A Protocol Logic

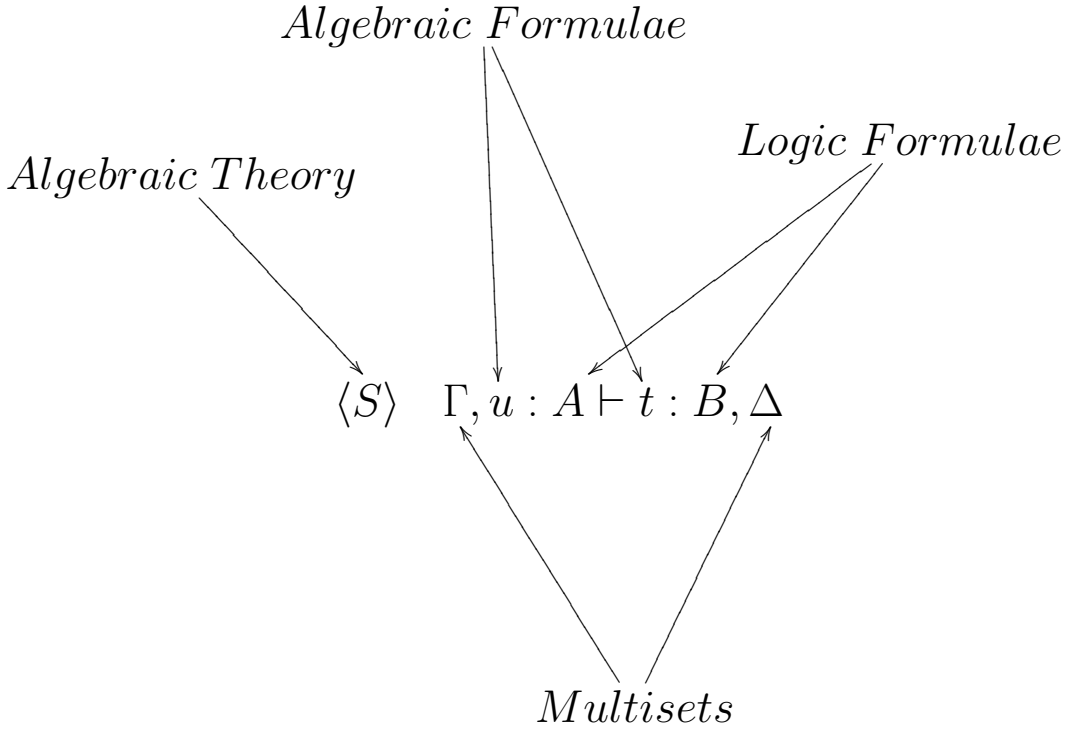
Gerard Allwein
Center for High Assurance Computer Systems
U.S. Naval Research Laboratory

Abstract

This paper presents a quantificational logic for protocols based on a spatial logic of Caires and Cardelli called "A spatial logic for concurrency: Parts I & II". The presentation is through a Gentzen system which implements a labeled deductive system. The labels are processes as specified via the π–calculus. The logic can be seen as combination of classical logic, linear logic, and modal logic in that it inherits some of the connectives of each.

Gentzen Sequents

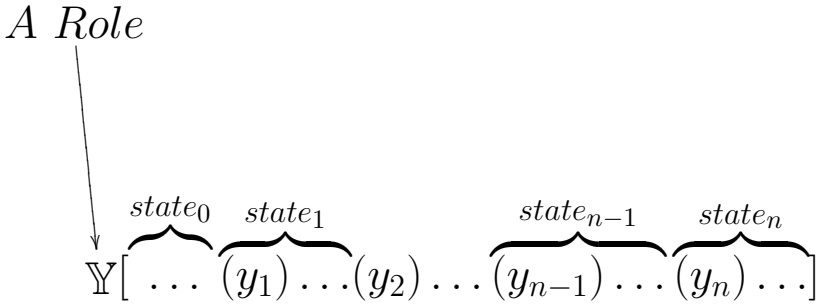
The formal logic has a Gentzen formulation where sequents are of the form



What is fixed? Ans: Nothing, really, but we will fixate on the π–calculus for the algebraic theory, logic analogues of π–calculus formulae, and classical logic for the Predicates. Hence, the formal logic contains classical logic and some other connectives inspired by the π–calculus. The extra connectives appear in other non-standard logics.

