

Intuitionistic layered graph logic

Simon Docherty and David Pym

University College London

simon.docherty14@ucl.ac.uk and d.pym@ucl.ac.uk

Abstract. Models of complex systems are widely used in the physical and social sciences, and the concept of layering, typically building upon graph-theoretic structure, is a common feature. We describe an intuitionistic substructural logic that gives an account of layering. As in bunched systems, the logic includes the usual intuitionistic connectives, together with a non-commutative, non-associative conjunction (used to capture layering) and its associated implications. We give soundness and completeness theorems for labelled tableaux and Hilbert-type systems with respect to a Kripke semantics on graphs. To demonstrate the utility of the logic, we show how to represent a range of systems and security examples, illuminating the relationship between services/policies and the infrastructures/architectures to which they are applied.

1 Introduction

Complex systems can be defined as the field of science that studies, on the one hand, how it is that the behaviour of a system, be it natural or synthetic, derives from the behaviours of its constituent parts and, on the other, how the system interacts with its environment. A commonly employed and highly effective concept that helps to manage the difficulty in conceptualizing and reasoning about complex systems is that of *layering*: the system is considered to consist of a collection of interconnected layers each of which has a distinct, identifiable role in the system's operations. Layers can be informational or physical and both kinds may be present in a specific system. In [6, 19], multiple layers are given by multiple relations over a single set of nodes.

We employ three illustrative examples. First, a transport network that uses buses to move people. It has an infrastructure layer (i.e., roads, together with their markings, traffic signals, etc., and buses running to a timetable), and a social layer (i.e., the groupings and movements of people enabled by the bus services). Second, a simple example of the relationship between a security policy and its underlying system architecture. Finally, we consider the security architecture of an organization that operates high- and low-security internal systems as well as providing access to its systems from external mobile devices. These examples illustrate the interplay between services/policies and the architectures/infrastructures to which they are intended to apply.

We give a graph-theoretic definition of layering and provide an associated logic for reasoning about layers. There is very little work in the literature on layering in graphs. Notable exceptions are [14, 28, 27]. Layered graphs are an instance of a general algebraic semantics for the logic. Our approach stands in contrast to our previous work in this area [9, 10] in that the additive component of the bunched logic [26, 18] we employ is intuitionistic, with the consequence that we are able to obtain a tableaux system

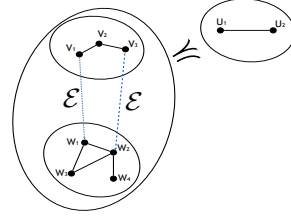
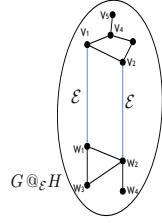
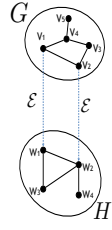


Fig. 1. A graph for which $G @_{\mathcal{E}} H$ is defined, and the resulting composition

Fig. 2. Preordered scaffold

for the logic together with a completeness theorem for the layered graph semantics. In Section 2, we introduce layered graph semantics and ILGL, the associated intuitionistic layered graph logic. In Section 3, we establish its basic metatheory — the soundness and completeness of ILGL’s tableaux system with respect to layered graph semantics — and, in Section 4, we give an algebraic semantics and a (sound and complete) Hilbert-type proof system for ILGL. In Section 5, we sketch a modal extension of ILGL that is convenient for practical modelling, explaining its theoretical status and developing the three examples mentioned above. We discuss further work in Section 6.

2 Intuitionistic layered graph logic

Layered graph semantics. We begin with a formal, graph-theoretic account of the notion of layering that, we claim, captures the concept as used in complex systems. In this notion, two layers in a directed graph are connected by a specified set of edges, each element of which starts in the upper layer and ends in the lower layer.

Given a directed graph, \mathcal{G} , we refer to its *vertex set* and its *edge set* by $V(\mathcal{G})$ and $E(\mathcal{G})$ respectively, while its set of subgraphs is denoted $Sg(\mathcal{G})$ with $H \subseteq \mathcal{G}$ iff $H \in Sg(\mathcal{G})$. For a distinguished edge set $\mathcal{E} \subseteq E(\mathcal{G})$, the reachability relation $\rightsquigarrow_{\mathcal{E}}$ on subgraphs of \mathcal{G} is $H \rightsquigarrow_{\mathcal{E}} K$ iff a vertex of K can be reached from a vertex of H by an \mathcal{E} -edge.

We then have a composition $@_{\mathcal{E}}$ on subgraphs where $G @_{\mathcal{E}} H \downarrow$ iff $V(G) \cap V(H) = \emptyset$, $G \rightsquigarrow_{\mathcal{E}} H$ and $H \not\rightsquigarrow_{\mathcal{E}} G$ (where \downarrow denotes definedness) with output given by the graph union of the two subgraphs and the \mathcal{E} -edges between them. For a graph \mathcal{G} , we say it is *layered* (with respect to \mathcal{E}) if there exist H, K such that $H @_{\mathcal{E}} K \downarrow$ and $\mathcal{G} = H @_{\mathcal{E}} K$ (see Figure 1). Layering is evidently neither commutative nor associative.

Within a given ambient graph, \mathcal{G} , we can identify a specific form of layered structure, called a *preordered scaffold*, that will facilitate our definition of a model of intuitionistic layered graph logic. Properties of graphs that are inherited by their subgraphs are naturally captured in an intuitionistic logic. This idea is generalized by the structure carried by a preordered scaffold. To set this up, we begin by defining an *admissible subgraph set* is a subset $X \subseteq Sg(\mathcal{G})$ such that, for all $G, H \in Sg(\mathcal{G})$, if $G @_{\mathcal{E}} H \downarrow$, then $G, H \in X$ iff $G @_{\mathcal{E}} H \in X$. Then, a *preordered scaffold* (see Figure 2) is a structure $\mathcal{X} = (\mathcal{G}, \mathcal{E}, X, \preceq)$ such that \mathcal{G} is a graph, $\mathcal{E} \subseteq E(\mathcal{G})$, X an admissible subgraph set, \preceq a preorder on X . Layers are present if $G @_{\mathcal{E}} H \downarrow$ for at least one pair $G, H \in X$.

Note that the scaffold is preordered and we choose a subset of the subgraph set. There are several reasons for these choices. From a modelling perspective, we can look closely at the precise layering structure of the graph that is of interest. In particular, we can avoid degenerate cases of layering. (Note that this is a more general definition of scaffold than that taken in [9, 10], where the structure was less tightly defined.) Technical considerations also come into play. When we restrict to interpreting ILGL on the full subgraph set, it is impossible to perform any composition of models without the worlds (states) proliferating wildly. A similar issue arises during the construction of countermodels from the tableaux system of Section 3, a procedure that is impossible when we are forced to take the full subgraph set as the set of worlds.

Having established the basic semantic structures that are required, we can now set up ILGL. The grammar of ILGL is the following:

$$\phi ::= p \mid \top \mid \perp \mid \phi \wedge \phi \mid \phi \vee \phi \mid \phi \rightarrow \phi \mid \phi \blacktriangleright \phi \mid \phi \blacktriangleright\!\!\blacktriangleright \phi \mid \phi \blacktriangleright\!\!\blacktriangleright\!\!\blacktriangleright \phi$$

The familiar connectives will be interpreted intuitionistically. The non-commutative, non-associative conjunction, \blacktriangleright , which will be used to capture layering, is interpreted intuitionistically, as in BI [26, 18], and has associated right (\blacktriangleright) and left ($\blacktriangleright\!\!\blacktriangleright$) implications. We define intuitionistic negation in terms of the connectives: $\neg\phi ::= \phi \rightarrow \perp$.

Definition 1 (Layered graph model). A layered graph model, \mathcal{M} , of ILGL is a pair (X, \mathcal{V}) , where X is a preordered scaffold and $\mathcal{V} : \text{Prop} \rightarrow \wp(X)$ is a persistent valuation; that is, $G \leq H$ and $G \in \mathcal{V}(p)$ implies $H \in \mathcal{V}(p)$. \square

Satisfaction in layered graph models is then defined in a familiar way.

Definition 2 (Satisfaction in layered graph models). Given a layered graph model $\mathcal{M} = (X, \mathcal{V})$, we generate the satisfaction relation $\models_{\mathcal{M}} \subseteq X \times \text{Form}$ as follows:

$$\begin{aligned} G \models_{\mathcal{M}} \top & \text{ always} & G \models_{\mathcal{M}} \perp & \text{ never} & G \models_{\mathcal{M}} p & \text{ iff } G \in \mathcal{V}(p) \\ G \models_{\mathcal{M}} \phi \wedge \psi & \text{ iff } G \models_{\mathcal{M}} \phi \text{ and } G \models_{\mathcal{M}} \psi & G \models_{\mathcal{M}} \phi \vee \psi & \text{ iff } G \models_{\mathcal{M}} \phi \text{ or } G \models_{\mathcal{M}} \psi \\ G \models_{\mathcal{M}} \phi \rightarrow \psi & \text{ iff, for all } G' \text{ such that } G \leq G', G' \models_{\mathcal{M}} \phi \text{ implies } G' \models_{\mathcal{M}} \psi \end{aligned}$$

$$\begin{aligned} G \models_{\mathcal{M}} \phi \blacktriangleright \psi & \text{ iff there exist } H, K \text{ such that } H @_{\varepsilon} K \downarrow, H @_{\varepsilon} K \leq G, \text{ and } H \models_{\mathcal{M}} \phi \text{ and } K \models_{\mathcal{M}} \psi \\ G \models_{\mathcal{M}} \phi \blacktriangleright\!\!\blacktriangleright \psi & \text{ iff for all } G \leq H \text{ and all } K \text{ such that } H @_{\varepsilon} K \downarrow, K \models_{\mathcal{M}} \phi \text{ implies } H @_{\varepsilon} K \models_{\mathcal{M}} \psi \\ G \models_{\mathcal{M}} \phi \blacktriangleright\!\!\blacktriangleright\!\!\blacktriangleright \psi & \text{ iff for all } G \leq H \text{ and all } K \text{ such that } K @_{\varepsilon} H \downarrow, K \models_{\mathcal{M}} \phi \text{ implies } K @_{\varepsilon} H \models_{\mathcal{M}} \psi \quad \square \end{aligned}$$

Definition 3 (Validity). A formula ϕ is valid in a layered graph model \mathcal{M} ($\models_{\mathcal{M}} \phi$) iff, for all $G \in X$, $G \models_{\mathcal{M}} \phi$. A formula ϕ is valid ($\models \phi$) iff, for all layered graph models \mathcal{M} , $\models_{\mathcal{M}} \phi$. \square

Lemma 1 (Persistence). Persistence extends to all formulae with respect to the layered graph semantics. That is, for all $\varphi \in \text{Form}$, $G \leq H$ and $G \models_{\mathcal{M}} \varphi$ implies $H \models_{\mathcal{M}} \varphi$.

