Intuitionistic Layered Graph Logic

Simon Docherty

University College London

Tuesday 27th June 2016

Joint work with David Pym

Outline

Complex Systems and Layering

Intutionistic Layered Graph Logic

Modelling

Metatheory

Complex Systems and Layering

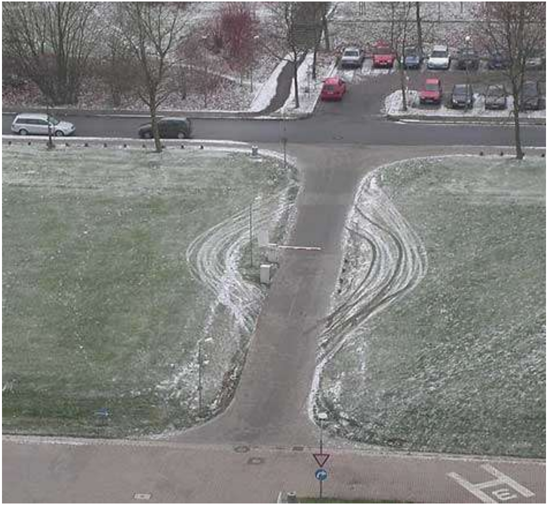
Layering In The Wild

- A complex system can be thought of a structure comprised of interconnected and interacting layers.
- More broadly: The IP stack, access control models, distributed systems, bus networks[1].
- Issues in security often arise due to a mismatch between policy and the structure of the layers of the system it applies to[2].

[1] M. Kurant and P. Thiran. Layered complex networks. *Phys. Rev. Lett.*. 96:138701. 2006

[2] T. Caulfield and D. Pym. Modelling and simulating system security policy. *Proceedings SIMUTools '15*, 9-18, 2015

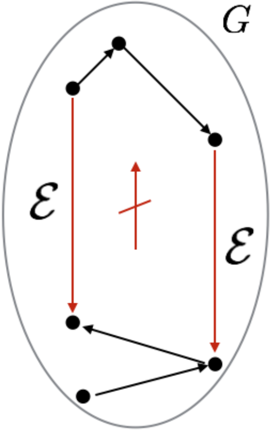
Schneier’s Gate



https://www.schneier.com/blog/archives/2005/02/the_weakest_lin.html

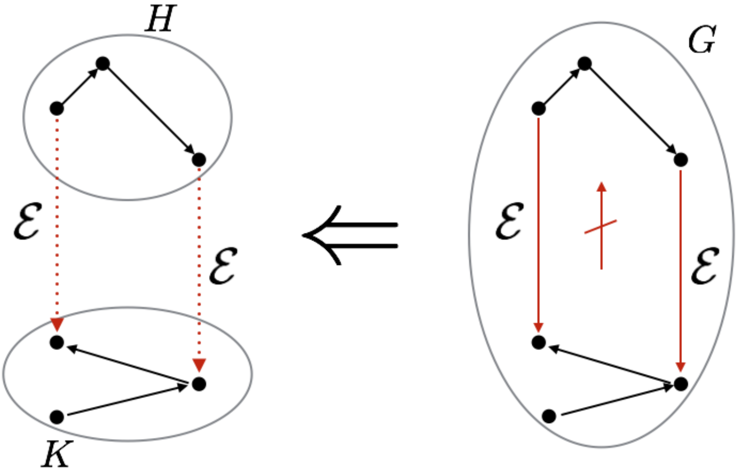
A Mathematical Definition Of Layering

Let $\mathcal{G}$ be an *ambient* directed graph, $\mathcal{E}$ a non-empty subset of $\mathcal{G}$'s edges and G a subgraph.



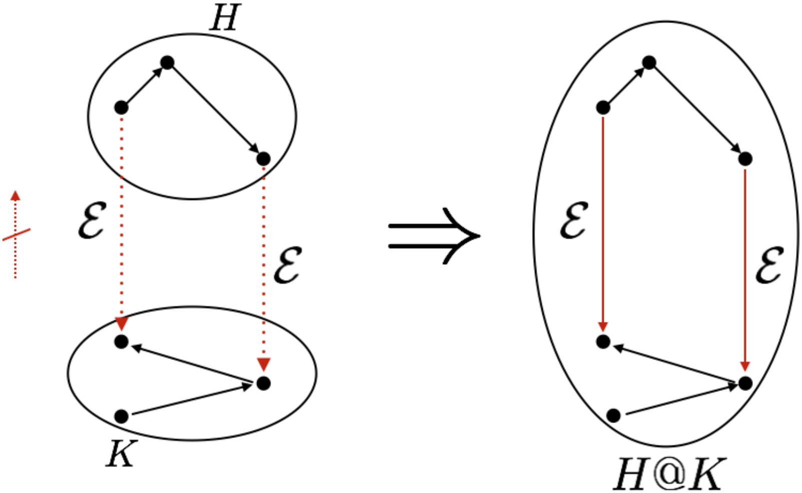
A Mathematical Definition Of Layering

Let $\mathcal{G}$ be an *ambient* directed graph, $\mathcal{E}$ a non-empty subset of $\mathcal{G}$'s edges and G a subgraph.