Local State vs. Global State

Definition 1 *A* **state** *is a region from either the beginning of the protocol or anything including the last message reception up to the next receipt. In hack notation, this appears as*



Let each protocol role be segregated into states.

π–Calculus vs. Logical Machinery

π–Calculus Notions	Logical Notions
Parallel $\mid$ operator	Intensional, symmetric conjunction $\circ$
Sequential $\cdot$ operator	Intensional, non–symmetric conjunction $\cdot$
Send formulae	Send formulae
Receive formulae	Send formulae, entailment $\multimap$ and local modal quantifiers
Reduction of terms	Proof structure
	Predicates
	Quantifiers
	Boolean connectives

Encoding reception:

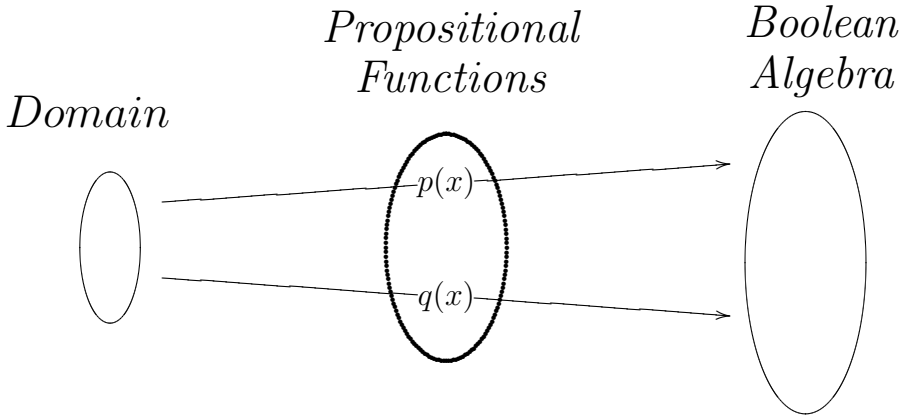
$$x(y) \cdot A \stackrel{def}{=} \forall y.x\langle y\rangle \multimap \Diamond A.$$

from Caires and Cardelli is replaced with

$$x(y) \cdot A \stackrel{def}{=} \mathbb{Y}\, y.\langle y\rangle \multimap A$$

Definition 2 *A sequential formula is any formula of the logic not containing the* $\circ$ *connective.*

Note: We are not using the whole π-calculus as Caires and Cardelli do, but hope to eventually.



To induce a Boolean algebra structure on the *Propositional Functions*, define

$$(p \wedge q)(x) \stackrel{def}{=} p(x) \wedge q(x)$$
$$(p \vee q)(x) \stackrel{def}{=} p(x) \vee q(x)$$
$$(\neg p)(x) \stackrel{def}{=} \neg p(x)$$

A quantifier, say, $\forall$, is an operator on the function space:

$$\forall : Prop.\ Fcns \longrightarrow Constant\ Prop.\ Fcns.$$

meeting certain axioms. Consequently, $\forall$ looks like a modal operator on a Boolean algebra of propositional functions.

Kripke Frames for Quantifiers: $(W, K_1, \ldots, K_n)$ where W is a collection of interpretations and the K_i's are equivalence relations on the interpretations.

Kripke Frames for Local Modal Quantifiers: $(W, \mathbb{Y}_1, \ldots, \mathbb{Y}_n)$ where W is a collection of worlds and the $\mathbb{Y}_i$'s are binary relations on the worlds used to interpret local modal quantifiers $\mathbb{Y}_1$, $\mathbb{Y}_2$, etc.

