Project Report
Intuitionistic Multimodal Logic as an Authorization Logic

15-816 Modal Logic

Anand Subramanian, Zachary Sparks

May 9, 2010

Abstract

This project presents an intuitionistic multimodal logic based on indexed modalities of validity and possibility, and its potential application as a logic for Proof Carrying Authorization [AF99] in a distributed system. The report begins by considering an authorization logic presented by Garg and Pfenning in [GP06] which describes statements certified by principals as lax truth indexed by the name of the certifying principal. We then incrementally revise it to arrive at a tethered sequent calculus in the style of [Pfe10c], called TM4s.

TM4s is at once a small fragment of the logic BL presented by Garg in his thesis [Gar09], as well as a small extension to it that makes the logic more friendly to an operational interpretation for distributed computation.

Keywords: Authorization Logic, Multimodal Logic, Tethered Semantics.

1 Introduction

The focus of this project is to explore the application of intuitionistic multimodal logics to the specification of policies and authorization in a multiagent system. We are particularly interested in multimodal logics that are formulated using the judgmental method, and whose modalities correspond to the modalities of validity and possibility in [PD01] and their analogous modalities in Intuitionistic Kripke semantics [Pfe10c, Pfe10a]. We are also specifically interested in authorization logics developed in a multimodal setting, in which the agents of the system are represented in a discernible manner by subscripts attached to the modalities rather than as any other formulae in the system.

Constructive logics have been actively studied for decades, and constructive *authorization* logics formulated using the judgmental method have been studied for a few years now in [GP06, DLK^{+}06, LJK^{+}08, Gar09]. Recent work (especially that cited in this project) exhibit a few major trends:

1. The logics utilize and endorse the philosophy of Proof Carrying Authorization (PCA) [AF99]. In a system that implements PCA, the burden of determining whether a principal is authorized to perform a particular action, and *why* it is authorized to perform that operation, like on the principal requesting access. This is as opposed to a design philosophy in which the entity responsible for granting access derives a proof of authorization.

2. Most of these logics introduced an operator, most often of the form k `says` s, where k stands for a principal, and s stands for any formula that said principal is asserting. This operator abstracts away the details of authentication, i.e. the logic is unconcerned with cryptographic protocols or other details that are involved in actually implementing a means by which a principal can attach its credentials to a statement.

3. In most of these logics, the `says` operator corresponds to the strong monad or lax modality with an index, i.e. the modality is additionally qualified, or "indexed" by the name of a principal.

This project endorses and follows the first two trends. However, it is both motivated by, and diverges from, the third trend. We were motivated to explore the application of indexed possibility and validity to authorization logic for two reasons:

1. There is a well established translation that embeds the monomodal lax logic in a logic of validity and necessity [PD01]. This suggests that there is some correspondence between their multimodal equivalents.

2. Constructive S5 logic (based on non-indexed validity and possibility) has already been interpreted as a type theory for distributed computation by Murphy et al [Mur08] in light of the Curry-Howard isomorphism and Intuitionistic Kripke semantics. This opens up the possi-

bility that the indexed equivalents may correspondingly be computationally interpreted as a type theory for distributed computation in a multi-agent system with PCA.

The result of this project is a tethered sequent calculus called TM4s, arrived at by incrementally revising the logic GP [GP06]. TM4s is simultaneously a small fragment of the logic BL presented by Garg in his dissertation [Gar09], and a small extension to it that makes the logic more friendly to distributed computation.

The report is structured as follows: ∮ 2 briefly recapitulates the logics presented in [GP06] and [DLK+06], and slightly modifies them to come up with the logic M4 based on indexed modalities of validity and truth. Some undesirable properties are identified. This leads to ∮ 3 which implicitly indexes truth with principals to resolve the issues present in M4. The resulting judgmental sequent calculus is called JM4s, and its tethered counterpart is called TM4s.

2 The Logic M4

We begin exploring the logic M4 that supports a notion of indexed validity and possibility. M4 is inspired by the pure fragment of the linear logic of affirmation and knowledge presented in [DLK+06]. The linear logic of affirmation and knowledge is an interesting first candidate because it presents an authorization logic that simultaneously makes use of two different indexed judgments, one of them corresponding to validity and the other corresponding to lax truth. Our first thought was to revise the rules for affirmation to make it correspond to possibility instead of lax truth. Since [DLK+06] uses a sequent calculus, we too use formalize M4 as a sequent calculus.

2.1 JM4: Judgmental M4

The judgmental sequent calculus M4 has sequents of the form:

$$\Delta; \Gamma \rightarrow \gamma$$

Δ contains assumptions of the form k *cert* A and Γ contains assumptions of the form A *true*. The *cert* judgment corresponds to the `knows` judgment from [DLK+06], and has been renamed to avoid naming collisions when the logic is revised. It can be read as "principal k has certifying authority over a proposition A". The γ on the right side is a place-holder for one of two judgments: A *true* or k *claims* A. The judgment *claims* is roughly equivalent to the judgment `affirms` in [DLK+06], and has been renamed to avoid name collisions. As of now, it can be read as "k claims that it has access to A, but cannot certify complete ownership". We recapitulate the judgmental rules and the rules defining the modal operators.