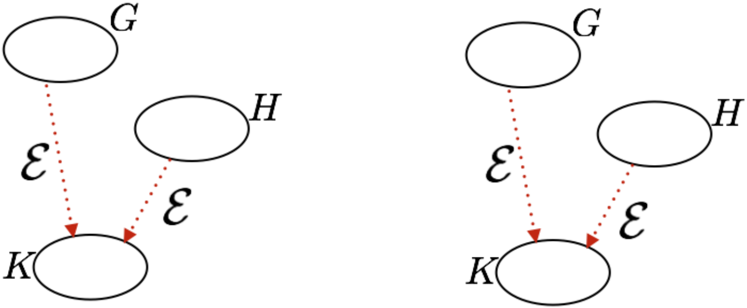
A Mathematical Definition Of Layering

This decomposition determines a *layering composition* operator @ on subgraphs of $\mathcal{G}$.



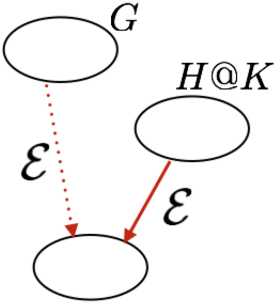
Properties of layering

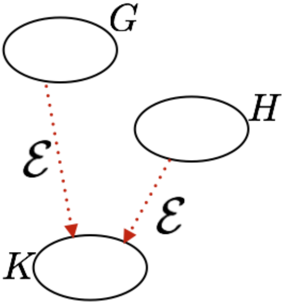
The layering operation @ on subgraphs is *partial*, *non-commutative* and ***non-associative***.



Properties of layering

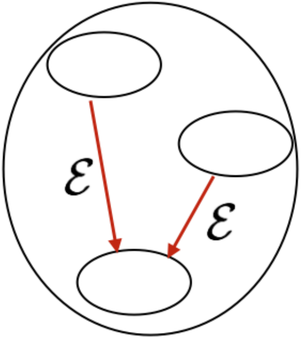
The layering operation @ on subgraphs is *partial*, *non-commutative* and ***non-associative***.



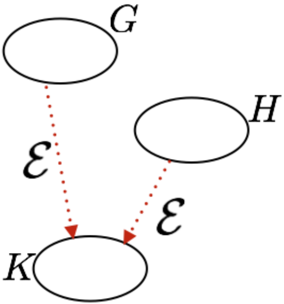


Properties of layering

The layering operation @ on subgraphs is *partial*, *non-commutative* and ***non-associative***.

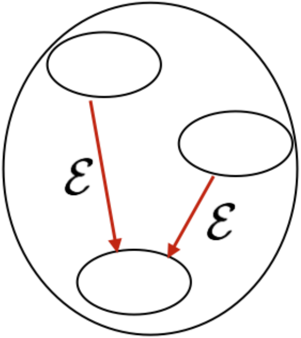


$G@(H@K)$

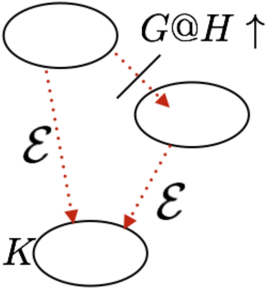


Properties of layering

The layering operation @ on subgraphs is *partial*, *non-commutative* and ***non-associative***.

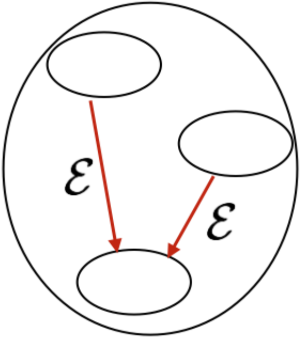


$G@(H@K)$

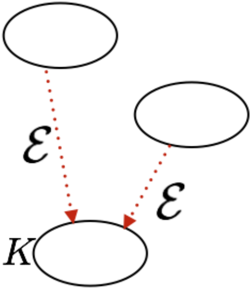


Properties of layering

The layering operation @ on subgraphs is *partial*, *non-commutative* and ***non-associative***.