Sequencing Conjunction Rules:

$$\frac{[A \textit{ is a sequential formula}] \quad \langle S, u \doteq \mathcal{X} \cdot \mathcal{X}' \rangle \quad \Gamma, \mathcal{X} : A, \mathcal{X}' : B \vdash \Delta}{\langle S \rangle \quad \Gamma, u : A \cdot B \vdash \Delta} \cdot \vdash$$

$$\frac{[A \textit{ is a sequential formula}] \quad \langle S \rangle \quad \Gamma_1 \vdash v : A, \Delta_1 \quad \langle S \rangle \quad \Gamma_2 \vdash t : B, \Delta_2 \qquad u \doteq_S v \cdot t}{\langle S \rangle \quad \Gamma_1, \Gamma_2 \vdash u : A \cdot B, \Delta_1, \Delta_2} \vdash \cdot$$

Parallel Conjunction Rules:

$$\frac{\langle S, u \doteq \mathbb{X}[\mathcal{X}] \mid \mathbb{Y}[\mathcal{Y}] \rangle \quad \Gamma, \mathcal{X} : A, \mathcal{Y} : B \vdash \Delta}{\langle S \rangle \quad \Gamma, u : \mathbb{X}[A] \circ \mathbb{Y}[B] \vdash \Delta} \circ \vdash$$

$$\frac{\langle S \rangle \quad \Gamma_1 \vdash s : A, \Delta_1 \quad \langle S \rangle \quad \Gamma_2 \vdash t : B, \Delta_2 \qquad u \doteq_S \mathbb{X}[v] \mid \mathbb{Y}[t]}{\langle S \rangle \quad \Gamma_1, \Gamma_2 \vdash u : \mathbb{X}[A] \circ \mathbb{Y}[B], \Delta_1, \Delta_2} \vdash \circ$$

Modal Quantifier Rules:

$$\frac{\langle S, u \xrightarrow{y \leftarrow x} \mathcal{X} \rangle \quad \Gamma, \mathcal{X} : A\{y \leftarrow x\} \vdash \Delta}{\langle S \rangle \quad \Gamma, u : \mathbb{Y}\, y.A \vdash \Delta}\ \mathbb{Y} \vdash$$

$$\frac{\langle S \rangle \quad \Gamma \vdash v : A\{y \leftarrow x\} \quad u \xrightarrow{y \leftarrow x}_S v}{\langle S \rangle \quad \Gamma \vdash u : \mathbb{Y}\, y.A}\ \vdash \mathbb{Y}$$

Entailment Rules:

$$\frac{\begin{array}{l}[A \textit{ is a sequential formula}] \\ \langle S \rangle \quad \Gamma_1 \vdash t : A, \Delta_1 \\ \langle S, t \mid u \circ\!\!\rightarrow \mathcal{X} \rangle \quad \Gamma_2, \mathcal{X} : B \vdash \Delta_2 \end{array}}{\langle S \rangle \quad \Gamma_1, \Gamma_2, u : A \multimap B \vdash \Delta_1, \Delta_2}\ \multimap \vdash$$

$$\frac{\begin{array}{l}[\mathcal{X} \textit{ is not free in the conclusion}] \\ \langle S \rangle \quad \Gamma, \mathcal{X} : A \vdash v : B, \Delta \qquad \mathcal{X} \mid u \circ\!\!\rightarrow v \end{array}}{\langle S \rangle \quad \Gamma \vdash u : A \multimap B, \Delta}\ \vdash \multimap$$

One should be able to prove that

$$\mathbb{X}[\langle \mathfrak{a} \rangle \cdot (x)] \circ \mathbb{Y}[(y) \cdot (\langle \mathfrak{b} \rangle \cdot P(y, \mathfrak{b}))] \vdash \mathbb{Y}\, y\, \mathbb{X}\, x.P(y, x).$$