$$\frac{\Delta, k\ \mathit{cert}\ A; \Gamma, A\ \mathit{true} \rightarrow C\ \mathit{true}}{\Delta, k\ \mathit{cert}\ A; \Gamma \rightarrow C\ \mathit{true}}\ \mathit{cert} \qquad \frac{\Delta; \Gamma \rightarrow A\ \mathit{true}}{\Delta; \Gamma \rightarrow k\ \mathit{claims}\ A}\ \mathit{claims}$$

$$\frac{\Delta_k; \cdot \rightarrow A\ \mathit{true}}{\Delta; \Gamma \rightarrow \Box_k A\ \mathit{true}}\ \Box R \qquad \frac{\Delta; \Gamma \rightarrow k\ \mathit{claims}\ A}{\Delta; \Gamma \rightarrow \Diamond_k A\ \mathit{true}}\ \Diamond R$$

$$\frac{\Delta, k\ \mathit{cert}\ A; \Gamma, \Box_k A\ \mathit{true} \rightarrow C\ \mathit{true}}{\Delta; \Gamma, \Box_k A\ \mathit{true} \rightarrow C\ \mathit{true}}\ \Box L \qquad \frac{\Delta; A\ \mathit{true} \rightarrow k\ \mathit{claims}\ C}{\Delta; \Gamma, \Diamond_k A\ \mathit{true} \rightarrow k\ \mathit{claims}\ C}\ \Diamond L$$

$$\begin{array}{rcl} (\cdot)_k & = & \cdot \\ (\Delta, k\ \mathit{cert}\ A)_k & = & k\ \mathit{cert}\ A, \Delta_k \\ (\Delta, j\ \mathit{cert}\ A)_k & = & \Delta_k \text{ when } j \neq k \end{array}$$

We briefly observe that the right rule for $\Box$ is responsible for restricting access to the assumptions in Δ, to prevent assumptions belonging to a principal from being stolen and recertified by other principals. Due to this restriction, the judgmental rule for *cert* can safely copy any assumption certified by any principal into Γ.

We also changed the left rule for $\Diamond$ to resemble the left rule for possibility, whereas [DLK+06] presented the following rule, corresponding to the strong monad:

$$\frac{\Delta; \Gamma, \langle k\rangle A\ \mathit{true}, A\ \mathit{true} \rightarrow k\ \mathit{claims}\ C}{\Delta; \Gamma, \langle k\rangle A\ \mathit{true} \rightarrow k\ \mathit{claims}\ C}\ \langle\rangle L$$

The following meta-theorems hold over JM4, in addition to weakening, contraction and exchange:

Theorem 1. ***Admissibility of Cut for JM4***

i. If $\Delta; \Gamma \rightarrow A$ true *and* $\Delta; \Gamma, A$ true $\rightarrow \gamma$ *then* $\Delta; \Gamma \rightarrow \gamma$.

ii. If $\Delta; \cdot \rightarrow A \text{ true}$ *and* $\Delta, k \text{ cert } A; \Gamma \rightarrow \gamma$ *then* $\Delta; \Gamma \rightarrow \gamma$.

iii. If $\Delta; \Gamma \rightarrow k \text{ claims } A$ *and* $\Delta; \cdot, A \text{ true} \rightarrow k \text{ claims } C$ *then* $\Delta; \Gamma \rightarrow k \text{ claims } C$.

Proof. By lexicographic induction, first on the size of the cut formula A, then on the on the ordering `(i) < (ii)` and `(i) < (iii)` of the induction hypotheses, and then simultaneously on the sizes of the two given derivations. □

Theorem 2. ***Admissibility of Identity for JM4***
$\Delta; \Gamma, A \text{ true} \rightarrow A \text{ true}$ *for any* Δ, Γ, *and* A.

Proof. By induction on the size of the proposition A. □

Admissibility of Cut and Identity are used as the metric for global soundness and completeness of the calculus. We do not include the full text of the proofs in this paper. The proofs proceed by structural induction in the style demonstrated in [Pfe10b], and there are no cases of special significance.

2.2 Admissible and Inadmissible Properties of JM4

This section considers some properties that this logic admits and some that it fails to admit in order to judge its suitability as an authorization logic. These properties serve as guiding principles for our next revision of the logic, called M4s. First, we examine □.

- □ has the usual interaction rules with the usual propositional connectives. It commutes with them in the same manner as its monomodal analogue. Most important to us is axiom K.

$$\vdash \Box_k(A \supset B) \supset (\Box_k A \supset \Box_k B)$$

- $\vdash \Box_k A \supset A$
  This property is undesirable, at least for an operator that purports to certify a statement only for one principal. If any principal encounters an error, or gives a faulty proof of authorization, the entire system can crash. The `says` operator presented in [GP06] does not admit this property. In fact, this is the first "non-interference" criterion tested for.

- $\nvdash A \supset \Box_k A$
  As always for the modality of validity.

- $\vdash \Box_k A \supset \Box_k \Box_k A$ – Axiom 4
  A desirable property – a principal consistently certifies that it has certifying authority over a principal.

- $\not\vdash \Box_k A \supset \Box_j \Box_k A$ – Axiom 4s
  4s is a desirable axiom to have in any system describing a reliable channel of communication, with a reliable method of authentication. In such a reliable system, every principal ought to be aware when a principal announces a signed statement.

Given our brief analysis, $\Box$ does not behave very much like name of the judgment it internalizes suggests. Furthermore, our inability to embed the GP logic in JM4 suggests that $\Box$ in its current form is not a useful operator. $\Diamond$ in its current form is a step backwards from the indexed lax modality.

- $\Diamond$ commutes in one direction with conjunction and disjunction, and not at all with implication except through $\Box$. This generally makes it clumsy to combines statements made by a principal using this modal operator. $\vdash \Box_j(A \supset B) \supset (\Diamond_k A \supset \Diamond_k B)$

- $\vdash \Box_j A \supset \Diamond_k A$
  The apparent lack of connection between the principals j and k is disturbing. At least, this property bodes ill for any interpretation as distributed computation or intuitionistic Kripke semantics.

- $\not\vdash \Diamond_k A \supset A$
  This is a desirable non-interference property.

The lack of correspondence between the *cert* assumption over which a principal claims ownership and the statements that it can *claim* or *affirm* is disturbing. It is one of the major problems to be addressed by the logic M4s. M4s is given its name because it satisfies the much stronger 4s axiom for $\Box$ whereas the logic in its current form satisfies only the 4 axiom. $\oint$ 2.3 documents a last-ditch effort to rescue M4 by giving it a tethered semantics and interpreting it as distributed computation with certain constraints imposed on principals. Though we derived a tethered calculus that admitted cut and identity, it was far from our expectations. Any readers who are uninterested in the details may skip to $\oint$ 3 without significantly affecting readability.