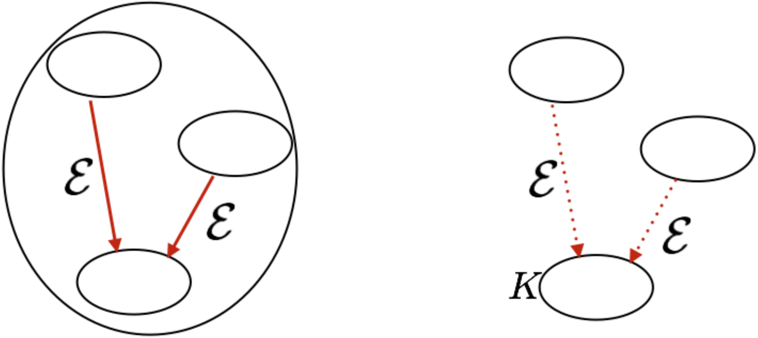
$G@(H@K)$



$(G@H)@K\uparrow$

Properties of layering

The layering operation @ on subgraphs is *partial*, *non-commutative* and ***non-associative***.



$$G@(H@K) \neq (G@H)@K$$

Layered Graph Logic

- LGL, a substructural logic for reasoning about graph layering, has been given[3] and developed into an access control assertion language[4].
- LGL lacks desirable metatheoretic properties for its layered graph semantics.
- Intuitionistic variant ILGL overcomes these deficiencies.

[3] M. Collinson, K. McDonald, and D. Pym. A substructural logic for layered graphs. *Journal of Logic and Computation*, 24(4):953–988, 2014

[4] M. Collinson, K. McDonald, and D. Pym. Layered graph logic as an assertion language for access control policy models. *Journal of Logic and Computation*, 2015. doi=10.1093/logcom/exv020.

Intutionistic Layered Graph Logic

Syntax

$$\phi ::= \mathrm{p} \mid \top \mid \bot \mid \phi \wedge \phi \mid \phi \vee \phi \mid \phi \rightarrow \phi \mid \phi \blacktriangleright \phi \mid \phi {-\!\!\blacktriangleright} \phi \mid \phi {\blacktriangleright\!\!-} \phi$$

- Additive fragment: intuitionistic propositional logic.
- Multiplicative fragment: non-associative Lambek calculus

Syntax

$$\phi ::= \mathrm{p} \mid \top \mid \bot \mid \phi \wedge \phi \mid \phi \vee \phi \mid \phi \to \phi \mid \phi \blacktriangleright \phi \mid \phi \mathrel{-\!\!\blacktriangleright} \phi \mid \phi \mathrel{\blacktriangleright\!\!-} \phi$$

- Additive fragment: intuitionistic propositional logic.
- Multiplicative fragment: non-associative Lambek calculus

$$\frac{}{\varphi \vdash \varphi}\,(\mathrm{Ax}) \qquad \frac{\varphi \vdash \psi \qquad \psi \vdash \chi}{\varphi \vdash \chi}\,(\mathrm{Cut}) \qquad \frac{}{\varphi \vdash \top}\,(\top) \qquad \frac{}{\bot \vdash \varphi}\,(\bot)$$

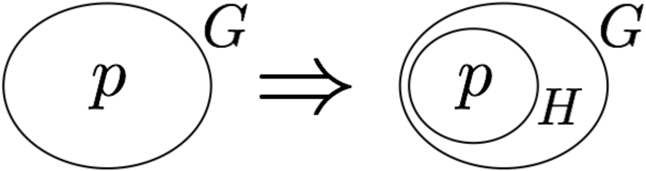
$$\frac{\varphi \vdash \psi \qquad \varphi \vdash \chi}{\varphi \vdash \psi \wedge \chi}\,(\wedge_1) \qquad \frac{}{\varphi_1 \wedge \varphi_2 \vdash \varphi_i}\,(\wedge_2) \qquad \frac{}{\varphi_i \vdash \varphi_1 \vee \varphi_2}\,(\vee_1) \qquad \frac{\varphi \vdash \chi \qquad \psi \vdash \chi}{\varphi \vee \psi \vdash \chi}\,(\vee_2)$$

$$\frac{\varphi \vdash \psi \to \chi \qquad \nu \vdash \psi}{\varphi \wedge \nu \vdash \chi}\,(\to_1) \qquad \frac{\varphi \wedge \psi \vdash \chi}{\varphi \vdash \psi \to \chi}\,(\to_2) \qquad \frac{\varphi \vdash \psi \qquad \chi \vdash \upsilon}{\varphi \blacktriangleright \chi \vdash \psi \blacktriangleright \upsilon}\,(\blacktriangleright)$$

$$\frac{\varphi \vdash \psi \mathrel{-\!\!\blacktriangleright} \chi \qquad \upsilon \vdash \psi}{\varphi \blacktriangleright \upsilon \vdash \chi}\,(\mathrel{-\!\!\blacktriangleright}_1) \qquad \frac{\varphi \blacktriangleright \psi \vdash \chi}{\varphi \vdash \psi \mathrel{-\!\!\blacktriangleright} \chi}\,(\mathrel{-\!\!\blacktriangleright}_2) \qquad \frac{\varphi \vdash \psi \mathrel{\blacktriangleright\!\!-} \chi \qquad \upsilon \vdash \psi}{\upsilon \blacktriangleright \varphi \vdash \chi}\,(\mathrel{\blacktriangleright\!\!-}_1) \qquad \frac{\varphi \blacktriangleright \psi \vdash \chi}{\psi \vdash \varphi \mathrel{\blacktriangleright\!\!-} \chi}\,(\mathrel{\blacktriangleright\!\!-}_2)$$

Semantics

Let $\mathcal{G}$ be a graph, $\mathcal{E}$ a set of its edges, X a set of its subgraphs closed under @ and $\mathcal{V} : \mathrm{Prop} \to P(X)$ a valuation satisfying *persistence*: if $G \in \mathcal{V}(p)$ and $H \sqsubseteq G$ then $H \in \mathcal{V}(p)$.

