If δ is not a-available, for any α $\langle\alpha \Rightarrow \delta\rangle_a^- = \langle\alpha\rangle_a^- \Rightarrow \langle\delta\rangle_a^- = \langle\alpha\rangle_a^- \Rightarrow \mathtt{tt}$; the result follows. If $b \not\preceq a$ and δ is not a-available: $\langle\Box_b\delta\rangle_a^- = \langle\delta\rangle_a^-$; the result follows by the induction hypothesis. □

We are now able to confirm that the $\langle\cdot\rangle_a^-$ translation is more restrictive than the $\langle\cdot\rangle_a^+$ translation.

Lemma 12. For all μ in multiple result form , $\langle\mu\rangle_a^+ \vdash \langle\mu\rangle_a^-$ is provable. □

PROOF.
Single Result Formulas: Consider first the case when μ is a formula δ in single result form. We prove the result by structural induction on the construction of δ.
If δ is of the form $\mathtt{tt}$ or p. In these cases, result follows since $\langle\delta\rangle_a^- = \mathtt{tt}$.
If δ is a-available: $\langle\beta \Rightarrow \delta\rangle_a^+ = \langle\beta\rangle_a^- \Rightarrow \langle\delta\rangle_a^+ \Rightarrow \langle\beta\rangle_a^- \Rightarrow \langle\delta\rangle_a^- = \langle\beta \Rightarrow \delta\rangle_a^-$
If δ is not a-available, $\beta \Rightarrow \delta$ is not a-available and result follows since $\langle\beta \Rightarrow \gamma\rangle_a^- = \mathtt{tt}$ by lemma 11.
If $b \not\preceq a$: $\langle\Box_b\delta\rangle_a^+ = \langle\delta\rangle_a^+ \Rightarrow \langle\delta\rangle_a^- = \langle\Box_b\delta\rangle_a^-$
If $b \preceq a$: $\langle\Box_b\delta\rangle_a^+ = \langle\delta\rangle_a^+ = \langle\Box_b\delta\rangle_a^-$
Multiple result formulas. Given the result for single-result formulas, the proof for multiple result formulas μ follows by structural induction on the formation of μ. □

3.2 Noninterference theorem

Theorem 13. Let Γ, α be formulas in multiple result form. If $\Gamma \vdash \alpha$, then:

$$\langle\Gamma\rangle_a^+ \vdash \langle\alpha\rangle_a^+, \text{ and}$$
$$\langle\Gamma\rangle_a^- \vdash \langle\alpha\rangle_a^-$$

are provable in intuitionist propositional logic. □

PROOF. Proof by induction on the structure of the proof of $\Gamma \vdash \alpha$.

Induction step for $\langle\Gamma\rangle_a^- \vdash \langle\alpha\rangle_a^-$. The proofs for the inductive case when the last rule is any rule except COUNIT or PROMOTE are all similar. In each of these cases, the inductive step to show $\langle\Gamma\rangle_a^- \vdash \langle\alpha\rangle_a^-$ follows because the translation $\langle(\cdot)\rangle_a^-$ is compositional on the structure of the propositional connectives and the universal quantifier.

For example consider the case when the last step in the proof of $\Gamma \vdash \alpha$ is &-R. So, we have $\alpha = \beta \,\&\, \gamma$ and the following proof structure:

$$\frac{\Gamma \vdash \beta \qquad \Gamma \vdash \gamma}{\Gamma \vdash \beta \,\&\, \gamma}$$

By inductive hypothesis, we deduce a proof of $\langle\Gamma\rangle_a^- \vdash \langle\beta\rangle_a^-$ and $\langle\Gamma\rangle_a^- \vdash \langle\gamma\rangle_a^-$. An application of &-R yields $\langle\Gamma\rangle_a^- \vdash \langle\beta\rangle_a^- \,\&\, \langle\gamma\rangle_a^-$ thus completing this case since $\langle\alpha\rangle_a^- = \langle\beta\rangle_a^- \,\&\, \langle\gamma\rangle_a^-$.

If the last rule is COUNIT, i.e.

$$\frac{\Gamma, \beta \vdash \alpha}{\Gamma, \Box_b\beta \vdash \alpha}$$

by induction hypothesis, we have a proof of $\langle\Gamma\rangle_a^-, \langle\beta\rangle_a^- \vdash \langle\alpha\rangle_a^-$. There are two cases depending on the order between b, a.