Let $U = u : \mathbb{Y}\, y\, \mathbb{X}\, x.P(\mathfrak{a}, x)$.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\langle u \doteq \mathbb{X}[\mathcal{X}_2' \cdot \mathcal{X}_2] \mid \mathbb{Y}[\mathcal{Y}_1], \mathcal{Y}_1 \xrightarrow{y \leftarrow \mathfrak{a}} \hat{\mathcal{Y}}_1, \mathcal{X}_2' \mid \hat{\mathcal{Y}}_1 \multimap \mathcal{Y}_2\rangle \quad \mathcal{X}_2 : (x), \mathcal{Y}_2 : \langle y' \rangle \cdot P(\mathfrak{a}, \mathfrak{b}) \vdash U}{\langle u \doteq \mathbb{X}[\mathcal{X}_2' \cdot \mathcal{X}_2] \mid \mathbb{Y}[\mathcal{Y}_1]\rangle \quad \mathcal{X}_2' : \langle \mathfrak{a} \rangle \vdash \mathcal{X}_2' : \langle \mathfrak{a} \rangle}}{\langle u \doteq \mathbb{X}[\mathcal{X}_2' \cdot \mathcal{X}_2] \mid \mathbb{Y}[\mathcal{Y}_1], \mathcal{Y}_1 \xrightarrow{y \leftarrow \mathfrak{a}} \hat{\mathcal{Y}}_1\rangle \quad \mathcal{X}_2' : \langle \mathfrak{a} \rangle, \mathcal{X}_2 : (x), \hat{\mathcal{Y}}_1 : \langle \mathfrak{a} \rangle \multimap (\langle \mathfrak{b} \rangle \cdot P(\mathfrak{a}, \mathfrak{b})) \vdash U}\ \multimap \vdash}{\langle u \doteq \mathbb{X}[\mathcal{X}_2' \cdot \mathcal{X}_2] \mid \mathbb{Y}[\mathcal{Y}_1]\rangle \quad \mathcal{X}_2' : \langle \mathfrak{a} \rangle, \mathcal{X}_2 : (x), \mathcal{Y}_1 : \mathbb{Y}\, y.\langle y \rangle \multimap (\langle \mathfrak{b} \rangle \cdot P(y, \mathfrak{b})) \vdash U}\ \mathbb{Y} \vdash}{\langle u \doteq \mathbb{X}[\mathcal{X}_1] \mid \mathbb{Y}[\mathcal{Y}_1]\rangle \quad \mathcal{X}_1 : \langle \mathfrak{a} \rangle \cdot (x), \mathcal{Y}_1 : \mathbb{Y}\, y.\langle y \rangle \multimap (\langle \mathfrak{b} \rangle \cdot P(y, \mathfrak{b})) \vdash U}\ \cdot \vdash}{\langle u \doteq \mathbb{X}[\mathcal{X}_1] \mid \mathbb{Y}[\mathcal{Y}_1]\rangle \quad \mathcal{X}_1 : \langle \mathfrak{a} \rangle \cdot (x), \mathcal{Y}_1 : \mathbb{Y}\, y.