Proof. By induction on the complexity of formulae. The additive fragment, corresponding to intuitionistic propositional logic (IPL), is standard and we restrict attention to two examples of the multiplicative connectives.

Suppose $G \models_{\mathcal{M}} \phi \blacktriangleright \psi$ and $G \leq H$. There are K, K' s.t. $K @_{\varepsilon} K' \downarrow$ and $K @_{\varepsilon} K' \leq G$, with $K \models_{\mathcal{M}} \phi$ and $K' \models_{\mathcal{M}} \psi$. By transitivity of \leq , $K @_{\varepsilon} K' \leq H$, so $H \models_{\mathcal{M}} \phi \blacktriangleright \psi$.

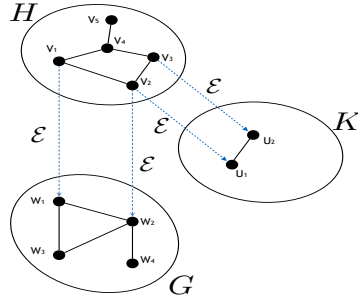


Fig. 3. The \mathcal{E} -reachability preorder

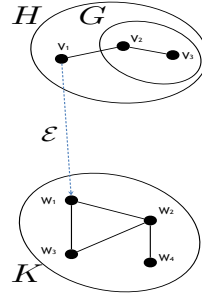


Fig. 4. The subgraph order

Suppose $G \models_{\mathcal{M}} \varphi \rightarrow \psi$. Then, for all K such that $G \leq K$ and all K' s.t. $K @_{\mathcal{E}} K' \downarrow$, if $K' \models_{\mathcal{M}} \varphi$, then $K @_{\mathcal{E}} K' \models_{\mathcal{M}} \psi$. Let $G \leq H$ and suppose $H \leq K$ and K' are s.t. $K @_{\mathcal{E}} K' \downarrow$ and $K' \models_{\mathcal{M}} \varphi$. So, since $G \leq H \leq K$, it follows that $K @_{\mathcal{E}} K' \models_{\mathcal{M}} \varphi$. So $H \models_{\mathcal{M}} \varphi \rightarrow \psi$. \square

Note that, unlike in BI, we require the restriction ‘for all $H, G \leq H \dots$ ’ in the semantic clauses for the multiplicative implications. Without this we cannot prove persistence because we cannot proceed with the inductive step in those cases. The reason for this is that we put no restriction on the interaction between \leq and $@$ in the definition of preordered scaffold. This is unlike the analogous case for BI, where the monoidal composition is required to be bifunctorial with respect to the ordering. One might resolve this issue with the following addendum to the definition of preordered scaffold: if $G \leq H$ and $H @_{\mathcal{E}} K \downarrow$, then $G @_{\mathcal{E}} K \downarrow$ and $G @_{\mathcal{E}} K \leq H @_{\mathcal{E}} K$.

Two natural examples of subgraph preorderings show that this would be undesirable. First, consider the layering preorder. Let \leq be the reflexive, transitive closure of the relation $R(G, H)$ iff $H @_{\mathcal{E}} G \downarrow$, restricted to the admissible subgraph set X . Figure 3 shows a subgraph H with $G \leq H$ and $H @_{\mathcal{E}} K \downarrow$ but $G @_{\mathcal{E}} K \uparrow$ (we write \uparrow for undefinedness). Second, consider the subgraph relation. In Figure 4, we have $G \subseteq H$ and $H @_{\mathcal{E}} K \downarrow$ but $G @_{\mathcal{E}} K \uparrow$. It is, however, the case that, with this ordering, if $G \subseteq H, H @_{\mathcal{E}} K$ and $G @_{\mathcal{E}} K \downarrow$, then $G @_{\mathcal{E}} K \subseteq H @_{\mathcal{E}} K$.

Labelled tableaux. We define a labelled tableaux system for ILGL in the spirit of previous work for BI, BBI, DBI, and LSM [16, 24, 12, 11].

Definition 4 (Graph labels). Let $\Sigma = \{c_i \mid i \in \mathbb{N}\}$ be a countable set of atomic labels. We define the set $\mathbb{L} = \{x \in \Sigma^* \mid 0 < |x| \leq 2\} \setminus \{c_i c_i \mid c_i \in \Sigma\}$ to be the set of graph labels. A sub-label y of a label x is a non-empty sub-word of x , and we denote the set of sub-labels of x by $\mathcal{S}(x)$. \square

The graph labels are a syntactic representation of the subgraphs of a model, with labels of length 2 representing a graph that can be decomposed into two layers. We exclude the possibility $c_i c_i$ as layering is anti-reflexive. In much the same way we give a syntactic representation of preorder.

Definition 5 (Constraints). A constraint is an expression of the form $x \leq y$, where x and y are graph labels. \square

Let C be a set of constraints. The *domain* of C is the set of all non-empty sub-labels appearing in C . In particular, $\mathcal{D}(C) = \bigcup_{x \leq y \in C} (\mathcal{S}(x) \cup \mathcal{S}(y))$. The *alphabet* of C is the set of atomic labels appearing in C . In particular, we have $\mathcal{A}(C) = \Sigma \cap \mathcal{D}(C)$.

$$\begin{array}{cccc} \frac{x \leq y}{x \leq x} \langle R_1 \rangle & \frac{x \leq y}{y \leq y} \langle R_2 \rangle & \frac{x \leq yz}{y \leq y} \langle R_3 \rangle & \frac{x \leq yz}{z \leq z} \langle R_4 \rangle \\ \frac{xy \leq z}{x \leq x} \langle R_5 \rangle & \frac{xy \leq z}{y \leq y} \langle R_6 \rangle & \frac{x \leq y \quad y \leq z}{x \leq z} \langle \text{Tr} \rangle \end{array}$$

Fig. 5. Rules for closure of constraints

Definition 6 (Closure of constraints). Let C be a set of constraints. The closure of C , denoted \overline{C} , is the least relation closed under the rules of Figure 5 such that $C \subseteq \overline{C}$. \square

This closure yields a preorder on $\mathcal{D}(C)$, with $\langle R_1 \rangle - \langle R_6 \rangle$ generating reflexivity and $\langle \text{Tr} \rangle$ yielding transitivity. Crucially, taking the closure of the constraint set does not cause labels to proliferate and the generation of any particular constraint from an arbitrary constraint set C is fundamentally a finite process.

Proposition 1. Let C be a set of constraints. (1) $x \in \mathcal{D}(\overline{C})$ iff $x \leq x \in \overline{C}$. (2) $\mathcal{D}(C) = \mathcal{D}(\overline{C})$ and $\mathcal{A}(C) = \mathcal{A}(\overline{C})$. \square

Lemma 2 (Compactness). Let C be a (possibly countably infinite) set of constraints. If $x \leq y \in \overline{C}$, then there is a finite set of constraints $C_f \subseteq C$ such that $x \leq y \in \overline{C}_f$. \square

Definition 7. A labelled formula is a triple $(S, \varphi, x) \in \{\mathbb{T}, \mathbb{F}\} \times \mathcal{L} \times \mathbb{L}$, written $\mathbb{S}\varphi : x$. A constrained set of statements (CSS) is a pair $\langle \mathcal{F}, C \rangle$, where \mathcal{F} is a set of labelled formulae and C is a set of constraints, satisfying the following properties: for all $x \in \mathbb{L}$ and distinct $c_i, c_j, c_k \in \Sigma$, (1) (Ref) if $\mathbb{S}\varphi : x \in \mathcal{F}$, then $x \leq x \in \overline{C}$, (2) (Contra) if $c_i c_j \in \mathcal{D}(C)$, then $c_j c_i \notin \mathcal{D}(C)$, and (3) (Freshness) if $c_i c_j \in \mathcal{D}(C)$, then $c_i c_k, c_k c_i, c_j c_k, c_k c_j \notin \mathcal{D}(C)$. A CSS $\langle \mathcal{F}, C \rangle$ is finite if \mathcal{F} and C are finite. The relation \subseteq is defined on CSSs by $\langle \mathcal{F}, C \rangle \subseteq \langle \mathcal{F}', C' \rangle$ iff $\mathcal{F} \subseteq \mathcal{F}'$ and $C \subseteq C'$. We denote by $\langle \mathcal{F}_f, C_f \rangle \subseteq_f \langle \mathcal{F}, C \rangle$ when $\langle \mathcal{F}_f, C_f \rangle \subseteq \langle \mathcal{F}, C \rangle$ holds and $\langle \mathcal{F}_f, C_f \rangle$ is finite. \square

The CSS properties ensure models can be built from the labels: (Ref) ensures we have enough data for the closure rules to generate a preorder, (Contra) ensures the contra-commutativity of graph layering is respected, and (Freshness) ensures the layering structure of the models we construct is exactly that specified by the labels and constraints in the CSS. As with constraint closure, CSSs have a finite character.