$b \preceq a$ By definition, $\langle\Box_b\beta\rangle_a^- = \langle\beta\rangle_a^+$. From lemma 12, $\langle\beta\rangle_a^+ \vdash \langle\beta\rangle_a^-$ is provable, so we get required result by use of CUT with the proof above yielded by the induction hypothesis.

$b \not\preceq a$. By definition, $\langle\Box_b\beta\rangle_a^- = \langle\beta\rangle_a^-$. Hence, the induction hypothesis yields the required result.

If the last rule is PROMOTE, i.e.

$$\frac{\Gamma \vdash \alpha}{\Gamma \vdash \Box_b\alpha}\ \Gamma \text{ is } b\text{-available}$$

There are two cases depending on the order between b, a.

$b \preceq a$ By induction hypothesis on the $\langle\cdot\rangle_a^+$ translation, we have a proof of

$$\langle\Gamma\rangle_a^+ \vdash \langle\alpha\rangle_a^+$$

Since $b \preceq a$, by lemma 2, Γ is also a-available. So, by lemma 10, $\langle\Gamma\rangle_a^+ = \langle\Gamma\rangle_a^-$. Also, by definition, $\langle\Box_b\alpha\rangle_a^- = \langle\alpha\rangle_a^+$.

$b \not\preceq a$. By induction hypothesis, we have a proof of

$$\langle\Gamma\rangle_a^- \vdash \langle\alpha\rangle_a^-$$

By definition, $\langle\Box_b\alpha\rangle_a^- = \langle\alpha\rangle_a^-$.

In either case, the required proof of $\langle\Gamma\rangle_a^- \vdash \langle\Box_b\alpha\rangle_a^-$ coincides with the proof yielded by the induction hypothesis. The additional formulas Δ on the left are added using weakening.

Induction step for $\langle\Gamma\rangle_a^+ \vdash \langle\alpha\rangle_a^+$. The translation $\langle(\cdot)\rangle_a^+$ is compositional on the structure of & and the modality. So, if the last rule is any except $\Rightarrow$-R or $\Rightarrow$-L, the inductive step to show that $\langle\Gamma\rangle_a^+ \vdash \langle\alpha\rangle_a^+$ holds follows immediately.

For example, consider the case when the last step in the proof of $\Gamma \vdash \alpha$ is &-R. So, we have $\alpha = \beta \,\&\, \gamma$ and the following proof structure:

$$\frac{\Gamma \vdash \beta \qquad \Gamma \vdash \gamma}{\Gamma \vdash \beta \,\&\, \gamma}$$

By inductive hypothesis, we deduce a proof of $\langle\Gamma\rangle_a^+ \vdash \langle\beta\rangle_a^+$ and $\langle\Gamma\rangle_a^+ \vdash \langle\gamma\rangle_a^+$. An application of &-R yields $\langle\Gamma\rangle_a^+ \vdash \langle\beta\rangle_a^+ \,\&\, \langle\gamma\rangle_a^+$. This completes this case of the proof since $\langle\alpha\rangle_a^+ = \langle\beta\rangle_a^+ \,\&\, \langle\gamma\rangle_a^+$.

If the last rule is $\Rightarrow$-R or $\Rightarrow$-L and the implication formula in question is $\beta \Rightarrow \gamma$, there are two cases based on whether γ is a-available or not.

If γ is not a-available, the $\langle\cdot\rangle_a^+$ translation is still compositional, i.e. $\langle\beta \Rightarrow \gamma\rangle_a^+ = \langle\beta\rangle_a^+ \Rightarrow \langle\gamma\rangle_a^+$ and the proof is similar to case above.

If γ is a-available, $\langle\beta \Rightarrow \gamma\rangle_a^+ = \langle\beta\rangle_a^- \Rightarrow \langle\gamma\rangle_a^+$.

$\Rightarrow$-R: The last rule is:

$$\frac{\Gamma, \beta \vdash \gamma}{\Gamma \vdash \beta \Rightarrow \gamma}$$

From induction hypothesis, we deduce the existence of a proof of

$$\langle\Gamma\rangle_a^-, \langle\beta\rangle_a^- \vdash \langle\gamma\rangle_a^-$$

and hence using $\langle\beta \Rightarrow \gamma\rangle_a^- = \langle\beta\rangle_a^- \Rightarrow \langle\gamma\rangle_a^-$, a proof of:

$$\langle\Gamma\rangle_a^- \vdash \langle\beta \Rightarrow \gamma\rangle_a^-$$

Since $\beta \Rightarrow \gamma$ is a-available, $\langle\beta \Rightarrow \gamma\rangle_a^- = \langle\beta \Rightarrow \gamma\rangle_a^+$ by lemma 10. So, we deduce :

$$\langle\Gamma\rangle_a^- \vdash \langle\beta \Rightarrow \gamma\rangle_a^+$$

From lemma 12, the sequents $\langle\alpha\rangle_a^+ \vdash \langle\alpha\rangle_a^-$ are provable for each $\alpha \in \Gamma$. So, by multiple uses of cut, we get a proof of: $\langle\Gamma\rangle_a^+ \vdash \langle\beta \Rightarrow \gamma\rangle_a^+$ as required.

