Partially-ordered Modalities

Gerard Allwein and William S. Harrison

24 August 2010

Introduction

- Logic Systems
  - Hilbert
  - Gentzen
- Models
  - Frames
  - General Frames
  - Morphisms
- Channel Theory
  - Basic Channel Theory
  - Simulations
- Security
- Current Work

The Modal Hilbert System $(H, \geq)$

We use the usual substrate with a normality axiom (but this latter is not essential):

- *C:* the axioms of classical propositional logic;
- *N:* the axiom $[h](A \to B) \to ([h]\, A \to [h]\, B), h \in H$,

In addition, we add the following simple axiom:

A1: $[k]\, A \to [h]\, A$ for $k \geq h$ and $k, h \in H$.

and the rules

$$\frac{A \in \Gamma}{\Gamma \vdash A}\ rep \qquad \frac{\Gamma \vdash A \qquad \Gamma \vdash A \to B}{\Gamma \vdash B}\ mp \qquad \frac{\vdash A}{\vdash [h]\, A}\ gen$$

and $\langle h \rangle\, A$ can be defined as $\neg\, [h]\, \neg A$.

The Modal Hilbert System $\mathbf{S4}$ *with* $(H, \geq)$

To axiomitize $\mathbf{S4}$, one adds the usual axioms:

A2 $[h]\,A \to A$.

A3 $[h]\,A \to [h]\,[h]\,A$.

Axioms A1 and A3 may be replaced with:

A3' $[k]\,A \to [h]\,[k]\,A$, $k \geq h$.

The axiom A1 is the axiom that codes the partial order, it may also be expressed using possibility as:

A1' $\langle k \rangle\,A \to \langle h \rangle\,A$ for $k \leq h$.

The Modal Hilbert System $\mathbf{S4}$ *with* $(H, \geq)$, *Continued*

There are two derived rules for the Hilbert-system when proofs are allowed to have assumptions, the usual deduction theorem and an extension of gen.

Theorem 1 (Gen). The classical deduction theorem continues to hold and an expanded gen rule is a derived rule of the Hilbert-style system:

$$[k_1]\, B_1, \ldots, [k_n]\, B_n \vdash A \text{ implies}$$
$$[k_1]\, B_1, \ldots, [k_n]\, B_n \vdash [h]\, A,\ k_i \geq h.$$

The Modal Gentzen System **S4** *with* $(H, \geq)$

- The usual Gentzen rules for propositional logic;
- The *active formula*is the formula newly introduced.
- The *modal class* of a formula is either necessary, possible, or neutral.
- The Modal Condition
  - all formulae on the same side of the $\vdash$ as the active formula must have the opposite modal class as the active formula,
  - all formulae on the opposite side of the $\vdash$ as the active formula must have the same modal class as the active formula.

The Modal Gentzen System **S4** *with* $(H, \geq)$*, Continued*

- Partially Ordered Modal Condition (NC)

$$MC \text{ and } \forall C \in \Gamma \cup \Delta . c(C) \geq h$$

where $c(C)$ is the "closure" value of a formula using the modal partial order.

$$\frac{\Gamma, A \vdash \Delta \qquad NC}{\Gamma, \langle h \rangle A \vdash \Delta} \langle h \rangle \vdash \qquad\qquad \frac{\Gamma \vdash \Delta, B}{\Gamma \vdash \Delta, \langle h \rangle B} \vdash \langle h \rangle$$

$$\frac{\Gamma \vdash \Delta, A \qquad NC}{\Gamma \vdash \Delta, [h] A} \vdash [h] \qquad\qquad \frac{\Gamma, A \vdash \Delta}{\Gamma, [h] A \vdash \Delta} [h] \vdash$$

The Modal Gentzen System **S4** *with* $(H, \geq)$*, Cut Elimination*

Theorem 2 (Cut Elimination). *The cut rule can be eliminated from the Gentzen system.*

Theorem 3 (Presentation Equivalence). *The Hilbert system and the Gentzen system present the same logic.*

Kripke Frames

- $(X, (\mathcal{R}, \geq))$:
  - X is a collection of points (worlds, states, etc.);
  - $(\mathcal{R}, \geq)$ is a partial order of binary relations;
  - $R_h \subseteq R_k$ is presented as $k \geq h$.
- Monotonicity: $R_h xy$ and $k \geq h$ implies $R_k xy$.

In addition, for $\mathbf{S4}$, the following axioms are added

- Reflexivity: $R_h xx$
- Transitivity: $R_h zx$ and $R_h xy$ implies $R_h zy$.

One can also take, in place of Monotonicity and Transitivity:

- Transitivity + Monotonicity: for $k \geq h$,
  $R_k yz \text{ and } R_h xy \text{ implies } R_k xz$.