Proposition 2. For any CSS $\langle \mathcal{F}_f, C \rangle$ in which \mathcal{F}_f is finite, there exists $C_f \subseteq C$ such that C_f is finite and $\langle \mathcal{F}_f, C_f \rangle$ is a CSS. \square

$\frac{\mathbb{T}\varphi \wedge \psi : x \in \mathcal{F}}{\langle \{\mathbb{T}\varphi : x, \mathbb{T}\psi : x\}, \emptyset \rangle} \langle \mathbb{T}\wedge \rangle$	$\frac{\mathbb{F}\varphi \wedge \psi : x \in \mathcal{F}}{\langle \{\mathbb{F}\varphi : x\}, \emptyset \mid \langle \{\mathbb{F}\psi : x\}, \emptyset \rangle} \langle \mathbb{F}\wedge \rangle$
$\frac{\mathbb{T}\varphi \vee \psi : x \in \mathcal{F}}{\langle \{\mathbb{T}\varphi : x\}, \emptyset \mid \langle \{\mathbb{T}\psi : x\}, \emptyset \rangle} \langle \mathbb{T}\vee \rangle$	$\frac{\mathbb{F}\varphi \vee \psi : x \in \mathcal{F}}{\langle \{\mathbb{F}\varphi : x, \mathbb{F}\psi : x\}, \emptyset \rangle} \langle \mathbb{F}\vee \rangle$
$\frac{\mathbb{T}\varphi \rightarrow \psi : x \in \mathcal{F} \text{ and } x \leq y \in \bar{C}}{\langle \{\mathbb{F}\varphi : y\}, \emptyset \mid \langle \{\mathbb{T}\psi : y\}, \emptyset \rangle} \langle \mathbb{T}\rightarrow \rangle$	$\frac{\mathbb{F}\varphi \rightarrow \psi : x \in \mathcal{F}}{\langle \{\mathbb{T}\varphi : c_i, \mathbb{F}\psi : c_i\}, \{x \leq c_i\}\rangle} \langle \mathbb{F}\rightarrow \rangle$
$\frac{\mathbb{T}\varphi \blacktriangleright \psi : x \in \mathcal{F}}{\langle \{\mathbb{T}\varphi : c_i, \mathbb{T}\psi : c_j\}, \{c_i c_j \leq x\}\rangle} \langle \mathbb{T}\blacktriangleright \rangle$	$\frac{\mathbb{F}\varphi * \psi : x \in \mathcal{F} \text{ and } yz \leq x \in \bar{C}}{\langle \{\mathbb{F}\varphi : y\}, \emptyset \mid \langle \{\mathbb{F}\psi : z\}, \emptyset \rangle} \langle \mathbb{F}\blacktriangleright \rangle$
$\frac{\mathbb{T}\varphi \twoheadrightarrow \psi : x \in \mathcal{F} \text{ and } x \leq y, yz \leq yz \in \bar{C}}{\langle \{\mathbb{F}\varphi : z\}, \emptyset \mid \langle \{\mathbb{T}\psi : yz\}, \emptyset \rangle} \langle \mathbb{T}\twoheadrightarrow \rangle$	$\frac{\mathbb{F}\varphi \twoheadrightarrow \psi : x \in \mathcal{F}}{\langle \{\mathbb{T}\varphi : c_j, \mathbb{F}\psi : c_i c_j\}, \{x \leq c_i, c_i c_j \leq c_j c_i\}\rangle} \langle \mathbb{F}\twoheadrightarrow \rangle$
$\frac{\mathbb{T}\varphi \blacktriangleright\blacktriangleright \psi : x \in \mathcal{F} \text{ and } x \leq y, zy \leq zy \in \bar{C}}{\langle \{\mathbb{F}\varphi : z\}, \emptyset \mid \langle \{\mathbb{T}\psi : zy\}, \emptyset \rangle} \langle \mathbb{T}\blacktriangleright\blacktriangleright \rangle$	$\frac{\mathbb{F}\varphi \blacktriangleright\blacktriangleright \psi : x \in \mathcal{F}}{\langle \{\mathbb{T}\varphi : c_j, \mathbb{F}\psi : c_j c_i\}, \{x \leq c_i, c_j c_i \leq c_j c_i\}\rangle} \langle \mathbb{F}\blacktriangleright\blacktriangleright \rangle$

with c_i and c_j being fresh atomic labels

Fig. 6. Tableaux rules for ILGL

Figure 6 presents the rules of the tableaux system for ILGL. That ‘ c_i and c_j are fresh atomic labels’ means $c_i \neq c_j \in \Sigma \setminus \mathcal{A}(C)$. We denote by \oplus the concatenation of lists.

Definition 8 (Tableaux). Let $\langle \mathcal{F}_0, C_0 \rangle$ be a finite CSS. A tableau for this CSS is a list of CSS, called branches, built inductively according the following rules:

1. The one branch list $[\langle \mathcal{F}_0, C_0 \rangle]$ is a tableau for $\langle \mathcal{F}_0, C_0 \rangle$;
2. If the list $\mathcal{T}_m \oplus [\langle \mathcal{F}, C \rangle] \oplus \mathcal{T}_n$ is a tableau for $\langle \mathcal{F}_0, C_0 \rangle$ and

$$\frac{\text{cond}\langle \mathcal{F}, C \rangle}{\langle \mathcal{F}_1, C_1 \rangle \mid \dots \mid \langle \mathcal{F}_k, C_k \rangle}$$

is an instance of a rule of Figure 6 for which $\text{cond}\langle \mathcal{F}, C \rangle$ is fulfilled, then the list $\mathcal{T}_m \oplus [\langle \mathcal{F} \cup \mathcal{F}_1, C \cup C_1 \rangle; \dots; \langle \mathcal{F} \cup \mathcal{F}_k, C \cup C_k \rangle] \oplus \mathcal{T}_n$ is a tableau for $\langle \mathcal{F}_0, C_0 \rangle$.

A tableau for the formula φ is a tableau for $\langle \{\mathbb{F}\varphi : c_0\}, \{c_0 \leq c_0\} \rangle$. □

It is a simple but tedious exercise to show that the rules of Figure 6 preserve the CSS properties of Definition 7. We now give the notion of proof for our labelled tableaux.

Definition 9 (Closed tableau/proof). A CSS $\langle \mathcal{F}, C \rangle$ is closed if one of the following conditions holds: (1) $\mathbb{T}\varphi : x \in \mathcal{F}$, $\mathbb{F}\varphi : y \in \mathcal{F}$ and $x \leq y \in \bar{C}$; (2) $\mathbb{F}\top : x \in \mathcal{F}$; and (3) $\mathbb{T}\perp : x \in \mathcal{F}$. A CSS is open iff it is not closed. A tableau is closed iff all its branches are closed. A proof for a formula φ is a closed tableau for φ . □

CSSs are related back to the graph semantics via the notion of realization.

Definition 10 (Realization). Let $\langle \mathcal{F}, \mathcal{C} \rangle$ be a CSS. A realization of $\langle \mathcal{F}, \mathcal{C} \rangle$ is a triple $\mathfrak{R} = (\mathcal{X}, \mathcal{V}, \lfloor \cdot \rfloor)$ where $\mathcal{M} = (\mathcal{X}, \mathcal{V})$ is a layered graph model and $\lfloor \cdot \rfloor : \mathcal{D}(\mathcal{C}) \rightarrow \mathcal{X}$ is such that (1) $\lfloor \cdot \rfloor$ is total: for all $x \in \mathcal{D}(\mathcal{C}) \cdot \lfloor x \rfloor \downarrow$, (2) for all $x \in \mathcal{D}(\mathcal{C})$, if $x = c_i c_j$, then $\lfloor c_i \rfloor @_{\mathcal{E}} \lfloor c_j \rfloor \downarrow$ and $\lfloor x \rfloor = \lfloor c_i \rfloor @_{\mathcal{E}} \lfloor c_j \rfloor$, (3) if $x \leq y \in \mathcal{C}$, then $\lfloor x \rfloor \leq_M \lfloor y \rfloor$, (4) if $\mathbb{T}\varphi : x \in \mathcal{F}$, then $\lfloor x \rfloor \models_M \varphi$, and (5) if $\mathbb{F}\varphi : x \in \mathcal{F}$, then $\lfloor x \rfloor \not\models_M \varphi$. \square

We say that a CSS is *realizable* if there exists a realization of it. We say that a tableau is *realizable* if at least one of its branches is realizable. We can also show that the relevant clauses of the definition extend to the closure of the constraint set automatically.

Proposition 3. Let $\langle \mathcal{F}, \mathcal{C} \rangle$ be a CSS and $\mathfrak{R} = (\mathcal{X}, \mathcal{V}, \lfloor \cdot \rfloor)$ a realization of it. Then: (1) for all $x \in \mathcal{D}(\overline{\mathcal{C}})$, $\lfloor x \rfloor$ is defined; (2) if $x \leq y \in \overline{\mathcal{C}}$, then $\lfloor x \rfloor \leq_M \lfloor y \rfloor$. \square

3 Metatheory

We now establish the soundness and, via countermodel extraction, the completeness of ILGL's tableaux system with respect to layered graph semantics. The proof of soundness is straightforward (cf. [15, 16, 24, 12, 11]). We begin with two key lemmas about realizability and closure. Their proofs proceed by simple case analysis.

Lemma 3. The tableaux rules for ILGL preserve realizability. \square

Lemma 4. Closed branches are not realizable. \square

Theorem 1 (Soundness). If there exists a closed tableau for the formula φ , then φ is valid in layered graph models.

Proof. Suppose that there exists a proof for φ . Then there is a closed tableau \mathcal{T}_φ for the CSS $\mathcal{C} = \{\{\mathbb{F}\varphi : c_0\}, \{c_0 \leq c_0\}\}$. Now suppose that φ is not valid. Then there is a countermodel $\mathcal{M} = (\mathcal{X}, \mathcal{V})$ and a subgraph $G \in \mathcal{X}$ such that $G \not\models_M \varphi$. Define $\mathfrak{R} = (\mathcal{M}, \mathcal{V}, \lfloor \cdot \rfloor)$ with $\lfloor c_0 \rfloor = G$. Note that \mathfrak{R} is a realization of \mathcal{C} , hence by Lemma 3, \mathcal{T}_φ is realizable. By Lemma 4, \mathcal{T}_φ cannot be closed. But, this contradicts the fact that \mathcal{T}_φ is a proof and therefore a closed tableau. It follows that φ is valid. \square

We now proceed to establish the completeness of the labelled tableaux with respect to layered graph semantics. We begin with the notion of a Hintikka CSS, which will facilitate the construction of countermodels. All remaining proofs omitted from this section are provided or cited in the appendix.