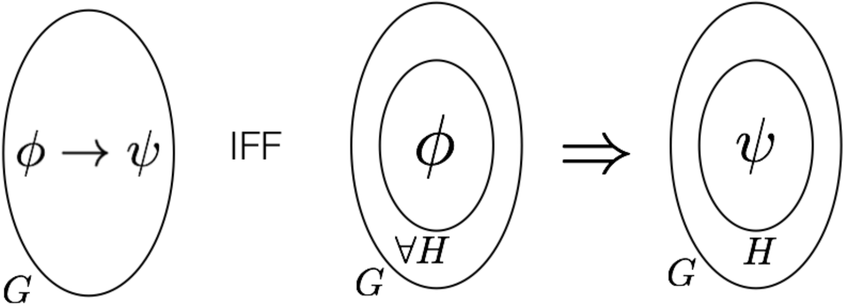


$G \vDash \top$ always $\quad G \vDash \bot$ never $\quad G \vDash \mathrm{p}$ iff $G \in \mathcal{V}(\mathrm{p})$

$G \vDash \varphi \wedge \psi$ iff $G \vDash \varphi$ and $G \vDash \psi \quad G \vDash \varphi \vee \psi$ iff $G \vDash \varphi$ or $G \vDash \psi$

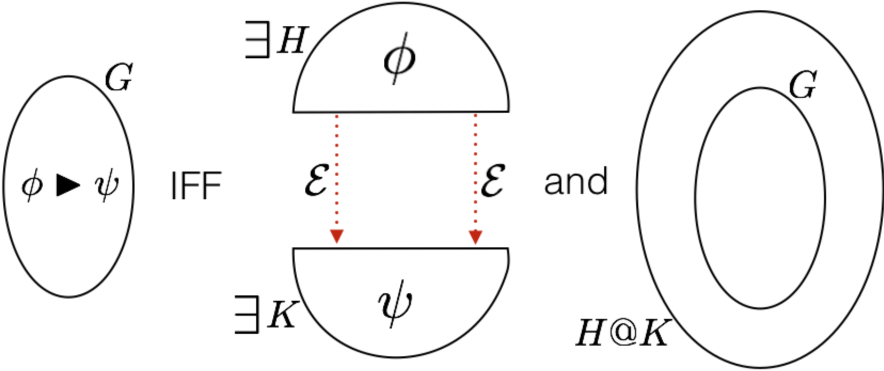
Additive Implication

$$G \vDash \phi \rightarrow \psi \text{ iff } \forall H \sqsubseteq G : \text{ if } H \vDash \phi \text{ then } H \vDash \psi$$



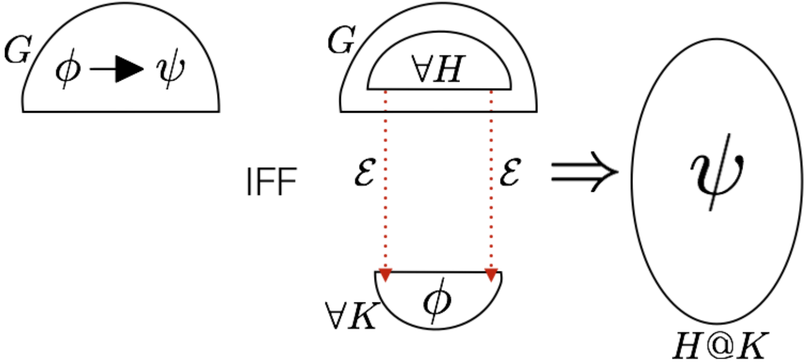
Multiplicative Conjunction

$$G \vDash \phi \blacktriangleright \psi \text{ iff } \exists H, K : H@K\downarrow, H \vDash \phi, K \vDash \psi \text{ and } G \sqsubseteq H@K$$



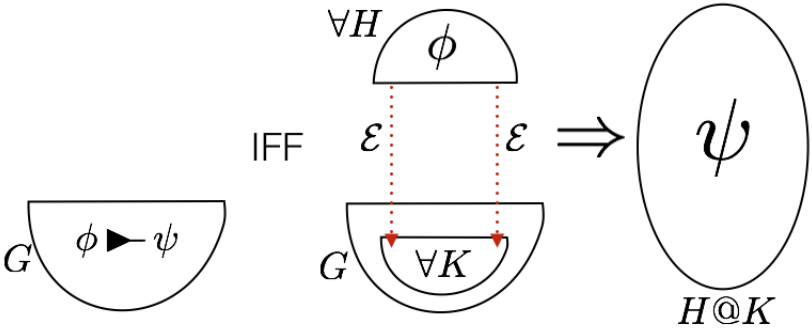
Multiplicative Implication 1

$G \vDash \phi \mathbin{-\!\!\blacktriangleright} \psi$ iff $\forall H, K :$ if $H \sqsubseteq G$, $H@K \downarrow$ and $K \vDash \phi$ then $H@K \vDash \psi$