2.3 TM4: Tethered M4

Tethering as we use it modifies the calculus so that the hypotheses in the sequent never have to be deleted to express a sub-derivation. Instead, propositions are "tethered" to "worlds" that indicate where the assumption is accessible, and when it isn't. Our hope in moving towards a tethered semantics was to make the logic more syntactically friendly for distributed computation, or computation distributed amongst many "worlds". Among other benefits, the properties of tethering also allow an easier representation of the logic in a type theory such as LF or in other languages that support Higher Order Abstract Syntax. TM4 was inspired by both [Pfe10c] and [Ree06]. In the former, the sequent has the form:

$$\Gamma \Rightarrow A@w$$

where w was the current world from which assumptions could be used. The latter, which was designed to facilitate the complexities of linear logic had the judgment

$$\Gamma \Rightarrow @_p A$$

where p is a permission to use some resource in the context. These permissions were of the form

$$p \quad ::= \quad \epsilon \quad | \quad \alpha \quad | \quad p_1 * p_2$$

where the operator $*$ has ϵ as its unit and is commutative and associative. The tag with which formulae were tethered had this additional structure in order to express the complexities encountered with connectives in linear logic that split the context.

The connectives of JM4 have interesting effects. In addition to completely clearing the context Γ the way monomodal $\Box$ and $\Diamond$ do, they can have nested effects when restricting the context Δ. For example, consider a proof of the formula $\Box_i \Box_k A$. It can be easily verified using JM4 that such a formula never holds true unless A is a tautology because the sub-derivation of the innermost A has no hypotheses to work with. These effects require that every world that is tagged to a proposition adequately keeps track of every assumption in Δ along with the certifying principals in such a way that they can fetched or removed.

We have adapted and combined both of the techniques of tethering cited to get a sequent of the form

$$\Gamma \;\Rightarrow\; A@(w;P)$$

where Γ is a collection of hypothetical judgments (we will revisit the exact judgments contained in Γ soon), C is some proposition, w is the current world, and P is the current set of permissions. Specifically, P is defined as

$$P \quad ::= \quad \epsilon \quad | \quad (k,p) \quad | \quad P_1 * P_2$$

In addition to commutativity and associativity (which pertain to contexts that allow exchange), the permissions also need to support weakening and contraction.

Connectives in TM4

TM4 is described here by translating the fragment of JM4 containing $\Box_k$ and $\supset$. It is trivial to add disjunction and conjunction. Furthermore, $\Diamond_k$ does not merit a complete treatment here. TM4 is not the focus of our presentation, and the chosen connectives are sufficient to illustrate the complications that arise when attempting to interpret JM4.

The context Γ contains two different judgments. The first judgment is of the form $A@w$; that is, the assumption A usable at world w. This gives us the initial sequent

$$\frac{}{\Gamma, Q@w \;\Rightarrow\; Q@(w;P)}$$

meaning that if we have some atomic proposition Q (chosen as to not overlap with the permissions P) usable at world w, then we can prove Q at that world. The rules for implication are straightforward:

$$\frac{\Gamma, A_1@w \;\Rightarrow\; A_2@(w;P)}{\Gamma \;\Rightarrow\; A_1 \supset A_2@(w;P)} \supset R$$

$$\frac{\Gamma, A_1 \supset A_2@w \;\Rightarrow\; A_1@(w;P) \quad \Gamma, A_1 \supset A_2@w, A_2@w \;\Rightarrow\; C@(w;P)}{\Gamma, A_1 \supset A_2@w \;\Rightarrow\; C@(w;P)} \supset L$$

Note that in neither rule does P change. The rules for $\Box_k$, however, do make use of P, as does the copy rule.

$$\frac{\Gamma \;\Rightarrow\; A@(\alpha; P_k)}{\Gamma \;\Rightarrow\; \Box_k A@(w; P)}\,\Box R \qquad \frac{\Gamma, \Box_k A@w, A!\rho \;\Rightarrow\; C@(w; P*(k,\rho))}{\Gamma, \Box_k A@w \;\Rightarrow\; C@(w; P)}\,\Box L$$

By convention, ρ stands for a fresh permission, and α stands for a fresh world. A "fresh" variable is a name chosen so as not to collide with any worlds named in the context, or in the current set of permissions.

These rules introduce several new concepts to our logic. First, we have the other form of judgment that can appear in our context: $A!p$. This is meant to be similar to the judgment $A!$ presented in [Pfe10c], but with one caveat: in order to use A, we must have the corresponding permission ρ, which is stored in the permission context P. Now we need the other piece of syntax we defined, P_k, which is meant to be analogous to Δ_k from the judgmental multimodal logic presented earlier. It is defined as follows:

$$\begin{array}{rcl}(\epsilon)_k & = & \epsilon \\ ((k,p))_k & = & (k,p) \\ ((k',p))_k & = & (k,p) \text{ if } k \neq k' \\ (P_1 * P_2)_k & = & P_{1k} * P_{2k}\end{array}$$

Just like Δ_k, it traverses P, removing any permissions from it that do not belong to k. The copy rule, then, can be defined as

$$\frac{\Gamma, A!p, A@w \;\Rightarrow\; C@(w; P*(k,p))}{\Gamma, A!p \;\Rightarrow\; C@(w; P*(k,p))}\,\textit{copy}$$

The following meta-theorems are admissible over TM4:

Theorem 3. ***Admissibility of Cut for TM4***

i. If $\Gamma \;\Rightarrow\; A@(w;P)$ *and* $\Gamma, A \;\Rightarrow\; C@(w;P)$ *then* $\Gamma \;\Rightarrow\; C@(w;P)$.

ii. If $\Gamma \;\Rightarrow\; A@(\alpha;P_k)$ *and* $\Gamma, A!\rho \;\Rightarrow\; C@(w;P*(k,\rho))$ *then* $\Gamma \;\Rightarrow\; C@(w;P)$.