Definition 11 (Hintikka CSS). A CSS $\langle \mathcal{F}, \mathcal{C} \rangle$ is a Hintikka CSS iff, for any formulas $\varphi, \psi \in \mathcal{L}$ and any graph labels $x, y \in \mathbb{L}$, we have the following:

1. $\mathbb{T}\varphi : x \notin \mathcal{F}$ or $\mathbb{F}\varphi : y \notin \mathcal{F}$ or $x \leq y \notin \overline{\mathcal{C}}$ 2. $\mathbb{F}\top : x \notin \mathcal{F}$ 3. $\mathbb{T}\perp : x \notin \mathcal{F}$
4. if $\mathbb{T}\varphi \wedge \psi : x \in \mathcal{F}$, then $\mathbb{T}\varphi : x \in \mathcal{F}$ and $\mathbb{T}\psi : x \in \mathcal{F}$
5. if $\mathbb{F}\varphi \wedge \psi : x \in \mathcal{F}$, then $\mathbb{F}\varphi : x \in \mathcal{F}$ or $\mathbb{F}\psi : x \in \mathcal{F}$
6. if $\mathbb{T}\varphi \vee \psi : x \in \mathcal{F}$, then $\mathbb{T}\varphi : x \in \mathcal{F}$ or $\mathbb{T}\psi : x \in \mathcal{F}$
7. if $\mathbb{F}\varphi \vee \psi : x \in \mathcal{F}$, then $\mathbb{F}\varphi : x \in \mathcal{F}$ and $\mathbb{F}\psi : x \in \mathcal{F}$
8. if $\mathbb{T}\varphi \rightarrow \psi : x \in \mathcal{F}$, then, for all $y \in \mathbb{L}$, if $x \leq y \in \overline{\mathcal{C}}$, then $\mathbb{F}\varphi : y \in \mathcal{F}$ or $\mathbb{T}\psi : y \in \mathcal{F}$
9. if $\mathbb{F}\varphi \rightarrow \psi : x \in \mathcal{F}$, then there exists $y \in \mathbb{L}$ such that $x \leq y \in \overline{\mathcal{C}}$ and $\mathbb{T}\varphi : y \in \mathcal{F}$ and $\mathbb{F}\psi : y \in \mathcal{F}$
10. if $\mathbb{T}\varphi \blacktriangleright \psi : x \in \mathcal{F}$, then there are $c_i, c_j \in \Sigma$ such that $c_i c_j \leq x \in \overline{\mathcal{C}}$ and $\mathbb{T}\varphi : c_i \in \mathcal{F}$ and $\mathbb{T}\psi : c_j \in \mathcal{F}$

11. if $\mathbb{F}\varphi \blacktriangleright \psi : x \in \mathcal{F}$, then, for all $c_i, c_j \in \Sigma$, if $c_i c_j \leq x \in \overline{\mathcal{C}}$, then
 $\mathbb{F}\varphi : c_i \in \mathcal{F}$ or $\mathbb{F}\psi : c_j \in \mathcal{F}$
12. if $\mathbb{T}\varphi \blacktriangleright \psi : x \in \mathcal{F}$, then, for all $c_i, c_j \in \Sigma$, if $x \leq c_i \in \overline{\mathcal{C}}$ and $c_i c_j \in \mathcal{D}(\overline{\mathcal{C}})$, then
 $\mathbb{F}\varphi : c_j \in \mathcal{F}$ or $\mathbb{T}\psi : c_i c_j \in \mathcal{F}$
13. if $\mathbb{F}\varphi \blacktriangleright \psi : x \in \mathcal{F}$, then there are $c_i, c_j \in \Sigma$ such that $x \leq c_i \in \overline{\mathcal{C}}$ and $c_i c_j \in \mathcal{D}(\overline{\mathcal{C}})$ and
 $\mathbb{T}\varphi : c_j \in \mathcal{F}$ and $\mathbb{F}\psi : c_i c_j \in \mathcal{F}$
14. if $\mathbb{T}\varphi \blacktriangleright \psi : x \in \mathcal{F}$, then, for all $c_i, c_j \in \Sigma$, if $x \leq c_i \in \overline{\mathcal{C}}$ and $c_j c_i \in \mathcal{D}(\overline{\mathcal{C}})$, then
 $\mathbb{F}\varphi : c_j \in \mathcal{F}$ or $\mathbb{T}\psi : c_j c_i \in \mathcal{F}$
15. if $\mathbb{F}\varphi \blacktriangleright \psi : x \in \mathcal{F}$, then there are $c_i, c_j \in \Sigma$ such that $x \leq c_i \in \overline{\mathcal{C}}$ and $c_j c_i \in \mathcal{D}(\overline{\mathcal{C}})$ and
 $\mathbb{T}\varphi : c_j \in \mathcal{F}$ and $\mathbb{F}\psi : c_j c_i \in \mathcal{F}$. □

We now give the definition of a function Ω that extracts a countermodel from a Hintikka CSS. A Hintikka CSS can thus be seen as the *labelled* tableaux counterpart of Hintikka sets, which are maximally consistent sets satisfying a subformula property.

Definition 12 (Function Ω). Let $\langle \mathcal{F}, \mathcal{C} \rangle$ be a Hintikka CSS. The function Ω associates to $\langle \mathcal{F}, \mathcal{C} \rangle$ a tuple $\Omega(\langle \mathcal{F}, \mathcal{C} \rangle) = (\mathcal{G}, \mathcal{E}, X, \leq, \mathcal{V})$, such that (1) $V(\mathcal{G}) = \mathcal{A}(\mathcal{C})$, (2) $E(\mathcal{G}) = \{(c_i, c_j) \mid c_i c_j \in \mathcal{D}(\mathcal{C})\} = \mathcal{E}$, $X = \{x^\Omega \mid x \in \mathcal{D}(\mathcal{C})\}$, where $V(c_i^\Omega) = \{c_i\}$, $E(c_i^\Omega) = \emptyset$, $V((c_i c_j)^\Omega) = \{c_i c_j\}$, and $E((c_i c_j)^\Omega) = \{(c_i, c_j)\}$, (3) $x^\Omega \leq y^\Omega$ iff $x \leq y \in \overline{\mathcal{C}}$, and (4) $x^\Omega \in \mathcal{V}(p)$ iff there exists $y \in \mathcal{D}(\mathcal{C})$ such that $y \leq x \in \overline{\mathcal{C}}$ and $\mathbb{T}p : y \in \mathcal{F}$. □

The next lemma shows that there is a precise correspondence between the structure that the Hintikka CSS properties impose on the labels and the layered structure specified by the construction of the model.

Lemma 5. Let $\langle \mathcal{F}, \mathcal{C} \rangle$ be a Hintikka CSS and $\Omega(\langle \mathcal{F}, \mathcal{C} \rangle) = (\mathcal{G}, \mathcal{E}, X, \leq, \mathcal{V})$. (1) If $c_i, c_j \in \mathcal{A}(\mathcal{C})$, then $c_i c_j \in \mathcal{D}(\mathcal{C})$ iff $c_i^\Omega @_{\mathcal{E}} c_j^\Omega \downarrow$. (2) If $c_i c_j \in \mathcal{D}(\mathcal{C})$, then $(c_i c_j)^\Omega = c_i^\Omega @_{\mathcal{E}} c_j^\Omega$. 3. $x^\Omega @_{\mathcal{E}} y^\Omega \downarrow$ iff there exist $c_i, c_j \in \mathcal{A}(\mathcal{C})$ s.t. $x = c_i$, $y = c_j$ and $c_i c_j \in \mathcal{D}(\mathcal{C})$. □

Lemma 6. Let $\langle \mathcal{F}, \mathcal{C} \rangle$ be a Hintikka CSS. $\Omega(\langle \mathcal{F}, \mathcal{C} \rangle)$ is a layered graph model. □

Lemma 7. Let $\langle \mathcal{F}, \mathcal{C} \rangle$ be a Hintikka CSS and $\mathcal{M} = \Omega(\langle \mathcal{F}, \mathcal{C} \rangle) = (\mathcal{G}, \mathcal{E}, X, \leq, \mathcal{V})$. For all formulas $\varphi \in \mathcal{L}$, and all $x \in \mathcal{D}(\mathcal{C})$. we have (1) if $\mathbb{F}\varphi : x \in \mathcal{F}$, then $x^\Omega \not\models_{\mathcal{M}} \varphi$, and (2) if $\mathbb{T}\varphi : x \in \mathcal{F}$, then $x^\Omega \models_{\mathcal{M}} \varphi$. Hence, if $\mathbb{F}\varphi : x \in \mathcal{F}$, then φ is not valid and $\Omega(\langle \mathcal{F}, \mathcal{C} \rangle)$ is a countermodel of φ . □

This construction of a countermodel would fail in a labelled tableaux system for LGL (i.e., the layered graph logic with classical additives [9]). This is because it is impossible to construct the internal structure of each subgraph in the model systematically, as the classical semantics for \blacktriangleright demands strict equality between the graph under interpretation and the decomposition into layers. This issue is sidestepped for ILGL since each time the tableaux rules require a decomposition of a subgraph into layers we can move to a ‘fresh’ layered subgraph further down the ordering. Thus we can safely turn each graph label into the simplest instantiation of the kind of graph it represents: either a single vertex (indecomposable) or two vertices and an edge (layered).

We now show how to construct such a CSS. We first require a listing of all labelled formulae that may need to be added to the CSS in order to satisfy properties 4–15. We require a particularly strong condition on the listing to make this procedure work: that every labelled formula appears infinitely often to be tested.

Definition 13 (Fair strategy). A fair strategy for a language \mathcal{L} is a labelled sequence of formulae $(\mathbb{S}_i \mathcal{X}_i : (x_i))_{i \in \mathbb{N}}$ in $\{\mathbb{T}, \mathbb{F}\} \times \mathcal{L} \times \mathbb{L}$ such that $\{i \in \mathbb{N} \mid \mathbb{S}_i \mathcal{X}_i : (x_i) \equiv \mathbb{S} \mathcal{X} : x\}$ is infinite for any $\mathbb{S} \mathcal{X} : x \in \{\mathbb{T}, \mathbb{F}\} \times \mathcal{L} \times \mathbb{L}$. \square

Proposition 4. There exists a fair strategy for the language of ILGL. \square

Next we need the concept of an oracle. Here an oracle allows Hintikka sets to be constructed inductively, testing the required consistency properties at each stage.