$\Rightarrow$-L: The last rule is:

$$\frac{\Gamma \vdash \beta \qquad \Gamma, \gamma \vdash \alpha}{\Gamma, \beta \Rightarrow \gamma \vdash \alpha}$$

From induction hypothesis, we deduce the existence of proofs:

$$\langle\Gamma\rangle_a^- \vdash \langle\beta\rangle_a^- \qquad\qquad \langle\Gamma\rangle_a^+, \langle\gamma\rangle_a^+ \vdash \langle\alpha\rangle_a^+$$

From lemma 12, the sequents $\langle\alpha\rangle_a^+ \vdash \langle\alpha\rangle_a^-$ are provable for each $\alpha \in \Gamma$. So, by multiple uses of cut with the left proof, we get a proof of:

$$\langle\Gamma\rangle_a^+ \vdash \langle\beta\rangle_a^-$$

Using $\Rightarrow$-L with the right proof above yields a proof of:

$$\langle\Gamma\rangle_a^+, \langle\beta\rangle_a^- \Rightarrow \langle\gamma\rangle_a^+ \vdash \langle\alpha\rangle_a^+$$

Required result follows since $\langle\beta \Rightarrow \gamma\rangle_a^+ = \langle\beta\rangle_a^- \Rightarrow \langle\gamma\rangle_a^+$. □

The main use of this theorem is to prove that certain sequents are not provable. We illustrate with very simple examples.

Example 14. In all the following examples, we use theorem 13 for $\langle\cdot\rangle_a^-$.

- If $p \vdash \Box_a p$ is provable, so is $\mathtt{tt} \vdash p$.
- Let $b \not\preceq a$. If $\Box_b p \vdash \Box_a p$ is provable , so is $\mathtt{tt} \vdash p$ in IPL.
- Let $b \not\preceq a$. If $\Box_b p, \Box_a(p \Rightarrow q) \vdash \Box_a q$ is provable, so is $\mathtt{tt}, p \Rightarrow q \vdash q$.

Since $\mathtt{tt} \vdash p$ and $p \Rightarrow q \vdash q$ are unprovable in IPL, all the above three sequents are unprovable. □

4 Conclusions

Recent research in both type theories and security have used indexed necessity modalities of intuitionist S4 as the logical foundations. Noninterference between the different indices is a key metatheoretic property that is essential to the soundness of this modeling. In this paper, we establish noninterference for indexed intuitionist necessity modalities.

Our work is inspired by noninterference theorems for monads—logically speaking, the "says" modality from logics for access control. However, to the best of our knowledge, noninterference has not been investigated for the necessity modality. The dual of the necessity modality is not the says modality but the possibility modality. So, our proof incorporates novelties in the form of normal forms for intuitionist S4 inspired by game semantics.

Our desire is to ultimately build a similar metatheory for a modal logic that incorporates *both* kinds of modalities. Such logics are already used for security policies and in type theories for functional languages.

This research was supported by NSF CCF-0915704.

References

1. Martín Abadi. Access control in a core calculus of dependency. *ENTCS*, 172:5–31, 2007.
2. Martín Abadi, Anindya Banerjee, Nevin Heintze, and Jon G. Riecke. A core calculus of dependency. In *POPL*, pages 147–160, 1999.
3. Martín Abadi, Michael Burrows, Butler W. Lampson, and Gordon D. Plotkin. A calculus for access control in distributed systems. *ACM Trans. Program. Lang. Syst.*, 15(4):706–734, 1993.
4. Samson Abramsky and Radha Jagadeesan. Game semantics for access control. *ENTCS*, 249:135–156, 2009.
5. Natasha Alechina, Michael Mendler, Valeria de Paiva, and Eike Ritter. Categorical and kripke semantics for constructive s4 modal logic. In *Proc. of CSL*, volume 2142 of *LNCS*, pages 292–307, 2001.
6. G M Bierman and V C V de Paiva. On an intuitionistic modal logic. *Studia Logica*, 65:2000, 2001.
7. Henry DeYoung, , and Frank Pfenning. Reasoning about the consequences of authorization policies in a linear epistemic logic. Technical Report 1213, CMU-CS, 2009.