Theorem 4. ***Admissibility of Identity for TM4***
$\Gamma, A@w \;\Rightarrow\; A@(w;P)$ *for any context* Γ*, proposition* A*, world* w*, and permission context* P*.*

Due to the unusual structure of this calculus, we give a full statement of soundness and completeness of TM4 with respect to JM4. The proofs of these properties are listed in the appendix. The rest of this section does not significantly affect the readability of $\oint$ 3.

Theorem 5. ***Correctness of Translation from TM4 to JM4***
If $\Gamma \;\Rightarrow\; A@(w;P)$ *and* $\Gamma\{w;P\} = (\hat{\Delta};\hat{\Gamma})$*, then* $\hat{\Delta};\hat{\Gamma} \rightarrow A$ true*.*

Before we prove this, we must define the translation $\Gamma\{w;P\}$ from tethered contexts to judgmental contexts. This can be defined inductively as

$$\frac{}{(\cdot)\{w;P\} = (\cdot;\cdot)}$$

$$\frac{\Gamma\{w;P\} = (\hat{\Delta};\hat{\Gamma})}{\Gamma, A@w\{w;P\} = (\hat{\Delta};\hat{\Gamma}, A\ \mathit{true})} \qquad \frac{\Gamma\{w;P\} = (\hat{\Delta};\hat{\Gamma}) \quad w \neq w'}{\Gamma, A@w'\{w;P\} = (\hat{\Delta};\hat{\Gamma})}$$

$$\frac{\Gamma\{w;P\} = (\hat{\Delta};\hat{\Gamma}) \quad (k,p) \in P}{\Gamma, A!p\{w;P\} = (\hat{\Delta}, k\ \mathit{cert}\ A;\hat{\Gamma})} \qquad \frac{\Gamma\{w;P\} = (\hat{\Delta};\hat{\Gamma}) \quad (k,p) \notin P}{\Gamma, A!p\{w;P\} = (\hat{\Delta};\hat{\Gamma})}$$

Theorem 6. ***Correctness of Translation from JM4 to TM4***
Let $\ulcorner\Delta\urcorner = (\hat{\Delta};P)$*. If* $\Delta;\Gamma \rightarrow A$ true*, then* $\hat{\Delta}, \Gamma@\alpha \;\Rightarrow\; A@(\alpha;P)$*.*

Once again, this introduces some auxiliary judgments that we can define inductively. The first one, $\ulcorner\Delta\urcorner$, translates the judgmental knowledge context Δ into a list of assumptions $\hat{\Delta}$ of the form $A!p$, along with a permissions context P that contains all of the newly generated permissions in $\hat{\Delta}$ paired with the agents from which they came. The transformation $\Gamma@\alpha$ changes each assumption A in Γ to $A@\alpha$ for the same new world α.

$\ulcorner\Delta\urcorner$ is defined below.

$$\frac{}{\ulcorner\cdot\urcorner = (\cdot;\epsilon)} \qquad \frac{\ulcorner\Delta\urcorner = (\hat{\Delta};P)}{\ulcorner\Delta, k\ \mathit{cert}\ A\urcorner = (\hat{\Delta}, A!\rho; P * (k,\rho))}$$

Again, the proof of this is in the appendix.

3 The Logic M4s

It is possible to correct several of the shortcomings of M4 by slightly modifying the presented calculi to admit the 4s axiom. Therefore, the revised logic is called M4s. First, we present the judgmental sequent calculus JM4s. Following this, we present a tethered sequent calculus TM4s that we conjecture would be a useful addition to a type theory for distributed computation for the purposes of proof carrying authorization.

3.1 JM4s: Judgmental M4s

Two key insights derived from M4 influence the formulation of M4s: First, we need to track the "current principal" with whose certified assumptions a proof is derived, so that we may not have to delete assumptions from Δ. Second, truth is the modality that directly interacts with the definitions of $\Box$ and $\Diamond$. Therefore we also treat truth as an indexed modality. From these observations, a sequent of the following form emerges:

$$\Delta; \Gamma \xrightarrow{k} \gamma$$

Δ contains assumptions of the form $k\ \mathit{cert}\ A$ and Γ contains assumptions of the form $A\ \mathit{true}$, as in JM4. k simultaneously indexes the judgment on the right, and allows access to only those assumptions available to k. This change means that Γ is not just a context of locally available assumptions, but specifically a context designated for use in a particular proof by the current principal. As usual, γ is a place-holder referring to either a truth or a possibility. The `init` rule and the $\supset$ connective are recounted to illustrate the behavior of the sequent.

$$\frac{}{\Delta; \Gamma, A\ \mathit{true} \xrightarrow{k} A\ \mathit{true}}\ \texttt{init} \qquad \frac{\Delta; \Gamma, A\ \mathit{true} \xrightarrow{k} B\ \mathit{true}}{\Delta; \Gamma \xrightarrow{k} A \supset B\ \mathit{true}}\ \supset_R$$

$$\frac{\Delta; \Gamma, A \supset B\ \mathit{true} \xrightarrow{k} A\ \mathit{true} \quad \Delta; \Gamma, A \supset B\ \mathit{true}, B\ \mathit{true} \xrightarrow{k} \gamma}{\Delta; \Gamma, A \supset B\ \mathit{true} \xrightarrow{k} \gamma}\ \supset_L$$