Definition 14. Let \mathcal{P} be a set of CSSs. (1) \mathcal{P} is \subseteq -closed if $\langle \mathcal{F}, \mathcal{C} \rangle \in \mathcal{P}$ holds whenever $\langle \mathcal{F}, \mathcal{C} \rangle \subseteq \langle \mathcal{F}', \mathcal{C}' \rangle$ and $\langle \mathcal{F}', \mathcal{C}' \rangle \in \mathcal{P}$ holds. (2) \mathcal{P} is of finite character if $\langle \mathcal{F}, \mathcal{C} \rangle \in \mathcal{P}$ holds whenever $\langle \mathcal{F}_f, \mathcal{C}_f \rangle \in \mathcal{P}$ holds for every $\langle \mathcal{F}_f, \mathcal{C}_f \rangle \subseteq_f \langle \mathcal{F}, \mathcal{C} \rangle$. (3) \mathcal{P} is saturated if, for any $\langle \mathcal{F}, \mathcal{C} \rangle \in \mathcal{P}$ and any instance

$$\frac{\text{cond}(\mathcal{F}, \mathcal{C})}{\langle \mathcal{F}_1, \mathcal{C}_1 \rangle \mid \dots \mid \langle \mathcal{F}_k, \mathcal{C}_k \rangle}$$

of a rule of Figure 6 if $\text{cond}(\mathcal{F}, \mathcal{C})$ is fulfilled, then $\langle \mathcal{F} \cup \mathcal{F}_i, \mathcal{C} \cup \mathcal{C}_i \rangle \in \mathcal{P}$, for at least one $i \in \{1, \dots, k\}$. \square

Definition 15 (Oracle). An oracle is a set of open CSSs which is \subseteq -closed, of finite character, and saturated. \square

Definition 16 (Consistency/finite consistency). Let $\langle \mathcal{F}, \mathcal{C} \rangle$ be a CSS. We say $\langle \mathcal{F}, \mathcal{C} \rangle$ is consistent if it is finite and has no closed tableau. We say $\langle \mathcal{F}, \mathcal{C} \rangle$ is finitely consistent if every finite sub-CSS $\langle \mathcal{F}_f, \mathcal{C}_f \rangle$ is consistent. \square

Proposition 5. (1) Consistency is \subseteq -closed. (2) A finite CSS is consistent iff it is finitely consistent. \square

Lemma 8. The set of finitely consistent CSS, \mathcal{P} , is an oracle. \square

We can now show completeness of our tableaux system. Consider a formula φ for which there exists no closed tableau. We show there is a countermodel to φ . We start with the initial tableau \mathcal{T}_0 for φ . Then, we have (1) $\mathcal{T}_0 = [\langle \{\mathbb{F}\varphi : c_0\}, \{c_0 \leq c_0\} \rangle]$ and (2) \mathcal{T}_0 cannot be closed. Let \mathcal{P} be as in Lemma 8. By Proposition 4, there exists a fair strategy, which we denote by \mathcal{S} , with $\mathbb{S}_i \mathcal{X}_i : (x_i)$ the i^{th} formula of \mathcal{S} . As \mathcal{T}_0 cannot be closed, $\langle \{\mathbb{F}\varphi : c_0\}, \{c_0 \leq c_0\} \rangle \in \mathcal{P}$. We build a sequence $\langle \mathcal{F}_i, \mathcal{C}_i \rangle_{i \geq 0}$ as follows:

- $\langle \mathcal{F}_0, \mathcal{C}_0 \rangle = \langle \{\mathbb{F}\varphi : c_0\}, \{c_0 \leq c_0\} \rangle$;
- if $\langle \mathcal{F}_i \cup \{\mathbb{S}_i \mathcal{X}_i : (x_i)\}, \mathcal{C}_i \rangle \notin \mathcal{P}$, then we have $\langle \mathcal{F}_{i+1}, \mathcal{C}_{i+1} \rangle = \langle \mathcal{F}_i, \mathcal{C}_i \rangle$; and
- if $\langle \mathcal{F}_i \cup \{\mathbb{S}_i \mathcal{X}_i : (x_i)\}, \mathcal{C}_i \rangle \in \mathcal{P}$, then we have $\langle \mathcal{F}_{i+1}, \mathcal{C}_{i+1} \rangle = \langle \mathcal{F}_i \cup \{\mathbb{S}_i \mathcal{X}_i : (x_i)\} \cup F_e, \mathcal{C}_i \cup C_e \rangle$ such that F_e and C_e are determined by

\mathbb{S}_i	\mathcal{X}_i	F_e	C_e
\mathbb{F}	$\varphi \rightarrow \psi$	$\{\mathbb{T}\varphi : c_{\mathfrak{S}+1}, \mathbb{F}\psi : c_{\mathfrak{S}+1}\}$	$\{x_i \leq c_{\mathfrak{S}+1}\}$
\mathbb{T}	$\varphi \blacktriangleright \psi$	$\{\mathbb{T}\varphi : c_{\mathfrak{S}+1}, \mathbb{T}\psi : c_{\mathfrak{S}+2}\}$	$\{c_{\mathfrak{S}+1} c_{\mathfrak{S}+2} \leq x_i\}$
\mathbb{F}	$\varphi \blacktriangleright \psi$	$\{\mathbb{T}\varphi : c_{\mathfrak{S}+2}, \mathbb{F}\psi : c_{\mathfrak{S}+1} c_{\mathfrak{S}+2}\}$	$\{x_i \leq c_{\mathfrak{S}+1}, c_{\mathfrak{S}+1} c_{\mathfrak{S}+2} \leq c_{\mathfrak{S}+1} c_{\mathfrak{S}+2}\}$
\mathbb{F}	$\varphi \blacktriangleright \psi$	$\{\mathbb{T}\varphi : c_{\mathfrak{S}+2}, \mathbb{F}\psi : c_{\mathfrak{S}+2} c_{\mathfrak{S}+1}\}$	$\{x_i \leq c_{\mathfrak{S}+1}, c_{\mathfrak{S}+2} c_{\mathfrak{S}+1} \leq c_{\mathfrak{S}+2} c_{\mathfrak{S}+1}\}$
Otherwise		\emptyset	\emptyset

with $\mathfrak{S} = \max\{j \mid c_j \in \mathcal{A}(\mathcal{C}_i) \cup \mathcal{S}(x_i)\}$.

Proposition 6. For any $i \in \mathbb{N}$, the following properties hold: (1) $\mathcal{F}_i \subseteq \mathcal{F}_{i+1}$ and $C_i \subseteq C_{i+1}$; (2) $\langle \mathcal{F}_i, C_i \rangle \in \mathcal{P}$. \square

We now define the limit $\langle \mathcal{F}_\infty, C_\infty \rangle = \langle \bigcup_{i \geq 0} \mathcal{F}_i, \bigcup_{i \geq 0} C_i \rangle$ of the sequence $\langle \mathcal{F}_i, C_i \rangle_{i \geq 0}$.

Proposition 7. The following properties hold: (1) $\langle \mathcal{F}_\infty, C_\infty \rangle \in \mathcal{P}$; (2) For all labelled formulae $\mathbb{S}\varphi : x$, if $\langle \mathcal{F}_\infty \cup \{\mathbb{S}\varphi : x\}, C_\infty \rangle \in \mathcal{P}$, then $\mathbb{S}\varphi : x \in \mathcal{F}_\infty$. \square

Lemma 9. The limit CSS is a Hintikka CSS. \square

Theorem 2 (Completeness). If φ is valid, then there exists a closed tableau for φ . \square

4 A Hilbert system and an algebraic semantics

We give a Hilbert-type proof system, ILGL_H , for ILGL in Figure 7. The additive fragment, corresponding to intuitionistic propositional logic, is standard (e.g., [4]). The presentation of the multiplicative fragment is similar to that for BI's multiplicatives [29], but for the non-commutative and non-associative (following from the absence of a multiplicative counterpart to \wedge_2) conjunction, \blacktriangleright , together with its associated left and right implications (cf. [20–23]).

$$\begin{array}{c}
\frac{}{\varphi \vdash \varphi} \text{(Ax)} \quad \frac{\varphi \vdash \psi \quad \psi \vdash \chi}{\varphi \vdash \chi} \text{(Cut)} \quad \frac{}{\varphi \vdash \top} \text{(T)} \quad \frac{}{\perp \vdash \varphi} \text{(\perp)} \\
\\
\frac{\varphi \vdash \psi \quad \varphi \vdash \chi}{\varphi \vdash \psi \wedge \chi} \text{(\wedge}_1\text{)} \quad \frac{}{\varphi_1 \wedge \varphi_2 \vdash \varphi_i} \text{(\wedge}_2\text{)} \quad \frac{}{\varphi_i \vdash \varphi_1 \vee \varphi_2} \text{(\vee}_1\text{)} \quad \frac{\varphi \vdash \chi \quad \psi \vdash \chi}{\varphi \vee \psi \vdash \chi} \text{(\vee}_2\text{)} \\
\\
\frac{\varphi \vdash \psi \rightarrow \chi \quad \nu \vdash \psi}{\varphi \wedge \nu \vdash \chi} \text{(\rightarrow}_1\text{)} \quad \frac{\varphi \wedge \psi \vdash \chi}{\varphi \vdash \psi \rightarrow \chi} \text{(\rightarrow}_2\text{)} \quad \frac{\varphi \vdash \psi \quad \chi \vdash \nu}{\varphi \blacktriangleright \chi \vdash \psi \blacktriangleright \nu} \text{(\blacktriangleright)} \\
\\
\frac{\varphi \vdash \psi \rightarrow \chi \quad \nu \vdash \psi}{\varphi \blacktriangleright \nu \vdash \chi} \text{(\blacktriangleright}_1\text{)} \quad \frac{\varphi \blacktriangleright \psi \vdash \chi}{\varphi \vdash \psi \rightarrow \chi} \text{(\blacktriangleright}_2\text{)} \quad \frac{\varphi \vdash \psi \blacktriangleright \chi \quad \nu \vdash \psi}{\nu \blacktriangleright \varphi \vdash \chi} \text{(\blacktriangleright}_1\text{)} \quad \frac{\varphi \blacktriangleright \psi \vdash \chi}{\psi \vdash \varphi \blacktriangleright \chi} \text{(\blacktriangleright}_2\text{)}
\end{array}$$

Fig. 7. Rules of the Hilbert system, ILGL_H , for ILGL

This section concludes with equivalence of ILGL_H and ILGL 's tableaux system.

Definition 17 (Layered Heyting algebra). A layered Heyting algebra is a structure $\mathbb{A} = (A, \wedge, \vee, \rightarrow, \perp, \top, \blacktriangleright, \blacktriangleright, \blacktriangleright)$ such that $(A, \wedge, \vee, \rightarrow, \perp, \top)$ is a Heyting algebra, $\blacktriangleright, \blacktriangleright, \blacktriangleright$ and \blacktriangleright are binary operations on A satisfying $a \leq a'$ and $b \leq b'$ implies $a \blacktriangleright b \leq a' \blacktriangleright b'$ and $a \blacktriangleright b \leq c$ iff $a \leq b \rightarrow c$ iff $b \leq a \blacktriangleright c$. \square

We interpret ILGL on layered Heyting algebras. Let $\mathcal{V} : \text{Prop} \rightarrow A$ be a valuation on the layered Heyting algebra $(A, \wedge_A, \vee_A, \rightarrow_A, \perp_A, \top_A, \blacktriangleright_A, \blacktriangleright_A, \blacktriangleright_A)$. We maintain the subscripts to distinguish the operations of the algebra from the connectives of ILGL . We uniquely define an interpretation function $\llbracket - \rrbracket : \text{Form} \rightarrow A$ by extending with respect to the connectives in the usual fashion: $\llbracket \top \rrbracket = \top_A$, $\llbracket \perp \rrbracket = \perp_A$, $\llbracket p \rrbracket = V(p)$, and $\llbracket \varphi \circ \psi \rrbracket = \llbracket \varphi \rrbracket \circ_A \llbracket \psi \rrbracket$ for $\circ \in \{\wedge, \vee, \rightarrow, \blacktriangleright, \blacktriangleright, \blacktriangleright\}$.