\langle y \rangle \multimap (\langle \mathfrak{b} \rangle \cdot P(y, \mathfrak{b})) \vdash U}\ \text{def. of } (y)}{\langle u \doteq \mathbb{X}[\mathcal{X}_1] \mid \mathbb{Y}[\mathcal{Y}_1]\rangle \quad \mathcal{X}_1 : \langle \mathfrak{a} \rangle \cdot (x), \mathcal{Y}_1 : (y) \cdot (\langle \mathfrak{b} \rangle \cdot P(y, \mathfrak{b})) \vdash U}\ \circ \vdash}{\langle\ \rangle \quad u : \mathbb{X}[\langle \mathfrak{a} \rangle \cdot (x)] \circ \mathbb{Y}[(y) \cdot (\langle \mathfrak{b} \rangle \cdot P(y, \mathfrak{b}))] \vdash U}\ {}^{\infty}$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\langle S, u' \doteq \mathbb{X}[\mathcal{X}_2] \mid \mathbb{Y}[\mathcal{Y}_3 \mid 0], \mathcal{X}_2 \xrightarrow{x \leftarrow \mathfrak{b}} \hat{\mathcal{X}}_2, \hat{\mathcal{X}}_2 \mid \mathcal{Y}_3 \circ\!\!\rightarrow 0\rangle \quad 0 : t, 0 : P(\mathfrak{a}, \mathfrak{b}) \vdash U}{\langle S, u' \doteq \mathbb{X}[\mathcal{X}_2] \mid \mathbb{Y}[\mathcal{Y}_3 \mid 0]\rangle \quad \mathcal{Y}_3 : \langle \mathfrak{b} \rangle \vdash \mathcal{Y}_3 : \langle \mathfrak{b} \rangle}\ \multimap\!\vdash}{\langle S, u' \doteq \mathbb{X}[\mathcal{X}_2] \mid \mathbb{Y}[\mathcal{Y}_3 \cdot 0], \mathcal{X}_2 \xrightarrow{x \leftarrow \mathfrak{b}} \hat{\mathcal{X}}_2\rangle \quad \hat{\mathcal{X}}_2 : \langle \mathfrak{b} \rangle \multimap t, \mathcal{Y}_3 : \langle \mathfrak{b} \rangle, 0 : P(\mathfrak{a}, \mathfrak{b}) \vdash U}\ \mathbb{X}\vdash}{\langle S, u' \doteq \mathbb{X}[\mathcal{X}_2] \mid \mathbb{Y}[\mathcal{Y}_3 \cdot 0]\rangle \quad \mathcal{X}_2 : \mathbb{X}\, x.\langle x \rangle \multimap t, \mathcal{Y}_3 : \langle \mathfrak{b} \rangle, 0 : P(\mathfrak{a}, \mathfrak{b}) \vdash U}\ \cdot\vdash}{\langle S, u' \doteq \mathbb{X}[\mathcal{X}_2] \mid \mathbb{Y}[\mathcal{Y}_2]\rangle \quad \mathcal{X}_2 : \mathbb{X}\, x.\langle x \rangle \multimap t, \mathcal{Y}_2 : \langle \mathfrak{b} \rangle \cdot P(\mathfrak{a}, \mathfrak{b}) \vdash U}\ \text{def. of } (x)$$
$$\langle S, u' \doteq \mathbb{X}[\mathcal{X}_2] \mid \mathbb{Y}[\mathcal{Y}_2]\rangle \quad \mathcal{X}_2 : (x), \mathcal{Y}_2 : \langle \mathfrak{b} \rangle \cdot P(\mathfrak{a}, \mathfrak{b}) \vdash U$$