The implication rules are quite predictable. The right rule introduces premises available to the same principal, and the left rule allows access to local assumptions so introduced. Next, we examine the rules pertaining to the *cert* modality:

$$\frac{\Delta, k\ \mathit{cert}\ A; \Gamma, A\ \mathit{true} \xrightarrow{k} \gamma}{\Delta, k\ \mathit{cert}\ A; \Gamma \xrightarrow{k} \gamma}\ \mathit{cert}$$

$$\frac{\Delta; \cdot \xrightarrow{k} A\ \mathit{true}}{\Delta; \Gamma \xrightarrow{j} \Box_k A\ \mathit{true}}\ \Box_R \qquad \frac{\Delta, k\ \mathit{cert}\ A; \Gamma, \Box_k A\ \mathit{true} \xrightarrow{j} \gamma}{\Delta; \Gamma, \Box_k A\ \mathit{true} \xrightarrow{j} \gamma}\ \Box_L$$

The *cert* rule only allows the current principal to instantiate and manipulate policies for which it is the certifying authority. The right rule delegates the sub-derivation to the principal internalized by $\Box_k$. Only the locally available assumptions, i.e. Γ are cleared. We depend on the *cert* rule to restrict access to Δ appropriately. The left rule allows *any* principal to become aware of certified policies available to other principals in the sub-derivation. This formulation admits the 4s axiom. The rules for $\Diamond$ are also updated.

$$\frac{\Delta;\Gamma \xrightarrow{k} A\ \mathit{true}}{\Delta;\Gamma \xrightarrow{k} A\ \mathit{poss}}\ \mathit{poss}$$

$$\frac{\Delta;\Gamma \xrightarrow{k} A\ \mathit{poss}}{\Delta;\Gamma \xrightarrow{i} \Diamond_k A\ \mathit{true}}\ \Diamond_R \qquad \frac{\Delta; A\ \mathit{true} \xrightarrow{k} C\ \mathit{poss}}{\Delta;\Gamma,\Diamond_k A \xrightarrow{k} C\ \mathit{poss}}\ \Diamond_L$$

Like $\Box_k$, $\Diamond_k$ delegates the sub-derivation to k to be proven using the policies controlled by k – and some local resource "shared" with it.

In addition to Weakening, Contraction and Exchange, the calculus JM4s satisfies the following meta-theoretical properties:

Theorem 7. ***Admissibility of Cut for JM4s***

i. *If* $\Delta;\Gamma \xrightarrow{k} A$ true *and* $\Delta;\Gamma, A$ true $\xrightarrow{k} \gamma$ *then* $\Delta;\Gamma \xrightarrow{k} \gamma$.

ii. *If* $\Delta;\cdot \xrightarrow{k} A$ true *and* Δ, k cert $A;\Gamma \xrightarrow{i} \gamma$ *then* $\Delta;\Gamma \xrightarrow{i} \gamma$.

iii. *If* $\Delta;\Gamma \xrightarrow{k} A$ poss *and* $\Delta; A$ true $\xrightarrow{k} C$ poss *then* $\Delta;\Gamma \xrightarrow{k} C$ poss.

Proof. By lexicographic induction, first on the size of the cut formula A, then on the on the ordering `(i) < (ii)` and `(i) < (iii)` of the induction hypotheses, and then simultaneously on the sizes of the two given derivations. □

Theorem 8. ***Admissibility of Identity for JM4s***

$\Delta;\Gamma, A$ true $\xrightarrow{k}$ A true *for any contexts* Δ *and* Γ*, any proposition* A*, and any principal* k*.*

Proof. By induction on the size of the proposition A. □

3.2 TM4s: Tethered M4s

Next, we present a tethered sequent calculus for M4s. Due to the more palatable proof theoretic behavior of M4s, translating to it is much simpler. It is quite similar to the tethered calculus for distributed computation presented in [Pfe10c], and elucidates the direct connection between M4s and distributed computation in a multi agent system.

Once again, we present a sequent calculus, and begin by describing the sequent:

$$\Gamma \;\Rightarrow\; A * (w, k)$$

A context Γ entails a proposition A at a world w, within the view of a principal k. $*$ as it occurs in the consequent of a sequent is a place-holder that refers to any of two tagging operations: @ and ?. $A@(w, k)$ means that A is true at the world w within the view of a principal k, and $A?(w, k)$ means that A is possible at the world with some constraints. They respectively correspond to the truth and possibility judgments in JM4s.

The context, which supports weakening, contraction and exchange, is defined as follows:

$$\Gamma ::= \quad \cdot \quad | \quad \Gamma, A@w \quad | \quad \Gamma, A!k$$

$A!k$ describes certificates available at any world, but within the view of a specific principal. $A@w$ describes truths available at a particular world for use in a proof.

The rules for $\Box$ are covered in detail in order to recapitulate the style in which tethered semantics is formulated in [Pfe10c].

$$\frac{\Gamma, A!k, A@w \;\Rightarrow\; C * (w, k)}{\Gamma, A!k \;\Rightarrow\; C * (w, k)}\;\texttt{copy}$$

$A!k$ refers to a hypothesis available at any world, and protected by k. The copy rule simply copies it to the current world provided we are in the view of k.

$$\frac{\Gamma \;\Rightarrow\; A@(\alpha, i)}{\Gamma \;\Rightarrow\; \Box_i A@(w, k)}\;\Box_R$$

In order to prove a boxed formula, the right rule needs to switch the view to the appropriate principal, and make all previously available local resources unusable. Instead of clearing any assumptions from the context, the sub-derivation is “moved” to a world about which no information was previously available. The world is denoted by the fresh variable α. The left rule, which appears next, should be self-explanatory.

$$\frac{\Gamma, \Box_i A@w, A!i \;\Rightarrow\; C * (w,k)}{\Gamma, \Box_i A@w \;\Rightarrow\; C * (w,k)}\ \Box_L$$

The rules for $\Diamond$ make the following straightforward translation to the tethered semantics. As usual, occurrences of α refer to fresh variables.

$$\frac{\Gamma \;\Rightarrow\; A@(w,k)}{\Gamma \;\Rightarrow\; A?(w,k)}\ \mathit{poss}$$

$$\frac{\Gamma \;\Rightarrow\; A?(w,k)}{\Gamma \;\Rightarrow\; \Diamond_k A@(w,i)}\ \Diamond_R \qquad \frac{\Gamma, \Diamond_k A@w, A@\alpha \;\Rightarrow\; C?(\alpha,k)}{\Gamma, \Diamond_k A@w \;\Rightarrow\; C?(w,k)}\ \Diamond_L$$