Proposition 8 (Soundness). *For any layered Heyting algebra \mathbb{A} and any interpretation $\llbracket - \rrbracket : \text{Form} \rightarrow \mathbb{A}$: if $\varphi \vdash \psi$ then $\llbracket \varphi \rrbracket \leq \llbracket \psi \rrbracket$.*

Proof. By induction on the derivation rules of ILGL_H . The cases for the additive fragment are standard. For rule (\blacktriangleright) , we use the property $a \leq_A a'$ and $b \leq_A b'$ implies $a \blacktriangleright_A b \leq_A a' \blacktriangleright_A b'$ and for the remaining rules pertaining to the multiplicative implications we use the adjointness property $a \blacktriangleright_A b \leq_A c$ iff $a \leq_A b \blackrightarrow_A c$ iff $b \leq_A a \blacktriangleright_A c$. \square

Lemma 10. *There is a layered Heyting algebra \mathcal{T} and an interpretation $\llbracket - \rrbracket_{\mathcal{T}} : \text{Prop} \rightarrow \mathcal{T}$ such that if $\varphi \not\vdash \psi$ then $\llbracket \varphi \rrbracket_{\mathcal{T}} \not\leq \llbracket \psi \rrbracket_{\mathcal{T}}$.*

Proof. We give a Lindenbaum term-algebra construction on the syntax of ILGL with the equivalence relation $\varphi \equiv \psi$ iff $\varphi \vdash \psi$ and $\psi \vdash \varphi$. The set of all such equivalence classes $[\varphi]$ gives the underlying set of the layered Heyting algebra, $\mathcal{T} : \top_{\mathcal{T}} := [\top]$, $\perp_{\mathcal{T}} := [\perp]$, and $[\varphi] \circ_{\mathcal{T}} [\psi] := [\varphi \circ \psi]$ for $\circ \in \{\wedge, \vee, \rightarrow, \blacktriangleright, \blackrightarrow, \blacktriangleright\}$.

The fragment $(\mathcal{T}, \wedge_{\mathcal{T}}, \vee_{\mathcal{T}}, \top_{\mathcal{T}}, \perp_{\mathcal{T}})$ forms a bounded distributive lattice with order $[\varphi] \leq_{\mathcal{T}} [\psi]$ iff $[\varphi] \wedge_{\mathcal{T}} [\psi] = [\varphi]$. It is straightforward to use rules (Ax) , (\wedge_1) and (\wedge_2) to show that the right hand condition holds iff $\varphi \vdash \psi$. We then obtain adjointness of $\wedge_{\mathcal{T}}$ and $\rightarrow_{\mathcal{T}}$ from rules (\rightarrow_1) and (\rightarrow_2) , monotonicity of $\blacktriangleright_{\mathcal{T}}$ from rule (\blacktriangleright) and the adjointness of $\blacktriangleright_{\mathcal{T}}, \blackrightarrow_{\mathcal{T}}$ and $\blacktriangleright_{\mathcal{T}}$ from rules (\blackrightarrow_1) , (\blackrightarrow_2) , (\blacktriangleright_1) , and (\blacktriangleright_2) . Thus \mathcal{T} is a layered Heyting algebra with an interpretation given by $\llbracket \varphi \rrbracket = [\varphi]$. By the definition of the ordering, $\varphi \not\vdash \psi$ implies $\llbracket \varphi \rrbracket \not\leq_{\mathcal{T}} \llbracket \psi \rrbracket$, as required. \square

We now standardly obtain completeness.

Theorem 3 (Completeness). *For any propositions φ, ψ of ILGL , if $\llbracket \varphi \rrbracket \leq \llbracket \psi \rrbracket$ for all interpretations $\llbracket - \rrbracket$ on layered Heyting algebras then $\varphi \vdash \psi$ in ILGL_H .* \square

We now show that the layered graph semantics is a special case of the algebraic semantics.

Definition 18 (Preordered layered magma). *A preordered layered magma is a tuple (X, \leq, \circ) , with X a set, \leq a preorder on X , and \circ a binary partial operation on X .* \square

It is clear that, given a preordered scaffold $(\mathcal{G}, \mathcal{E}, X, \leq)$, the structure $(X, \leq, @_{\mathcal{E}})$ is a preordered layered magma. Analogously to the classical case [9], we can generate a layered Heyting algebra.

Proposition 9. *Every preordered layered magma generates a layered Heyting algebra.*

Proof. Let (X, \leq, \circ) be a preordered layered magma. An up-set of the preorder (X, \leq) is a set $U \subseteq X$ such that $x \in U$ and $x \leq y$ implies $y \in U$. Denote the set of all up-sets of X by $\text{Up}(X)$. The structure $(\text{Up}(X), \cup, \cap, \rightarrow, \emptyset, X)$ is a Heyting algebra, where \rightarrow is defined as follows: $U \rightarrow V := \{x \in X \mid \text{for all } y (x \leq y \text{ and } y \in U \text{ implies } y \in V)\}$ We define the operators $\blacktriangleright, \blackrightarrow, \blacktriangleright$ as follows:

$$\begin{aligned} U \blacktriangleright V &:= \{x \in X \mid \text{there exists } y \in U, z \in V (y \circ z \downarrow \text{ and } y \circ z \leq x)\} \\ U \blackrightarrow V &:= \{x \in X \mid \text{for all } y, z (x \leq y \text{ and } y \circ z \downarrow \text{ and } z \in U \text{ implies } y \circ z \in V)\} \\ U \blacktriangleright V &:= \{x \in X \mid \text{for all } y, z (x \leq y \text{ and } z \circ y \downarrow \text{ and } z \in U \text{ implies } z \circ y \in V)\} \end{aligned}$$

It is straightforward that these all define up-sets, and are thus well-defined. It remains to prove monotonicity of \blacktriangleright and adjointness of the operators. For monotonicity, let $U \subseteq U'$, $V \subseteq V'$ and $x \in U \blacktriangleright V$. Then there exist $y \in U \subseteq U'$ and $z \in V \subseteq V'$ such that $y \circ z \downarrow$ and $y \circ z \leq x$. It follows immediately that $x \in U' \blacktriangleright V'$.

Next, adjointness. We give just one case, for \blacktriangleright . The others are similar. Suppose $V \subseteq U \blacktriangleright W$. We must show $U \blacktriangleright V \subseteq W$, so assume $x \in U \blacktriangleright V$. It follows that there exist $x_0 \in U$ and $x_1 \in V$ such that $x_0 \circ x_1 \downarrow$ and $x_0 \circ x_1 \leq x$. By assumption, $x_1 \in U \blacktriangleright W$ and we have $x_1 \leq x_1$, $x_0 \circ x_1 \downarrow$ and $x_0 \in U$, so it follows that $x_0 \circ x_1 \in W$. Finally, W is an up-set, so $x_0 \circ x_1 \leq x$ entails $x \in W$, and the verification is complete. \square

We can now get the soundness and completeness of the layered graph semantics with respect to ILGL_H as a special case of the algebraic semantics. Note that a *persistent* valuation $\mathcal{V} : \text{Prop} \rightarrow \wp(X)$ corresponds uniquely to a valuation $\mathcal{V}' : \text{Prop} \rightarrow \text{Up}(X)$. By definition, for each propositional variable p , $\mathcal{V}(p)$ is an up-set of the preorder (X, \leq) and trivially an up-set of (X, \leq) is an element of $\wp(X)$. We can thus use a persistent valuation to generate an interpretation $\llbracket - \rrbracket_{\mathcal{V}}$ on the layered Heyting algebra generated by $(X, \leq, @_{\mathcal{E}})$.

Proposition 10. *For any layered graph model M with valuation $\mathcal{V} : \text{Prop} \rightarrow \wp(X)$ and every formula φ of ILGL , we have $\llbracket \varphi \rrbracket_{\mathcal{V}} = \{G \in X \mid G \models_M \varphi\} \in \text{Up}(X)$.* \square

Hence the layered graph semantics of ILGL is a special case of the algebraic semantics and ILGL_H is sound and complete with respect to the layered graph semantics.

Proposition 11 (Equivalence of the Hilbert and tableaux systems). *$\vdash \varphi$ is provable in ILGL_H iff there is closed tableau for φ .* \square

5 Extension to resources and actions: examples

To express the examples mentioned in Section 1 conveniently and efficiently, we consider an extension of layered graph semantics and ILGL in which we label the ambient graph with resources and consider action modalities (cf. Stirling's intuitionistic Hennessy–Milner logic [32]) that express resource manipulations. This extension introduces a degree of statefulness to ILGL without changing the underlying semantics.

This extension is based on an assignment of a set of resources R to the vertices of the graph G . That is, each $r \in R$ is situated at vertices of G . Such assignments are denoted $G[R]$, where we think of G as the (directed) graph of locations in a system model. Resources should also carry sufficient structure to allow some basic operations on resource elements. In [26, 8, 7], resources are required to form pre-ordered partial monoids, such as the natural numbers $(\mathbb{N}, \leq, +, 0)$, and we use this approach here. Let $(\mathcal{R}, \sqsubseteq, \circ, e)$ be a resource monoid, where \mathcal{R} is a collection of sets of resources and $\circ : \mathcal{R} \times \mathcal{R} \rightarrow \mathcal{R}$ is a commutative and associative binary operation. It is easy to see that assignments of resources can be composed and that the algebraic semantics can be easily extended (cf. [9]).