$$\frac{\dfrac{\dfrac{}{\langle S' \rangle \quad 0 : P(\mathfrak{a},\mathfrak{b}) \vdash 0 : P(\mathfrak{a},\mathfrak{b})} \quad \mathbb{X}[\mathcal{X}_2] \mid\mid \mathbb{Y}[\mathcal{Y}_2] \xrightarrow[S']{x \leftrightarrow \mathfrak{b}} 0}{\langle S' \rangle \quad 0 : P(\mathfrak{a},\mathfrak{b}) \vdash \mathcal{X}_2 \mid \mathcal{Y}_2 : \mathbb{X}\, x.P(\mathfrak{a},x)} \quad \mathbb{X}[\mathcal{X}_2' \cdot \mathcal{X}_2] \mid\mid \mathbb{Y}[\mathcal{Y}_1] \xrightarrow[S']{y \leftrightarrow \mathfrak{a}} \mathbb{X}[\mathcal{X}_2] \mid\mid \mathbb{Y}[\mathcal{Y}_2]}{\langle S' \rangle \quad 0 : P(\mathfrak{a},\mathfrak{b}) \vdash u : \mathbb{Y}\, y\, \mathbb{X}\, x.P(y,x)} \quad \mathbb{X}[\mathcal{X}_2' \cdot \mathcal{X}_2] \mid\mid \mathbb{Y}[\mathcal{Y}_1] \xrightarrow[S']{y \leftrightarrow \mathfrak{a}} \mathbb{X}[\mathcal{X}_2] \mid\mid \mathbb{Y}[\mathcal{Y}_2]}{\langle S' \rangle \quad 0 : t, 0 : P(\mathfrak{a},\mathfrak{b}) \vdash u : \mathbb{Y}\, y\, \mathbb{X}\, x.P(y,x)} \quad \mathbb{X}[\mathcal{X}_2' \cdot \mathcal{X}_2] \mid\mid \mathbb{Y}[\mathcal{Y}_1] \xrightarrow[S']{y \leftrightarrow \mathfrak{a}} \mathbb{X}[\mathcal{X}_2] \mid\mid \mathbb{Y}[\mathcal{Y}_2]}{\langle S' \rangle \quad 0 : t \vdash u : \mathbb{Y}\, y\, \mathbb{X}\, x.P(y,x)} \quad \mathbb{X}[\mathcal{X}_2' \cdot \mathcal{X}_2] \mid\mid \mathbb{Y}[\mathcal{Y}_1] \xrightarrow[S']{y \leftrightarrow \mathfrak{a}} \mathbb{X}[\mathcal{X}_2] \mid\mid \mathbb{Y}[\mathcal{Y}_2]}{\langle S' \rangle \quad \vdash u : \mathbb{Y}\, y\, \mathbb{X}\, x.P(y,x)} \quad \mathbb{X}[\mathcal{X}_2' \cdot \mathcal{X}_2] \mid\mid \mathbb{Y}[\mathcal{Y}_1] \xrightarrow[S']{y \leftrightarrow \mathfrak{a}} \mathbb{X}[\mathcal{X}_2] \mid\mid \mathbb{Y}[\mathcal{Y}_2]}{\vdash t} \quad \mathbb{X}[\mathcal{X}_2' \cdot \mathcal{X}_2] \mid\mid \mathbb{Y}[\mathcal{Y}_1] \xrightarrow[S']{y \leftrightarrow \mathfrak{a}} \mathbb{X}[\mathcal{X}_2] \mid\mid \mathbb{Y}[\mathcal{Y}_2]}{\vdash \mathbb{Y}}$$