Valuations and Soundness

The modalities are evaluated using the usual prescription from modal logic:

$$x \models \langle h \rangle P \text{ iff } \exists y. R_h xy \text{ and } y \models P$$
$$x \models [h] P \text{ iff } \forall y. R_h xy \text{ implies } y \models P.$$

It follows easily that: $[h] \neg P = \neg \langle h \rangle P$.

Theorem 4 (Soundness). Partially-ordered modal logic is sound with respect to the partially ordered models.

Canonical Representations and Competeness

Definition 5 (Canonical Frame). Let (A, H) be a modal algebra (Boolean lattice with partially ordered normal modalities),

- Worlds are maximal filters;
- $R_h xy$ iff $[h]\, a \in x$ implies $a \in y$;
- $[k]\, a \leq [h]\, a$ implies $R_h \subseteq R_k$.

Definition 6 (Canonical Representation). For A a set of maximal filters of the modal algebra,

$$[h]\, A = \{x \mid \forall y. R_h xy \text{ implies } y \in A\}$$
$$\langle h \rangle\, A = \{x \mid \exists y. R_h xy \text{ and } y \in A\}$$

Theorem 7 (Completeness). Partially-ordered modal logic is complete with respect to the partially ordered models.

General Frames

A *general frame* is a structure $\mathbb{X} = (X, R, A)$:

- (X, R) is a Kripke frame
- A is a collection of *admissible*subsets of X
- A is closed under the Boolean operations and under the operation $\langle R \rangle : \mathcal{P}(X) \to \mathcal{P}(X)$ given by:

$$\langle R \rangle C \overset{def}{=} \{y \in X \mid Ryx \text{ for some } x \in X\}.$$

General frames are defined in monadic second-order logic.

General Frames Continued

A general frame $(X, (\mathcal{R}, \geq), X_*)$ a Kripke frame and X_* is closed under derived modal operators using the prescriptions for $[h]\, A$ and $\langle h \rangle\, A$:[1]

- *differentiated* if for all $x, y \in X$ with $x \neq y$, there is a 'witness' $a \in X_*$ such that $x \in a$ and $y \notin a$;
- *tight* if whenever y is not an R_h-successor (for $R_h \in \mathcal{R}$) of x, there a 'witness' a such that $y \in a$ and $x \notin \langle R_h \rangle\, a$;
- *compact* if for every $C \subseteq X_*$, if C has the finite intersection property, then $\bigcap C \neq \emptyset$.

A general frame is *descriptive* if it is differentiated, tight, and compact.

[1] Following "Stone Coalgebras" by Kupke, Kurz, and Venema (and Goldblatt originally)

General Frames Continued

- X_* is the clopen basis for the Stone topology on the Kripke frame.
- The identity modal operator $[1_X]$ corresponds to the identity relation on X, and $[1_X]\,C = \langle 1_X \rangle\,C$ for all elements of X_* (or propositions) C.

All partial orders of relations can be extended with this relation with little effect on the dual algebras.

Lemma 8 (Clopen Sets). *For all C, $[1_X]\,C = C = \langle 1_X \rangle\,C$.*

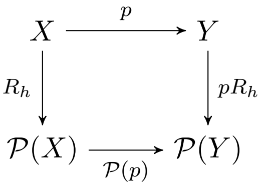
p-morphisms

The coalgebra for Kripke relation R in $\mathbb{X} = (X, (\mathcal{R}, \geq))$ is defined with:

$$R_h x = \{y \mid R_h xy\}$$

(where the symbol R_h is overloaded).

(forgetting the partial order for the moment) p is a p-morphism when the square commutes:



- $R_h xy$ implies $(pR_h)(px)(py)$;
- $(pR_h)(px)y$ implies there is some z such that $R_h xz$ and $pz = y$.

General Frame Morphisms

Denote the category of all coalgebras on $\mathbb{X}$ with $\mathsf{Coalg}(\mathbb{X})$:

- Partially order the relations which partially orders the relations as coalgebra morphisms.
- $\mathsf{Coalg}(\mathbb{X})$ then forms a simple category.
- A morphism of frames $p : \mathbb{X} \to \mathbb{Y}$ then can be expected to be p-morphism for all the relations of $\mathbb{X}$ with the additional constraint that it also be a morphism $p : \mathsf{Coalg}(\mathbb{X}) \to \mathsf{Coalg}(\mathbb{Y})$.
- A morphism $p : \mathbb{X} = (X, (\mathcal{R}, \geq), X_*) \to \mathbb{Y} = (Y, (\mathcal{S}, \geq), Y_*)$ is a general frame morphism if
    - it is a morphism for partially ordered frames, and
    - $p^{-1} : Y_* \to X_*$ is a modal homomorphism.
    - General frame morphisms are also descriptive frame morphisms.