Multiplicative Implication 2

$G \vDash \phi \blacktriangleright\!\!\!- \psi$ iff $\forall H, K$: if $K \sqsubseteq G$, $H@K \downarrow$ and $H \vDash \phi$ then $H@K \vDash \psi$



Modelling

Bunched Logic

- ILGL is an instance of a *bunched logic*[5].
- The bunched logics BI and BBI underpin *separation logic*[6] used in program verification.
- Frame rule + bi-abduction[7] = industrial applications (Facebook)
- LGL (ILGL) + commutativity + associativity + unit = BBI (BI).

[5] P O'Hearn, D Pym. The logic of bunched implications. *Bulletin Of Symbollic Logic* 5(2) 215-244, 1999

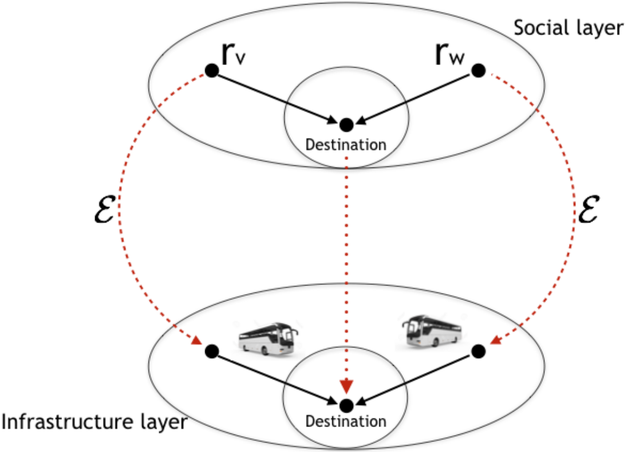
[6] J C Reynolds. Separation logic: a logic for shared mutable data structures. *Proceedings of LICS '02*, 55-74, 2002,

[7] C Calcagno et al. Compositional shape analysis by means of bi-abduction. *Proceedings POPL '09*, 289-300. 2009

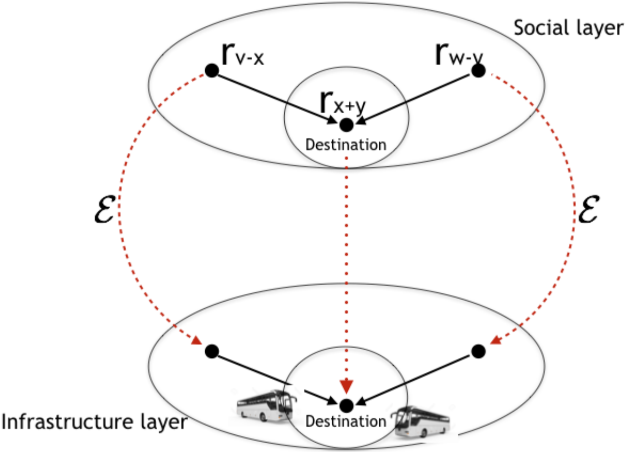
Resource Labelled Extension

- Idea: extend in the style of separation logic in order to model complex systems.
- Simple extension:
  - Vertices labelled with resources
  - Actions connected to modallties relabel vertices
  - Propositional language rich enough to express basic facts about labelling.
- Example doesn't utilise non-associativity/non-commutativity in an essential way, but gives indication of how modelling may work.

Bus Network


Social layer
r_v
r_w
Destination
$\mathcal{E}$
$\mathcal{E}$
Destination
Infrastructure layer

Bus Network



AFTER $\langle bus^a_x \rangle \langle bus^b_x \rangle$

Bus Network

- Let ϕ_x denote that buses pick up x people at the bus stops.
- Let ϕ_{meeting} denote that there is a meeting at the destination.
- Let ϕ_{quorum} denote that at least 50 people attend the meeting.
- We have $G_2 \vDash \langle bus^a_{25} \rangle \langle bus^b_{35} \rangle ((\phi_{\mathrm{meeting}} \blacktriangleright \phi_{60}) \mathrel{-\!\!\blacktriangleright} \phi_{\mathrm{quorum}})$ denoting that buses of joint capacity of 60 are sufficient to make the meeting quorate.
- We have $G_2 \vDash \langle bus^b_{40} \rangle ((\phi_{\mathrm{meeting}} \blacktriangleright \phi_{40}) \mathrel{-\!\!\blacktriangleright} \neg \phi_{\mathrm{quorum}})$ denoting that a single bus of capacity 40 is not sufficient.