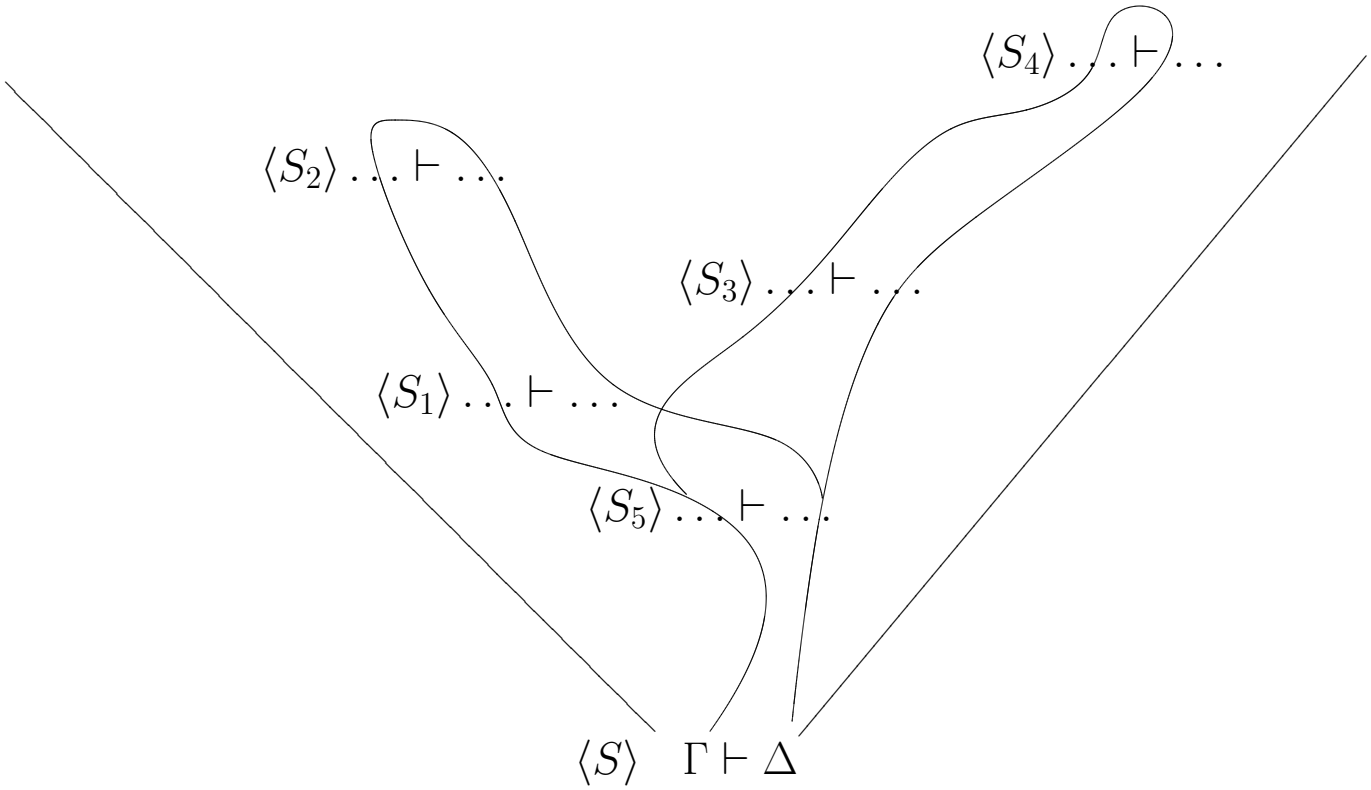
$$\dfrac{\dfrac{u \doteq \mathbb{X}[\mathcal{X}_2' \cdot \mathcal{X}_2] \mid \mathbb{Y}[\mathcal{Y}_1] \quad \mathcal{Y}_1 \xrightarrow{y \leftarrow \mathfrak{a}}_S \hat{\mathcal{Y}}_1}{u \doteq \mathbb{X}[\mathcal{X}_2' \cdot \mathcal{X}_2] \mid \mathbb{Y}[\mathcal{Y}_1] \xrightarrow{y \leftarrow \mathfrak{a}}_S \mathbb{X}[\mathcal{X}_2' \cdot \mathcal{X}_2] \mid \mathbb{Y}[\hat{\mathcal{Y}}_1]} \quad \dfrac{\mathcal{X}_2' \mid \hat{\mathcal{Y}}_1 \circ\!\!\rightarrow 0 \mid \mathcal{Y}_2}{\mathcal{X}_2' \cdot \mathcal{X}_2 \mid \hat{\mathcal{Y}}_1 \circ\!\!\rightarrow \mathcal{X}_2 \mid \mathcal{Y}_2}}{u \xrightarrow{y \leftarrow \mathfrak{a}}_{S'} \mathbb{X}[\mathcal{X}_2] \mid \mathbb{Y}[\mathcal{Y}_2]}$$