It is worth taking a moment to note the behavior of $\Diamond_R$. Every resource that was previously available as a truth in that world now becomes available to another principal. When policies are designed without care, this might lead to an unwarranted leakage of local resources to another principal. When designed correctly, it can be used to copy over specific resources protected and certified by a principal, and issuing these copies to another principal at a particular secure world as capabilities. Due to the behavior of the left rule, we can rest assured that these capabilities cannot be leaked to another world. To further understand this resource sharing, the logic may be enriched with a property similar to affirmation-flow [GP06]. A thorough treatment of flow is beyond the scope of this paper, but is likely to be simpler because indexed laxity has to respect many more constraints than indexed possibility in the left rule.

The following meta-theorems are admissible over Tethered M4s:

Theorem 9. ***Admissibility of Identity for TM4s***
$\Gamma, A@w \;\Rightarrow\; A@(w,k)$ for any context Γ, any proposition A, and an arbitrary principal k.

Proof. By induction on the size of the proposition A. □

Theorem 10. ***Admissibility of Strengthening for TM4s***
If $\Gamma \;\Rightarrow\; A@(w,k)$ then $\Gamma|_w \;\Rightarrow\; A@(w,k)$.

$\Gamma|_w$ is defined as follows:

$$\begin{aligned}
\cdot|_w &\equiv \cdot \\
\Gamma, A!k|_w &\equiv \Gamma|_w, A!k \\
\Gamma, A@w|_w &\equiv \Gamma|_w, A@w \\
\Gamma, A@w'|_w &\equiv \Gamma|_w \qquad\qquad w' \neq w
\end{aligned}$$

Proof. By induction on the structure of the given derivation. □

Strengthening tells us that we can discard any assumptions that can't be used in the current world. This theorem is instrumental in proving the next theorem.

Theorem 11. ***Admissibility of Cut for TM4s***

i. If $\Gamma \;\Rightarrow\; A@(w,k)$ and $\Gamma, A@w \;\Rightarrow\; C*(w,k)$ then $\Gamma \;\Rightarrow\; C*(w,k)$.

ii. If $\Gamma \;\Rightarrow\; A@(\alpha,k) \quad \alpha \notin \Gamma, \alpha \neq w$ and $\Gamma, A@w \;\Rightarrow\; C*(w,k)$ then $\Gamma \;\Rightarrow\; C*(w,k)$.

iii. If $\Gamma \;\Rightarrow\; A@(\alpha,k) \quad \alpha \notin \Gamma, \alpha \neq w$ and $\Gamma, A!k \;\Rightarrow\; C*(w,i)$ then $\Gamma \;\Rightarrow\; C*(w,i)$.

iv. If $\Gamma \;\Rightarrow\; A@(w,k)$ and $\Gamma, A@\alpha \;\Rightarrow\; C?(\alpha,k) \quad \alpha \notin \Gamma, \alpha \neq w$ then $\Gamma \;\Rightarrow\; C?(w,k)$.

Proof. By lexicographic induction, first on the size of the cut formula A, then on the on the ordering `(i) < (ii) < (iii)` and `(i) < (ii) < (iv)` of the induction hypotheses, and then simultaneously on the sizes of the two given derivations. □

The following is a formal statement of the equivalence between JM4s and TM4s.

Theorem 12. ***From JM4s to TM4s***

i. If $\Delta; \Gamma \xrightarrow{k} A$ true then $\Delta!, \Gamma@h \;\Rightarrow\; A@(h,k)$

ii. If $\Delta; \Gamma \xrightarrow{k} A$ poss then $\Delta!, \Gamma@h \;\Rightarrow\; A?(h,k)$

$\Delta!$ *is defined as follows:*

$$\cdot! \equiv \cdot$$
$$\Delta, k \text{ cert } A! \equiv \Delta!, A!k$$

$\Gamma@h$ *is defined as follows:*

$$\cdot! \equiv \cdot$$
$$\Gamma, A \text{ true}@h \equiv \Gamma@h, A@h$$

Proof. By simultaneous induction on the structure of the given derivation. □

Theorem 13. ***From TM4s to JM4s***

i. If $\Gamma \;\Rightarrow\; A@(h,k)$ *then* $\ulcorner \cdot; \cdot|\Gamma_h \urcorner; \xrightarrow{k} A \text{ true}$

ii. If $\Gamma \;\Rightarrow\; A?(h,k)$ *then* $\ulcorner \cdot; \cdot|\Gamma_h \urcorner; \xrightarrow{k} A \text{ poss}$

$\ulcorner \Delta, \Gamma|\Gamma'_h \urcorner$ *is defined as follows:*

$$\ulcorner \Delta; \Gamma|\cdot_h \urcorner \equiv \Delta; \Gamma$$
$$\ulcorner \Delta; \Gamma|(\Gamma', A!k)_h \urcorner \equiv \ulcorner \Delta, \text{cert}kA; \Gamma|\Gamma'_h \urcorner$$
$$\ulcorner \Delta; \Gamma|(\Gamma', A@h)_h \urcorner \equiv \ulcorner \Delta; \Gamma, A \text{ true}|\Gamma'_h \urcorner$$
$$\ulcorner \Delta; \Gamma|(\Gamma', A@w)_h \urcorner \equiv \ulcorner \Delta; \Gamma|\Gamma'_h \urcorner \quad w \neq h$$

Proof. By simultaneous induction on the structure of the given derivation. The strengthening theorem is key in permitting the use of the induction hypotheses. □

The translation and theorem are both straightforward, and resemble those given in [Pfe10c].