Metatheory

Labelled Tableaux

$$\frac{\mathbb{T}\varphi \land \psi : x \in \mathcal{F}}{\langle\{\mathbb{T}\varphi : x, \mathbb{T}\psi : x\}, \emptyset\rangle}\langle\mathbb{T}\land\rangle \qquad \frac{\mathbb{F}\varphi \land \psi : x \in \mathcal{F}}{\langle\{\mathbb{F}\varphi : x\}, \emptyset\rangle \mid \langle\{\mathbb{F}\psi : x\}, \emptyset\rangle}\langle\mathbb{F}\land\rangle$$

$$\frac{\mathbb{T}\varphi \lor \psi : x \in \mathcal{F}}{\langle\{\mathbb{T}\varphi : x\}, \emptyset\rangle \mid \langle\{\mathbb{T}\psi : x\}, \emptyset\rangle}\langle\mathbb{T}\lor\rangle \qquad \frac{\mathbb{F}\varphi \lor \psi : x \in \mathcal{F}}{\langle\{\mathbb{F}\varphi : x, \mathbb{F}\psi : x\}, \emptyset\rangle}\langle\mathbb{F}\lor\rangle$$

$$\frac{\mathbb{T}\varphi \to \psi : x \in \mathcal{F} \text{ and } x \preccurlyeq y \in \overline{C}}{\langle\{\mathbb{F}\varphi : y\}, \emptyset\rangle \mid \langle\{\mathbb{T}\psi : y\}, \emptyset\rangle}\langle\mathbb{T}\to\rangle \qquad \frac{\mathbb{F}\varphi \to \psi : x \in \mathcal{F}}{\langle\{\mathbb{T}\varphi : c_i, \mathbb{F}\psi : c_i\}, \{x \preccurlyeq c_i\}\rangle}\langle\mathbb{F}\to\rangle$$

$$\frac{\mathbb{T}\varphi \blacktriangleright \psi : x \in \mathcal{F}}{\langle\{\mathbb{T}\varphi : c_i, \mathbb{T}\psi : c_j\}, \{c_i c_j \preccurlyeq x\}\rangle}\langle\mathbb{T}\blacktriangleright\rangle \qquad \frac{\mathbb{F}\varphi \blacktriangleright \psi : x \in \mathcal{F} \text{ and } yz \preccurlyeq x \in \overline{C}}{\langle\{\mathbb{F}\varphi : y\}, \emptyset\rangle \mid \langle\{\mathbb{F}\psi : z\}, \emptyset\rangle}\langle\mathbb{F}\blacktriangleright\rangle$$

$$\frac{\mathbb{T}\varphi \mathrel{-\!\!\blacktriangleright} \psi : x \in \mathcal{F} \text{ and } x \preccurlyeq y, yz \preccurlyeq yz \in \overline{C}}{\langle\{\mathbb{F}\varphi : z\}, \emptyset\rangle \mid \langle\{\mathbb{T}\psi : yz\}, \emptyset\rangle}\langle\mathbb{T}\mathrel{-\!\!\blacktriangleright}\rangle \qquad \frac{\mathbb{F}\varphi \mathrel{-\!\!\blacktriangleright} \psi : x \in \mathcal{F}}{\langle\{\mathbb{T}\varphi : c_j, \mathbb{F}\psi : c_i c_j\}, \{x \preccurlyeq c_i, c_i c_j \preccurlyeq c_i c_j\}\rangle}\langle\mathbb{F}\mathrel{-\!\!\blacktriangleright}\rangle$$

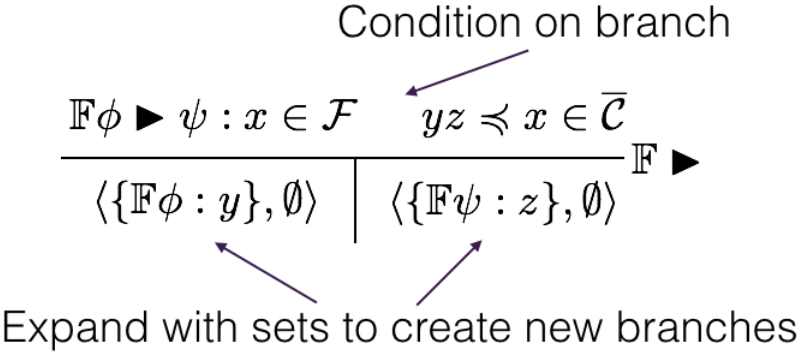
$$\frac{\mathbb{T}\varphi \mathrel{\blacktriangleright\!\!-} \psi : x \in \mathcal{F} \text{ and } x \preccurlyeq y, zy \preccurlyeq zy \in \overline{C}}{\langle\{\mathbb{F}\varphi : z\}, \emptyset\rangle \mid \langle\{\mathbb{T}\psi : zy\}, \emptyset\rangle}\langle\mathbb{T}\mathrel{\blacktriangleright\!\!-}\rangle \qquad \frac{\mathbb{F}\varphi \mathrel{\blacktriangleright\!\!-} \psi : x \in \mathcal{F}}{\langle\{\mathbb{T}\varphi : c_j, \mathbb{F}\psi : c_j c_i\}, \{x \preccurlyeq c_i, c_j c_i \preccurlyeq c_j c_i\}\rangle}\langle\mathbb{F}\mathrel{\blacktriangleright\!\!-}\rangle$$

with c_i and c_j being fresh atomic labels [8]