8. Deepak Garg, Lujo Bauer, Kevin D. Bowers, Frank Pfenning, and Michael K. Reiter. A linear logic of authorization and knowledge. In *Proc. of ESORICS*, volume 4189 of *LNCS*, pages 297–312, 2006.
9. Deepak Garg and Frank Pfenning. Non-interference in constructive authorization logic. In *CSFW*, pages 283–296, 2006.
10. Jean Goubault-Larrecq and Eric Goubault. On the geometry of intutionist s4 proofs. *Homology, Homotopy and Applications*, 5(2):137–209, 2003.
11. G. E. Hughes and M. J Cresswell. *An introduction to modal logic*. 1972.
12. Gregory Malecha and Stephen Chong. A more precise security type system for dynamic security tests. In *Proceedings of the 5th ACM SIGPLAN PLAS Workshop*, PLAS '10, pages 4:1–4:12, 2010.
13. Aleksandar Nanevski. A Modal Calculus for Exception Handling. In *Intuitionistic Modal Logics and Applications Workshop (IMLA '05)*, Chicago, IL, June 2005.
14. Frank Pfenning and Hao-Chi Wong. On a modal λ-calculus for S4. In *Proc. of the Eleventh MFPS*, 1995. ENTCS, Volume 1.
15. Stephen Tse and Steve Zdancewic. Translating dependency into parametricity. In *Proc. of the ninth ACM ICFP*, ICFP '04, pages 115–125, 2004.

A Factoring the translation

The translations $\langle\cdot\rangle_a^+$ and $\langle\cdot\rangle_a^-$ can be factored into two pieces:

- Translations $(|\cdot|)_a^+$ and $(|\cdot|)_a^-$ remove principals and result in formulas in the fragment of our logic that uses modalities indexed only by a. Thus, the target of this translation is a variant of Intutionist S4.
- The standard forgetful translation from Intuitionist S4 into intuitionist propositional logic simply erases all modalities.

For a formula α in multiple result normal form, define $(|\alpha|)_a^+, (|\alpha|)_a^-$ as follows. The only differences are in the cases for the modality.

$$
\begin{array}{ll}
(|\mathtt{tt}|)_a^+ & = \mathtt{tt} \\
(|p|)_a^+ & = p \\
(|\alpha \mathbin{\&} \beta|)_a^+ & = (|\alpha|)_a^+ \mathbin{\&} (|\beta|)_a^+ \\
(|\Box_b \alpha|)_a^+ & = \begin{cases} (|\alpha|)_a^+, & b \not\preceq a \\ \Box_a (|\alpha|)_a^+, & b \preceq a \end{cases} \\
(|\alpha \Rightarrow \beta|)_a^+ & = \begin{cases} (|\alpha|)_a^- \Rightarrow (|\beta|)_a^+, & \beta\ a-\text{available} \\ (|\alpha|)_a^+ \Rightarrow (|\beta|)_a^+, & \text{otherwise} \end{cases}
\end{array}
\qquad
\begin{array}{ll}
(|\mathtt{tt}|)_a^- & = \mathtt{tt} \\
(|p|)_a^- & = \mathtt{tt} \\
(|\alpha \mathbin{\&} \beta|)_a^- & = (|\alpha|)_a^- \mathbin{\&} (|\beta|)_a^- \\
(|\Box_b \alpha|)_a^- & = \begin{cases} (|\alpha|)_a^-, & b \not\preceq a \\ \Box_a (|\alpha|)_a^+, & b \preceq a \end{cases} \\
(|\alpha \Rightarrow \beta|)_a^- & = (|\alpha|)_a^- \Rightarrow (|\beta|)_a^-
\end{array}
$$

We are able to prove the analogue of theorem 13. If $\Gamma \vdash \alpha$, then:

$$(|\Gamma|)_a^+ \vdash (|\alpha|)_a^+, \text{ and}$$
$$(|\Gamma|)_a^- \vdash (|\alpha|)_a^-$$

are provable. The proof uses the analogues for Lemmas 10–12 that are listed below.

1. If α is a-available, then $(|\alpha|)_a^+ = (|\alpha|)_a^-$; furthermore, $(|\alpha|)_a^-$ is a-available.
2. If a single result formula δ is not a-available, then $(|\delta|)_a^- = \mathtt{tt}$.
3. For all μ in multiple result form , $(|\mu|)_a^+ \vdash (|\mu|)_a^-$ is provable.