3.3 Admissible and Inadmissible Properties of M4s

Here are a few axioms and interaction rules in the logic that give a better intuition for the properties that we expect to be provable in the logic:

- $\Box$ has the usual interaction rules with the usual propositional connectives. It commutes in both directions with conjunction, one direction with implication and one direction with disjunction:

  - $\vdash \Box_k(A \supset B) \supset (\Box_k A \supset \Box_k B)$ – axiom K
  - $\vdash (\Box_k A \vee \Box_k B) \supset \Box_k(A \vee B)$

- $\nvdash \Box_k A \supset A$
  In a distributed computational interpretation, this means that a local resource cannot be arbitrarily preempted by a principal and have a claim of ownership placed on it. Additionally,when we substitute $\bot$ for A, we get a basic non-interference criterion.
- $\nvdash A \supset \Box_k A$
  As always for the modality of validity.
- $\vdash \Box_k A \supset \Box_j \Box_k A$ – Axiom 4s
- $\nvdash \Box_k A \supset \Box_k \Box_j A$

These properties resolve the problems we had in the logic M4 using $\Box$ as the operator that globally certifies a formula. In fact $\Box_k s$ as presented in JM4s is equivalent to k `says` s of BL found in Deepak Garg's dissertation [Gar09]. The same work contains an in-depth justification of why the given behavior for $\Box$ or `says` is desirable, and further illustrates the utility of such an operator in a proof carrying file system. Next, we consider some interaction rules concerning $\Diamond$

- $\Diamond$ also has all the usual interaction rules with the usual propositional connectives. It commutes in one direction with conjunction and disjunction, and not at all with implication except through $\Box$. $\vdash \Box_k(A \supset B) \supset (\Diamond_k A \supset \Diamond_k B)$ – axiom K
- $\vdash \Box_k A \supset \Diamond_k A$ – Axiom D
  Unlike in M4, the indices must be the same. Computationally, this links $\Box$ and $\Diamond$ inextricably via their indices. The former becomes a strictly stronger operation, because in a system with at least one world, any globally valid certificate can be used in some specific world.
- $\nvdash \Diamond_k A \supset \Diamond_j \Diamond_k A$
- $\vdash \Diamond_k A \supset \Diamond_k \Diamond_j A$

These properties resolve the strange lack of correlation in M4 in the manner in which the two modalities were indexed. The last two properties are significantly different from those of box modality. Computationally, the lack of 4s says that proofs that require local resources cannot be freely delegated on a global level. The presence of its counterpart, however, tells us that in a particular world, a principal k can delegate a proof to another principal j while locally issuing capabilities to j for resources otherwise accessible only to k.

4 Conclusions and Future Work

We have presented a logic M4s, and a tethered calculus for it called TM4s. This logic replicates some of the functionality of BL, but also gives a simple reinterpretation of the same functionality in the context of distributed computation. We did not consider many features that would make TM4s practical, such as first order quantification over principals, and a notion of time. However, in hindsight, all of these extensions can be added as done in [Gar09]. The main contribution of this paper is an interpretation of the $\Diamond_k$ modal operator in authorization logic, and an interpretation in a distributed framework due to the connection with intuitionistic Kripke semantics and tethered semantics.

We see some potential applications for a logic like TM4s:

- A system of natural deduction for TM4s can be used as a type theory for a distributed computation, in which data and proofs of authorization are treated uniformly in the language. PCML5 (proof carrying ML5) is such a recently proposed programming language that extends ML5, a language for distributed computing, with the GP logic for PCA [KAH10]. We believe that TM4s is more naturally suited to the semantics of authorization in a distributed system, and overlaps more nicely with the type system of ML5.
- If TM4s were to be extended with linear logic, and given a notion of consumable credentials (similar to BL^L from [Gar09], the resulting logic could be applied to distributed computation as an abstraction for mutual exclusion and other synchronization primitives.

We leave it to future work to explore these possibilities.

A Theorems from $\oint$ 2

5: Translating TM4 to JM4

The proof for a fragment of the language is given here:

Case:

$$\frac{\Gamma \;\Rightarrow\; A@(\alpha; P_k)}{\Gamma \;\Rightarrow\; \Box_k A@(w;P)}\;\Box R$$

Our inductive hypothesis gives us

$$\hat{\Gamma}; \hat{\Delta} \rightarrow A$$

where $\Gamma\{\alpha; P\} = (\hat{\Delta}; \hat{\Gamma})$. By the definition of $\Gamma\{\alpha; P_k\}$, we know that $\hat{\Gamma}$ is just $\cdot$ since α is a fresh world. In addition, since P_k must only have permissions for k in it, $\hat{\Delta}$ must only have assumptions for k in it.

We are trying to prove $\hat{\Delta}'; \hat{\Gamma}' \rightarrow \Box_k A$, where $\Gamma\{w; P\} = (\hat{\Delta}'; \hat{\Gamma}')$. We know that $\hat{\Delta}$ to be a subset of $\hat{\Delta}'$ (specifically, $\hat{\Delta}' = \hat{\Delta}_k$).

Lemma 1. *If* $\Gamma\{w; P\} = (\hat{\Delta}; \hat{\Gamma})$*, then* $\Gamma\{\alpha; P_k\} = (\hat{\Delta}_k; \cdot)$*.*

Proof: by induction on the definitions of $\Gamma\{w; P\}$, P_k, and Δ_k.