[8] D. Larchey-Wendling. The formal proof of the strong completeness of partial monoidal Boolean BI. *Journal of Logic and Computation*. 2014. doi:10.1093/logcom/exu031

Labelled Tableaux

A branch is a set of labelled formulae $\mathcal{F}$ and a set of inequalities on labels $\mathcal{C}$.



Condition on branch

$$\frac{\mathbb{F}\phi \blacktriangleright \psi : x \in \mathcal{F} \qquad yz \preccurlyeq x \in \overline{\mathcal{C}}}{\langle\{\mathbb{F}\phi : y\}, \emptyset\rangle \;\Big|\; \langle\{\mathbb{F}\psi : z\}, \emptyset\rangle}\ \mathbb{F}\blacktriangleright$$

Expand with sets to create new branches

A branch $\langle\mathcal{F}, \mathcal{C}\rangle$ is closed iff there exists x, y, ϕ such that either i) $\mathbb{F}\top : x \in \mathcal{B}$ or ii) $\mathbb{T}\bot : x \in \mathcal{B}$ or iii) $\mathbb{T}\phi : x, \mathbb{F}\phi : y \in \mathcal{F}$ and $x \preccurlyeq y \in \overline{\mathcal{C}}$.

A tableaux proof

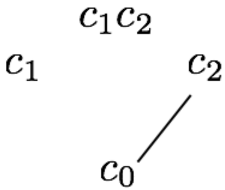
$$\mathbb{F} p \mathrel{-\!\!\blacktriangleright} (\top \blacktriangleright p) : c_0$$

A tableaux proof

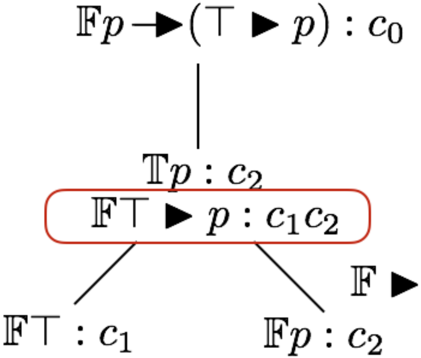
$$\boxed{\mathbb{F} p \mathrel{-\!\!\blacktriangleright} (\top \blacktriangleright p) : c_0}$$

$$\Big| \; \mathbb{F} \mathrel{-\!\!\blacktriangleright}$$

$$\mathbb{T} p : c_2$$
$$\mathbb{F} \top \blacktriangleright p : c_1 c_2$$



A tableaux proof



$\mathbb{F} p \mathrel{-\!\!\blacktriangleright} (\top \blacktriangleright p) : c_0$

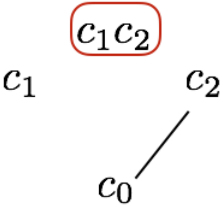
$\mathbb{T} p : c_2$

$\boxed{\mathbb{F} \top \blacktriangleright p : c_1 c_2}$

$\mathbb{F} \blacktriangleright$

$\mathbb{F} \top : c_1$

$\mathbb{F} p : c_2$



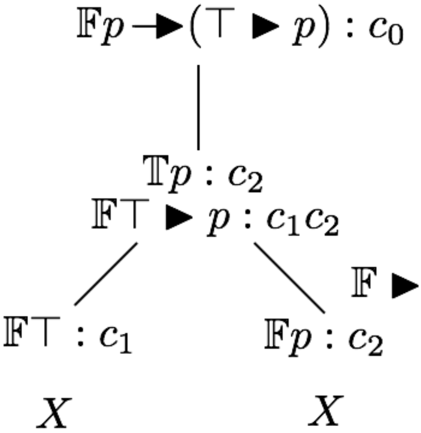
$\boxed{c_1 c_2}$

c_1

c_2

c_0

A tableaux proof



$\mathbb{F} p \mathrel{-\!\!\blacktriangleright} (\top \blacktriangleright p) : c_0$