Lemma 11. *Consider $@$ and \circ . Both are binary operations with $@$ non-commutative and non-associative while \circ is commutative and associative. A non-commutative, non-associative operation on graphs labelled with resources can be defined.*

Proof. We have $@_{\mathcal{E}} : \mathcal{G} \times \mathcal{G} \rightarrow \mathcal{G}$ and $\circ : \mathcal{R} \times \mathcal{R} \rightarrow \mathcal{R}$. Define $\bullet_{\mathcal{E}} : (\mathcal{G} \times \mathcal{R}) \times (\mathcal{G} \times \mathcal{R}) \rightarrow (\mathcal{G} \times \mathcal{R})$ as $(G_1, R_1) \bullet_{\mathcal{E}} (G_2, R_2) = (G_1 @_{\mathcal{E}} G_2, R_1 \circ R_2)$. It is clear that $\bullet_{\mathcal{E}}$ is both non-commutative and non-associative. \square

We write $G[R] \leq G'[R']$ to denote the evident containment ordering on labelled graphs and resources (i.e., G' is a subgraph of G and $R \sqsubseteq R'$). We assume also a countable set Act of actions, with elements a , etc.. Action modalities, $\langle a \rangle$ and $[a]$ manipulate (e.g., add to, remove from) the resources assigned to the vertices of the graph.

Definition 19 (Satisfaction in resource-labelled models). *We extend layered graph models to graphs labelled with resources and extend the interpretation of formulae to the action modalities. For a resource monoid \mathcal{R} , a countable set of actions, Act , and a layered graph model $\mathcal{M} = (X, \mathcal{V})$ over labelled graphs, with the containment ordering on labelled graphs, we generate the satisfaction relation $\models_{\mathcal{M}} \subseteq X[R] \times Form$ as*

$$\begin{aligned}
& G[R] \models_{\mathcal{M}} \top \text{ always} & G[R] \models_{\mathcal{M}} \perp \text{ never} & G[R] \models_{\mathcal{M}} p \text{ iff } G[R] \in \mathcal{V}(p) \\
& G[R] \models_{\mathcal{M}} \varphi \wedge \psi \text{ iff } G[R] \models_{\mathcal{M}} \varphi \text{ and } G[R] \models_{\mathcal{M}} \psi & G[R] \models_{\mathcal{M}} \varphi \vee \psi \text{ iff } G[R] \models_{\mathcal{M}} \varphi \text{ or } G[R] \models_{\mathcal{M}} \psi \\
& G[R] \models_{\mathcal{M}} \varphi \rightarrow \psi \text{ iff, for all } G'[R'] \text{ such that } G[R] \leq G'[R'], G'[R'] \models_{\mathcal{M}} \varphi \text{ implies } G'[R'] \models_{\mathcal{M}} \psi \\
& G[R] \models_{\mathcal{M}} \varphi_1 \blacktriangleright \varphi_2 \text{ iff for some } G_1[R_1], G_2[R_2] \text{ such that } G_1[R_1] \bullet_{\mathcal{E}} G_2[R_2] \leq G[R], \\
& \quad G_1[R_1] \models_{\mathcal{M}} \varphi_1 \text{ and } G_2[R_2] \models_{\mathcal{M}} \varphi_2 \\
& G[R] \models_{\mathcal{M}} \varphi \rightarrow \psi \text{ iff for all } G[R] \leq H[S] \text{ and all } K[T] \text{ such that } H[S] \bullet_{\mathcal{E}} K[T] \downarrow, \\
& \quad K[T] \models_{\mathcal{M}} \varphi \text{ implies } (H[S] \bullet_{\mathcal{E}} K[T]) \models_{\mathcal{M}} \psi \\
& G[R] \models_{\mathcal{M}} \varphi \blacktriangleright \psi \text{ iff for all } G[R] \leq H[S] \text{ and all } K[T] \text{ with } K[T] \bullet_{\mathcal{E}} H[S] \downarrow, \\
& \quad K[T] \models_{\mathcal{M}} \varphi \text{ implies } (K[T] \bullet_{\mathcal{E}} H[S]) \models_{\mathcal{M}} \psi \\
& G[R] \models_{\mathcal{M}} \langle a \rangle \varphi \text{ iff for some well-formed } G'[R'] \text{ such that } G[R] \xrightarrow{a} G'[R'], G'[R'] \models_{\mathcal{M}} \varphi \\
& G[R] \models_{\mathcal{M}} [a] \varphi \text{ iff for all well-formed } G'[R'] \text{ such that } G[R] \xrightarrow{a} G'[R'], G'[R'] \models_{\mathcal{M}} \varphi \quad \square
\end{aligned}$$

We defer the presentation of the metatheory to account for this extension, including proof systems and completeness results, to another occasion. To do so we follow the approach of dynamic epistemic logics [33], wherein the transitions underlying the action modalities correspond to maps between models rather than states. It is clear persistence will not (and should not) hold for action modalities, but at any given model persistence will hold. To extend the tableaux system we should instead take sequences of CSSs, together with a history of actions following similar approaches in the proof theory of Public Announcement Logic [3].

Example 1 (A transportation network). Here we abstract a public transportation network into social and infrastructure layers. For a meeting in the social layer to be quorate, sufficient people (say 50) must attend. To achieve this, there must be a buses of sufficient capacity to transport 50 people, represented as resources, to the meeting hall, in the infrastructure layer (see Figures 8 and 9). The formula ϕ_{quorum} denotes a quorate meeting, ϕ_x denotes that x number of people are picked up at bus stops, and the arrival of buses of capacity x in the infrastructure layer is denoted by the action modality $\langle bus_x \rangle$. These actions move x amount of people from the bus stops to the meeting hall in the social layer. Let $\phi_{meeting}$ assert the existence of a meeting in the social layer, G_1 . Then, if G_2 denotes the graph of the infrastructure layer, we have the formulae

$$\begin{aligned}
G_2[R] \models_{\mathcal{M}} \langle bus_{25} \rangle \langle bus_{35} \rangle (\phi_{meeting} \blacktriangleright \phi_{50}) \rightarrow \phi_{quorum} \\
G_2[R] \models_{\mathcal{M}} \langle bus_{40} \rangle (\phi_{meeting} \blacktriangleright \phi_{40}) \rightarrow \neg \phi_{quorum}
\end{aligned}$$

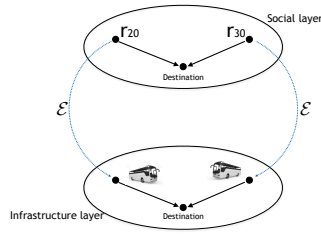


Fig. 8. Buses ready to roll

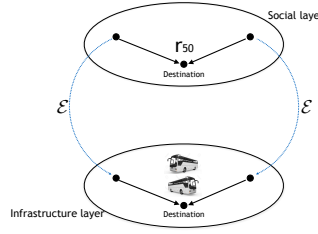


Fig. 9. Buses arrive at meeting

which assert that having two buses available with a total capacity of more than 50 will allow the meeting to proceed, but that a single bus with capacity 40 will not.

Example 2 (A security barrier). This example (see Figure 10) is a situation highlighted by Schneier [30], wherein a security system is ineffective because of the existence of a side-channel that allows a control to be circumvented. The security policy, as expressed

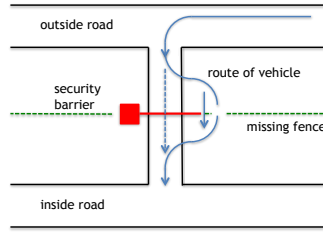


Fig. 10. The security barrier and side channel

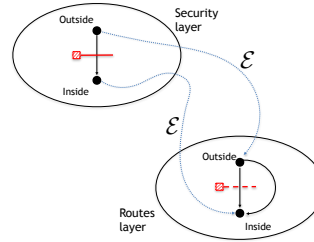


Fig. 11. The layered graph model

in the security layer, with graph G_1 , requires that a token be possessed in order to pass from from the outside to the inside; that is, $\langle \text{pass} \rangle (\phi_{\text{inside}} \rightarrow \phi_{\text{token}})$. However, in the routes layer, with graph G_2 , it is possible to perform an action $\langle \text{swerve} \rangle$ to drive around the gate, as shown in the Figure 11; that is,

$$G_1 @_{\mathcal{E}} G_2 \models_{\mathcal{M}} (\langle \text{pass} \rangle (\phi_{\text{inside}} \rightarrow \phi_{\text{token}}) \blacktriangleright \langle \text{swerve} \rangle (\phi_{\text{inside}} \wedge \neg \phi_{\text{token}}))$$

Thus we can express the mismatch between the security policy and architecture to which it is intended to apply.

Example 3 (An organizational security architecture). Our final example concerns an organization which internally has high- and low-security parts of its network. It also operates mobile devices that are outside of its internal network but able to connect to it. Figure 12 illustrates our layered graph model of this set-up. We can give a characterization in ILGL of a side channel that allows a resource from the high-security part of the internal network to transfer to the low-security part via the external mobile connection.

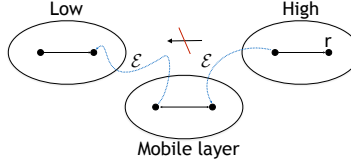


Fig. 12. Organizational Security Architecture

Associated with the mobile layer are actions that allow the transference We have two local compliance properties, in the high- and low-security parts of the network, respectively: $\chi_{\text{high}}(r)$ describes compliance with a policy allowing resource in the high-security network and $\chi_{\text{sec}}(r)$ is a correctness condition that if a resource r is not permitted in the low-security network, then it is not in it. We take actions copy, download, upload associated with the mobile layer G_2 , allowing data to be copied to another location as well as moved down and up \mathcal{E} -edges respectively, with $\theta(r)$ a compliance property such that $G_2[R] \models_{\mathcal{M}} \langle \text{copy} \rangle \theta(r)$ in order to copy data r . Now we have that

$$G_2[R] \models_{\mathcal{M}} \langle \text{download} \rangle (\chi_{\text{high}}(r) \blacktriangleright \theta(r)) \wedge \langle \text{copy} \rangle \langle \text{upload} \rangle (\theta(r) \blacktriangleright \neg \chi_{\text{sec}}(r))$$

showing that the mobile layer is a side channel that can undermine the policy χ_{sec} .

6 Conclusions and further work

Much meta-theoretic work remains to be done. In particular, a decidability result. ILGL is closely related to BI, a logic which enjoys the finite model property (FMP). It is apparent that our countermodel construction method is irreducibly infinite. However, if, as in BI, we base the tableaux system on the algebraic semantics, we conjecture we will obtain the FMP. The similarity of ILGL to BI raises another possible line of inquiry. It has been shown [17] that BI faithfully embeds into its classical variant BBI: is the same true of ILGL and LGL? Similarly, it is clear that by considering the multiplicative connectives to be ternary modalities we obtain a modal intuitionistic logic of the sort described in (e.g., [31, 5, 13]). We wish to investigate if the connectives generalize the modalities of any of those systems. Besides this, we have already completed work on a display calculus with cut-elimination and topological semantics extending those of IPL.