Channel Theory

- Objects are classifications: $\boldsymbol{X}$
  - Types: $\mathit{Typ}(\boldsymbol{X})$
  - Tokens: $\mathit{Tok}(\boldsymbol{X})$
  - Satisfaction: $x \models_{\boldsymbol{X}} P$ for x a token and P a type.
- Infomorphisms: $f : \boldsymbol{X} \to \boldsymbol{Y}$

$$\begin{array}{ccc} \mathit{Typ}(\boldsymbol{X}) & \xrightarrow{\hat{f}} & \mathit{Typ}(\boldsymbol{Y}) \\ {\scriptstyle \models_{\boldsymbol{X}}} \Big| & & \Big| {\scriptstyle \models_{\boldsymbol{Y}}} \\ \mathit{Tok}(\boldsymbol{X}) & \xleftarrow[\check{f}]{} & \mathit{Tok}(\boldsymbol{Y}) \end{array}$$

satisfying

$$\check{f}x \models_{\boldsymbol{X}} P \text{ iff } f \models_{\boldsymbol{Y}} \hat{f}P$$

Theory in a Classification

- Gentzen sequents of types: $\Gamma \Vdash_{\boldsymbol{X}} \Delta$
- Γ conjunctive, Δ disjunctive
- Classical rules
  - Reflexivity

$$P \Vdash_{\boldsymbol{X}} P$$

  - Thinning

$$\frac{\Gamma \Vdash_{\boldsymbol{X}} \Delta}{\Gamma, \Gamma' \Vdash_{\boldsymbol{X}} \Delta, \Delta'}$$

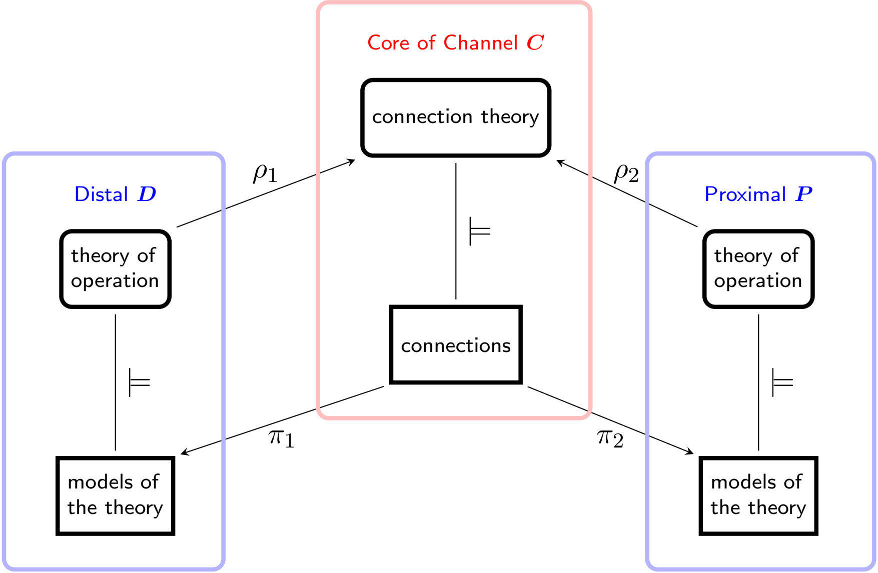
  - Global Cut: for any $\Theta \subseteq \mathit{Typ}(\boldsymbol{X})$,

$$\frac{\Gamma, \Sigma_1 \Vdash_{\boldsymbol{X}} \Sigma_2, \Delta \quad \text{all partitions } \langle \Sigma_1, \Sigma_2 \rangle \text{ of } \Theta}{\Gamma \Vdash_{\boldsymbol{X}} \Delta}$$

- Given $f : \boldsymbol{X} \to \boldsymbol{Y}$, f preserves validity and reflects non-validity,

$$\frac{\Gamma \Vdash_{\boldsymbol{X}} \Delta}{\Gamma^f \Vdash_{\boldsymbol{Y}} \Delta^f}(f\text{--}Intro) \qquad \frac{\Gamma^f \Vdash_{\boldsymbol{Y}} \Delta^f}{\Gamma \Vdash_{\boldsymbol{X}} \Delta}(f\text{--}Elim)$$

Binary Channel $\boldsymbol{C}$



Theory in the Channel

- All the classical rules
- Connection sequents of the form

$$\Gamma^{\rho_1} \Vdash_{\boldsymbol{C}} \Delta^{\rho_2}$$

for $\Gamma^{\rho_1}, \Delta^{\rho_2}$ the forward images of Γ and Δ along ρ_1 and ρ_2.