$\mathbb{T} p : c_2$

$\mathbb{F} \top \blacktriangleright p : c_1 c_2$

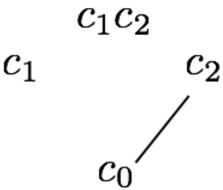
$\mathbb{F} \blacktriangleright$

$\mathbb{F} \top : c_1$

$\mathbb{F} p : c_2$

X

X



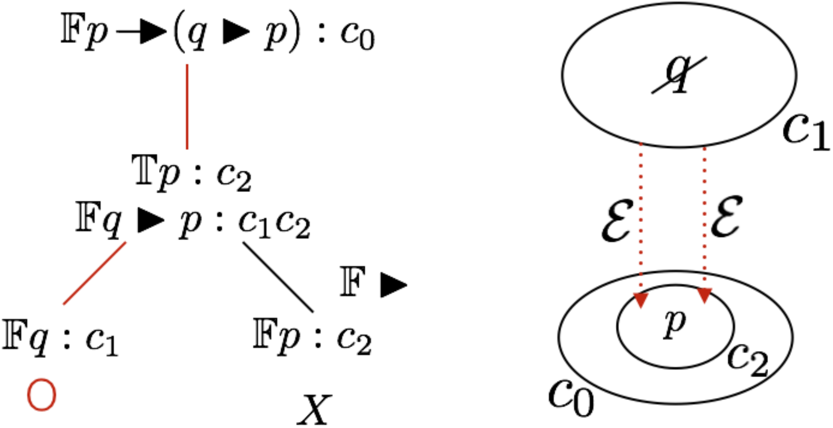
$c_1 c_2$

c_1

c_2

c_0

Countermodel construction


$\mathbb{F}p \multimap\!\blacktriangleright (q \blacktriangleright p) : c_0$
$\mathbb{T}p : c_2$
$\mathbb{F}q \blacktriangleright p : c_1c_2$
$\mathbb{F}\blacktriangleright$
$\mathbb{F}q : c_1$
O
$\mathbb{F}p : c_2$
X
$\cancel{q}$
c_1
$\mathcal{E}$
$\mathcal{E}$
p
c_2
c_0

Soundness And Completeness

Theorem

ϕ is valid in the graph theoretic semantics iff there exists a closed tableau for ϕ.

Alternative Semantics

Algebraic Semantics: A layered Heyting algebra is a structure $(\mathcal{A}, \wedge, \vee, \to, \bot, \top, \blacktriangleright, -\!\!\blacktriangleright, \blacktriangleright\!\!-)$ such that $(\mathcal{A}, \wedge, \vee, \to, \bot, \top)$ is a Heyting algebra and $(A, \leq, \blacktriangleright, -\!\!\blacktriangleright, \blacktriangleright\!\!-)$ is a residuated groupoid:

$$a \blacktriangleright b \leq c \text{ iff } a \leq b -\!\!\blacktriangleright c \text{ iff } b \leq a \blacktriangleright\!\!- c$$

Theorem

ϕ is valid on layered Heyting algebras iff $\vdash \phi$.

Relational Semantics A relational frame is a structure $(X, \preccurlyeq, R)$ such that $\preccurlyeq$ is a preorder and $R \subseteq X^3$.

Theorem

ϕ is valid on relational frames iff a closed tableau for ϕ exists.

Equivalences

Theorem (Representation Theorem)

1. *Every relational frame generates a layered Heyting algebra.*
2. *Every layered Heyting algebra can be embedded in a concrete layered Heyting algebra generated by a relational frame.*

Corollary

$\vdash \phi$ *iff* ϕ *valid on algebras iff* ϕ *valid on graphs iff there exists a closed tableau for* ϕ*.*

Theorem

The category of layered Heyting algebras is dually equivalent to the category of ILGL spaces.

Decidability

A variety of algebras has the *finite embeddability property* (FEP) iff for any algebra $\mathcal{A}$ and finite subset $\mathcal{B}_0 \subseteq \mathcal{A}$, there exists a finite algebra $\mathcal{B}$ and a homomorphic embedding $\mathcal{B}_0 \to \mathcal{B}$.

Theorem

The variety of layered Heyting algebras has the FEP.

Corollary

ILGL has the finite model property.

Proof.

$\mathcal{A}$ is (possibly infinite) countermodel for invalid ϕ.
$\mathcal{B}_0 = \{[\![\psi]\!] \mid \psi$ subformula of $\phi\}$. $\mathcal{B}$ is a finite countermodel for ϕ.

□

Future Work

- Modal and/or separation logic style extensions for modelling.
- Tool development: simulation modelling[9] and theorem proving (via tableaux[10]).
- Connections to intuitionistic modal logic (on a ternery relation).
- Algebraic/topological techniques for bunched logics/separation logic.

[9] M. Collinson, B. Monahan and D. Pym. A discipline of mathematical systems modelling. *College Publications*. 2012

[10] F. Béal, D Méry and D. Galmiche. B I L L: A theorem prover for propositional BI logic. `webloria.loria.fr/~dmery/tools/BILL`

Conclusions

- Well motivated substructural logic with Kripke semantics on graphs, sound and complete for labelled tableaux and Hilbert-style proof systems.
- Potential for complex system modelling.
- Equivalence of proof systems via equivalence of algebraic and relational semantics.
- Countermodel extraction that produces graph models.
- Decidability via finite model property.
- Case study for algebraic/topological methods in bunched/seperation logic.