Similarly, noting that $\mathcal{Y}_3 \mid 0 \doteq \mathcal{Y}_3$,

$$\dfrac{\dfrac{u' \doteq \mathbb{X}[\mathcal{X}_2] \mid \mathbb{Y}[\mathcal{Y}_2] \quad \mathcal{X}_2 \xrightarrow{x \leftarrow \mathfrak{b}}_{S'} \hat{\mathcal{X}}_2}{u' \doteq \mathbb{X}[\mathcal{X}_2] \mid \mathbb{Y}[\mathcal{Y}_2] \xrightarrow{x \leftarrow \mathfrak{b}}_{S'} \mathbb{X}[\hat{\mathcal{X}}_2] \mid \mathbb{Y}[\mathcal{Y}_2]} \quad \dfrac{\dfrac{\hat{\mathcal{X}}_2 \mid \mathcal{Y}_3 \circ\!\!\rightarrow 0 \mid 0}{\mathcal{Y}_2 \doteq \mathcal{Y}_3 \cdot 0}}{\hat{\mathcal{X}}_2 \mid \mathcal{Y}_2 \circ\!\!\rightarrow 0 \mid 0 \cdot 0} \; 0 \mid 0 \cdot 0 \doteq 0 \mid 0}{u' \xrightarrow{x \leftarrow \mathfrak{b}}_{S'} \mathbb{X}[0] \mid \mathbb{Y}[0] \doteq 0}$$

Future Directions:

A Better User Interface:



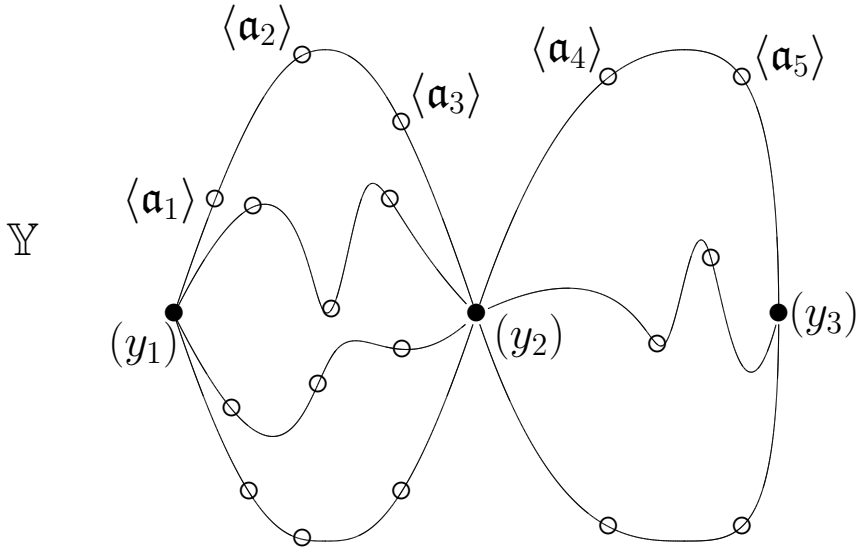
1	$\underline{\langle S \rangle \quad \Gamma}$	Hyp
2	A step	reason
3	Another step	reason
4	$\underline{\langle S_5 \rangle}$	Hyp
5	A subproof step	reason
6	An outer proof step	reason
7	$\langle S_2 \rangle$An inner black box,	
8	new rules apply in here	
9	A step	reason
10	$\langle S \rangle \quad \Delta$	reason

Possible Worlds Semantics = Strand Semantics?:

The role

$$\mathbb{Y}[(y_1) \cdot \langle x_1 \rangle \cdot \langle x_2 \rangle \cdot \langle x_3 \rangle \cdot (y_2) \cdot \langle x_4 \rangle \cdot \langle x_5 \rangle \cdot (y_3)]$$

has as its semantics all paths through $\mathbb{Y}$ below (from left to right):



where all universes between two consecutive $\bullet$'s are clusters of worlds for evaluating FO formulae.

Two roles run in parallel have links between the send and receives that pair up. In short, we have the strand semantics where the nodes are FO world clusters.

Domain Information:

The logic so far is sterile in that it can only tell you how to break apart a protocol. You cannot prove much until domain specific axioms about protocols are added.

Proof Transformations:

- Protocols can be built from smaller protocols using protocol transforms.
- Proofs should get transformed inductively according to the specification of the protocol transform.