This can be used to underwrite information flow:

$x \models_{\mathbf{D}} \Gamma$	iff $\pi_1\langle x, y\rangle \models_{\mathbf{D}} \Gamma$	assumption
	iff $\langle x, y\rangle \models_{\mathbf{C}} \Gamma^{\rho_1}$	infomorphism condition
	implies $\langle x, y\rangle \models_{\mathbf{C}} \Delta^{\rho_2}$	channel constraint
	iff $\pi_2\langle x, y\rangle \models_{\mathbf{P}} \Delta$	infomophism condition
	iff $y \models_{\mathbf{P}} \Delta$	assumption

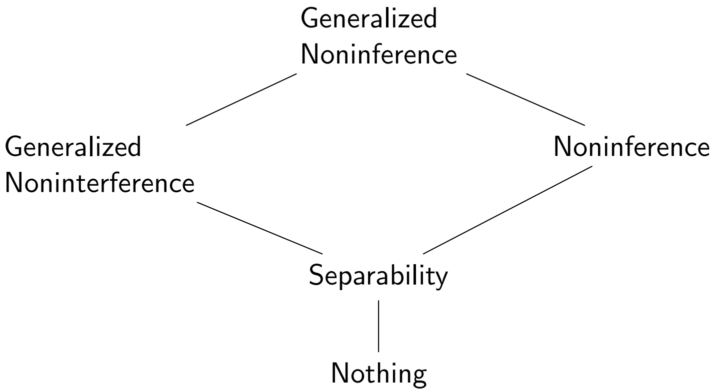
Simulation via a Channel

- Proximal $A' \Vdash [h]\, B'$ transforms to distal $A \Vdash [h]\, B$;
- Note the two languages at Proximal and Distal are different.
- The connections in the channel are a simulation relation.
- The connection theory in $\mathbf{C}$ relates non-modal proximal and distal types:
  - The connection theory in $\mathbf{C}$ relates non-modal proximal and distal types.
  - The projection π_1 is surjective, i.e., must cover $Tok(\mathbf{D})$.
  - $\mathbf{P}$ simulates $\mathbf{D}$ via the channel tokens $Tok(\mathbf{C})$.

Theorem 9 (Simulation). For channel $\mathbf{C}$, if $\mathbf{P}$ simulates $\mathbf{D}$, $\rho_1 A \Vdash_{\mathbf{C}} \rho_2 A'$, and $\rho_2 B' \Vdash_{\mathbf{C}} \rho_1 B$:

$$\left(A' \Vdash_{\mathbf{P}} [h']\, B'\right) \text{ implies } \left(A \Vdash_{\mathbf{D}} [h]\, B\right).$$

The Partial Order of Possibilistic Security Properties



Possibilistic Security Properties

Two security domains, High and Low, both with Inputs and Outputs:

- Separability: given a particular trace of high's behavior, any trace of low's behavior is possible, and vice versa.
- Generalized Noninterference: any high-level trace is co-possible with any low-level trace, and *when only high-level input is considered* any low-level trace is co-possible with any high-level trace.
- Noninference "purges" high information from the input and output traces by overwriting that information.
- Generalized Noninference: only high input is purged.

Possibilistic Security Properties, Continued

- Each property can be described as a system's behavior being closed under a particular kind of interleaving functions.
- Closure under a collection of functions can be considered closure in a topological space.
- Closures can be apprehended using $S4$ modalities.
- These modalities must be partially ordered.
- The diagram looks like a lattice but it is not; those are not joins and meets but merely upper and lower bounds.

Current Work

- The entire relational algebra will yield joins and meets.
- The partial order is used to pick out the coalgebras that are relevant to a particular application.
- One could outfit the relations with a Directed, Complete Partial Order structure (DCPO) and use notions of computation.

Current Work, Continued

- The algebra of coalgebras uses Composition, Converses, and the Identity relation.
- These can be used to specify

Modal System	Relation Condition	Modal Axiom	Kleisli condition
D	serial	$\Box A \to \Diamond A$	$I \leq \alpha^* \circ \alpha^{-1}$
T	reflexive	$\Box A \to A$	$I \leq \alpha$
B	symmetric	$A \to \Box \Diamond A$	$\alpha \leq \alpha^{-1}$
$T4$	transitive	$\Box A \to \Box \Box A$	$\alpha^* \circ \alpha \leq \alpha$
$T5$	Euclidian	$\Diamond A \to \Box \Diamond A$	$\alpha^* \circ \alpha^{-1} \leq \alpha$

- Now we can make morphisms respect these conditions so that, say, $S4$ relations are taken to $S4$ relations.

Current Work, Continued

- Not all conditions we'd like to preserve are first-order logic conditions, some are monadic second-order, i.e., well-founded relations, induction (for action logic), etc.
- What kind of categorical structure must we have to specify these?
- Categorical sketches with formal 2-cells is necessary for the algebra of coalgebras.
- We need to incorporate the functor so we are specifying an algebra of coalgebras and not any old algebra.