This gives us the derivation

$$\cfrac{\cfrac{\hat{\Delta}; \hat{\Gamma} \rightarrow A}{\hat{\Delta}'_k; \cdot \rightarrow A}\;defn}{\hat{\Delta}'; \hat{\Gamma}' \rightarrow \Box_k A}\;\Box R$$

Case:

$$\frac{\Gamma, \Box_k A@w, A@\rho \;\Rightarrow\; C@(w; P * (k, \rho))}{\Gamma, \Box_k A@w \;\Rightarrow\; C@(w; P)}\;\Box L$$

Our inductive hypothesis gives us

$$\hat{\Delta}, k\; \mathit{cert}\; A; \hat{\Gamma}, \Box_k A \rightarrow C$$

which allows us to construct the derivation

$$\frac{\hat{\Delta}, k\; \mathit{cert}\; A; \hat{\Gamma}, \Box_k A \rightarrow C}{\hat{\Delta}; \hat{\Gamma}, \Box_k A \rightarrow C}\;\Box L$$

Case:

$$\frac{\Gamma, A!p, A@w \;\Rightarrow\; C@(w; P * (k, p))}{\Gamma, A!p \;\Rightarrow\; C@(w; P * (k, p))}\;\mathit{copy}$$

Our inductive hypothesis gives us

$$\hat{\Delta}, k\ \mathit{cert}\ A; \hat{\Gamma} \to C$$

We can now construct the derivation

$$\frac{\hat{\Delta}, k\ \mathit{cert}\ A; \hat{\Gamma} \to C}{\hat{\Delta}, k\ \mathit{cert}\ A; \hat{\Gamma}, A \to C}\ \mathit{copy}$$

6: Translating JM4 to TM4

The proof for a fragment of the language is given here:
Case:

$$\frac{\Delta_k; \cdot \to A}{\Delta; \Gamma \to \Box_k A}\ \Box R$$

By our inductive hypothesis, we get

$$\hat{\Delta_k} \ \Rightarrow\ A@(\alpha; P_1)$$

where $\ulcorner \Delta_k \urcorner = (\hat{\Delta_k}, P_1)$. We also have $\ulcorner \Delta \urcorner = (\hat{\Delta}, P)$, and by the definition of $\ulcorner \Delta \urcorner$ we get that $P_k = P_1$. This gives us the derivation

$$\frac{\dfrac{\hat{\Delta_k} \ \Rightarrow\ A@(\alpha; P_1)}{\hat{\Delta}, \Gamma@w \ \Rightarrow\ A@(\alpha; P_1)}\ \mathit{weakening}}{\hat{\Delta}, \Gamma@w \ \Rightarrow\ \Box_k A@(w; P)}\ \Box R$$

Case:

$$\frac{\Delta, k\ \mathit{cert}\ A; \Gamma, \Box_k A \to C}{\Delta; \Gamma, \Box_k A \to C}\ \Box L$$

By our inductive hypothesis, we get

$$\hat{\Delta}, A!\rho, \hat{\Gamma}, \Box_k A@\alpha \ \Rightarrow\ C@(\alpha; P * (k, \rho))$$

allowing us to construct the derivation

$$\dfrac{\hat{\Delta}, A!\rho, \hat{\Gamma}, \Box_k A@\alpha \;\Rightarrow\; C@(\alpha; P * (k,\rho))}{\hat{\Delta}, \hat{\Gamma}, \Box_k A@\alpha \;\Rightarrow\; C@(\alpha; P)}\ \Box L$$

Case:

$$\dfrac{\Delta, k\ \mathit{cert}\ A; \Gamma, A \to C}{\Delta, k\ \mathit{cert}\ A; \Gamma \to C}\ \mathit{copy}$$

By our inductive hypothesis, we get

$$\hat{\Delta}, A!\rho, \hat{\Gamma}, A@\alpha \;\Rightarrow\; C@(\alpha; P * (k,\rho))$$

allowing us to construct the derivation

$$\dfrac{\hat{\Delta}, A!\rho, \hat{\Gamma}, A@\alpha \;\Rightarrow\; C@(\alpha; P * (k,\rho))}{\hat{\Delta}, A!\rho, \hat{\Gamma} \;\Rightarrow\; C@(\alpha; P * (k,\rho))}\ \mathit{copy}$$

References

[AF99] Andrew Appel and Edward Felten. Proof-carrying authentication. In *Proceedings of the 6th ACM conference on Computer and communications security*, pages 52–62, Kent Ridge Digital Labs, Singapore, 1999. ACM, New York, NY, USA.

[DLK+06] Deepak Garg, Lujo Bauer, Kevin Bowers, Frank Pfenning, and Michael Reiter. A linear logic of affirmation and knowledge. In J. Meier D. Gollman and A. Sabelfeld, editors, *Proceedings of the 11th European Symposium on Research in Computer Security (ESORICS'06)*, pages 297–312, Hamburg, Germany, September 2006.

[Gar09] Deepak Garg. *Proof Theory for Authorization Logic and its Application to a Practical Filesystem*. PhD thesis, Carnegie Mellon University, 2009.

[GP06] Deepak Garg and Frank Pfenning. Non-interference in constructive authorization logic. In J. Guttman, editor, *Proceedings of the 19th Computer Security Foundations Workshop (CSFW'06)*, pages 283–293, Venice, Italy, July 2006. IEEE Computer Society.

[KAH10] Anupam Datta Kumar Avijit and Robert Harper. Distributed programming with distributed authorization. In *Proceedings of the 5th ACM SIGPLAN workshop on Types in language design and implementation*, pages 27–38. ACM, New York, NY, USA, 2010.

[LJK$^+$08] Limin Jia, Jeffrey A. Vaughan, Karl Mazurak, Jianzhou Zhao, Luke Zarko, Joseph Schorr, and Steve Zdancewic. Aura: a programming language for authorization and audit. In *ACM SIGPLAN notices*, volume 43, pages 27–38. 2008.

[Mur08] Tom Murphy VII. *Modal Types for Mobile Code*. PhD thesis, Carnegie Mellon University, 2008.

[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.

[Pfe10a] Frank Pfenning. Lecture notes on intuitionistic kripke semantics, March 2010.

[Pfe10b] Frank Pfenning. Lecture notes on modal sequent calculus, February 2010.

[Pfe10c] Frank Pfenning. Lecture notes on tethered semantics, March 2010.

[Ree06] Jason Reed. Hybridizing a logical framework. *Electr. Notes Theor. Comput. Sci.*, 174(6):135–148, 2006.