More substantially, we wish to develop a modelling technology based on layered graph logics. A simple dynamic variant is given in Section 5 and we must first ensure its meta-theoretic foundations are sound, following our conjectured proof-sketch. From there we will build extensions which take seriously the notions of agent and resource. Preliminary work in this direction appears in the papers of one of us [11, 1, 2], but, unlike those papers, our approach will take inter-relations with architecture as a central notion.

References

1. G. Anderson and D. Pym. A calculus and logic of bunched resources and processes. *Theoretical Computer Science*, 614:63–96, 2016.
2. G. Anderson and D. Pym. A substructural modal logic of utility. Submitted. Manuscript at <http://www0.cs.ucl.ac.uk/staff/D.Pym/AndersonPymSubstModalUtility.pdf> (accessed 26 January 2016). Preliminary version presented at *Strategic Reasoning 2015*, St. Catharine’s College, Oxford, September 21–22, 2015, 2016.
3. P. Balbiani, H. van Ditmarsch, A. Herzig, and T. de Lima. Tableaux for public announcement logic. *Journal of Logic and Computation*, 20(1):55–76, 2008.
4. N. Bezhanishvili and D. de Jongh. Intuitionistic logic. Technical Report PP-2006-25, Institute for Logic, Language and Computation Universiteit van Amsterdam, 2006.
5. G. Bierman and V. de Paiva. On an intuitionistic modal logic. *Studia Logica*, 65:2000, 2001.
6. P. Bródka, K. Skibicki, P. Kazienko, and K. Musiał. A degree centrality in multi-layered social network. In *International Conference on Computational Aspects of Social Networks*, 2011.
7. M. Collinson, B. Monahan, and D. Pym. *A Discipline of Mathematical Systems Modelling*. College Publications, 2012.
8. M. Collinson and D. Pym. Algebra and logic for resource-based systems modelling. *Mathematical Structures in Computer Science*, 19(5):959–1027, 2009.
9. M. Collinson, K. McDonald, and D. Pym. A substructural logic for layered graphs. *Journal of Logic and Computation*, 24(4):953–988, 2014. Erratum at <http://logcom.oxfordjournals.org/content/early/2015/06/04/logcom.exv019.full.pdf+html>. doi: 10.1093/logcom/exv019.
10. 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.
11. J.-R. Courtault, D. Galmiche, and D. Pym. A logic of separating modalities. Submitted. Manuscript at <http://www0.cs.ucl.ac.uk/staff/D.Pym/CGP15.pdf> (accessed 26 January 2016), 2015.
12. J.-R. Courtault. *Logiques de ressources dynamiques: modèles, propriétés et preuves*. PhD thesis, Université de Lorraine, 2015.
13. V. de Paiva. Intuitionistic modal logic: 15 years later <http://logic.berkeley.edu/colloquium/dePaivaSlides.pdf> (accessed 26 January 2016).
14. A. Fiat, D. Foster, H. Karloff, Y. Rabani, Y. Ravid, and S. Vishwanathan. Competitive algorithms for layered graph traversal. *SIAM Journal on Computing*, 28(2):447–462, 1998.
15. M. Fitting. Tableau methods of proof for modal logics. *Notre Dame J. Formal Logic*, 13(2):237–247, 04 1972.
16. D. Galmiche, D. Méry, and D. Pym. The semantics of BI and Resource Tableaux. *Math. Struct. in Comp. Science*, 15(6):1033–1088, 2005.
17. D. Galmiche and D. Larchey-Wendling. Expressivity properties of boolean bi through relational models. In *FSTTCS 2006: Foundations of Software Technology and Theoretical Computer Science*, volume 4337 of *LNCS*, pages 357–368, 2006.
18. D. Galmiche, D. Méry, and D. Pym. The semantics of BI and resource tableaux. *Mathematical Structures in Computer Science*, 15(06):1033–1088, 2005.
19. M. Kurant and P. Thiran. Layered complex networks. *Phys. Rev. Lett.*, 96:138701, Apr 2006.
20. J. Lambek. Deductive Systems and Categories I. *J. Math. Systems Theory*, 2:278–318, 1968.
21. J. Lambek. Deductive Systems and Categories II. *Springer LNM*, 86:76–122, 1969.
22. J. Lambek. Deductive Systems and Categories III. *Springer LNM*, 274:57–82, 1972.

23. J. Lambek. From categorical grammar to bilinear logic. In P. Schroeder-Heister and K. Došen, editors, *Substructural Logics*, pages 207–237. Oxford University Press, 1993.
24. 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.
25. D. Larchey-Wendling. The formal strong completeness of partial monoidal boolean bi. *Logic and Computation*, 2014.
26. P. O’Hearn and D. Pym. The logic of bunched implications. *Bulletin of Symbolic Logic*, 5(2):215–244, 1999.
27. C. Papadimitriou and M. Yannakakis. Shortest paths without a map. *Theoretical Computer Science*, 84(1):127–150, 1991.
28. A. Paz. A theory of decomposition into prime factors of layered interconnection networks. *Discrete Applied Mathematics*, 159(7):628–646, 2011.
29. D. Pym, P. O’Hearn, and H. Yang. Possible worlds and resources: The semantics of BI. *Theoretical Computer Science*, 315(1):257–305, 2004. Erratum: p. 285, l. -12: “, for some $P', Q \equiv P; P'$ ” should be “ $P \vdash Q$ ”.
30. B. Schneier. The weakest link (https://www.schneier.com/blog/archives/2005/02/the_weakest_lin.html). Schneier on Security (<https://www.schneier.com/>), 2005.
31. A. Simpson. *The Proof Theory and Semantics of Intuitionistic Modal Logic*. PhD thesis, University of Edinburgh, 1994.
32. C. Stirling. Modal logics for communication systems. *Theoretical Computer Science*, 49:311–347, 1987.
33. H. van Ditmarsch and Barteld Kooi Wiebe van der Hoek. *Dynamic Epistemic Logic*. Synthese Library, 2008.

A Proof of completeness of tableaux for layered graph semantics

We provide the proofs omitted from the body of the paper.

Proof (Lemma 5).

1. Let $c_i c_j \in \mathcal{D}(C)$. Then by CSS property (Contra) we have $c_j c_i \notin \mathcal{D}(C)$. Hence by definition of Ω we have $(c_i, c_j) \in \mathcal{E}$ and $(c_j, c_i) \notin \mathcal{E}$. Thus $c_i @_{\mathcal{E}} c_j \downarrow$ as required. The other direction is trivial.
2. Immediate from 1. and the definition of Ω .
3. The right-to-left direction is trivial, so assume $x^{\Omega} @_{\mathcal{E}} y^{\Omega} \downarrow$. There are three possible cases for x and y other than $x = c_i$ and $y = c_j$: we attend to one as the others are similar. Suppose $x = c_i c_j$ and $y = c_k$. Then $x^{\Omega} @_{\mathcal{E}} y^{\Omega} \downarrow$ must hold because of either $(c_i, c_k) \in \mathcal{E}$ or $(c_j, c_k) \in \mathcal{E}$. That is, $c_i c_k \in \mathcal{D}(C)$ or $c_j c_k \in \mathcal{D}(C)$. In both cases the CSS property (Freshness) is contradicted so neither can hold. It follows that only the case $x = c_i$ and $y = c_j$ is non-contradictory, and so by 1. $c_i c_j \in \mathcal{D}(C)$. \square

Proof (Lemma 6). \mathcal{G} is clearly a graph and \preceq being a preorder on X can be read off of the rules for the closure of constraint sets. Thus the only non-trivial aspects of the proof are that X is admissible and that \mathcal{V} is persistent.

- X is an admissible subgraph set.

Let $G, H \in \mathcal{Sg}(\mathcal{G})$ with $G @_{\mathcal{E}} H \downarrow$. First we assume $G, H \in X$. Then $G = x^{\Omega}$ and

$H = y^\Omega$ for labels x, y . By the previous lemma it follows that $x = c_i$ and $y = c_j$ and $c_i c_j \in \mathcal{D}(C)$. Thus $G @_\varepsilon H = c_i^\Omega @_\varepsilon c_j^\Omega = (c_i c_j)^\Omega \in X$. Now suppose $G @_\varepsilon H \in X$. Then $G @_\varepsilon H = x^\Omega$ for some $x \in \mathcal{D}(C)$. The case $x = c_i$ is clearly impossible as $E(c_i^\Omega) = \emptyset$ so necessarily $x = c_i c_j$. Then we have $c_i, c_j \in \mathcal{D}(C)$ as sub-labels of $c_i c_j$ and $c_i^\Omega @_\varepsilon c_j^\Omega \downarrow$ with $c_i^\Omega @_\varepsilon c_j^\Omega$ the only possible composition equal to $(c_i c_j)^\Omega$. It follows that $G = c_i^\Omega \in X$ and $H = c_j^\Omega \in X$ as required.

- \mathcal{V} is a persistent valuation.

Let $G \in \mathcal{V}(p)$ with $G \leq H$. Then $G = x^\Omega$ and $H = y^\Omega$ for some $x, y \in \mathcal{D}(C)$ with $x \leq y \in \overline{C}$. By definition of \mathcal{V} there exists $z \in \mathcal{D}(C)$ with $z \leq x \in \overline{C}$ and $\mathbb{T}p : z \in \mathcal{F}$. By closure rule $\langle Tr \rangle$ we have $z \leq y \in \overline{C}$ so $H = y^\Omega \in \mathcal{V}(p)$. \square

Proof (Lemma 7). We proceed by a simultaneous structural induction on φ .

- Base cases.

- Case $\mathbb{F}p : x \in \mathcal{F}$. We suppose that $x^\Omega \models_M p$. Then $x^\Omega \in \mathcal{V}(p)$. By the definition of \mathcal{V} , there is a label y such that $y \leq x \in \overline{C}$ and $\mathbb{T}p : y \in \mathcal{F}$. Then by condition (1) of Definition 11, $\langle \mathcal{F}, C \rangle$ is not a Hintikka CSS, a contradiction. It follows that $x^\Omega \not\models_M p$.
- Case $\mathbb{T}p : x \in \mathcal{F}$. By property (Ref), $x \leq x \in \overline{C}$. Thus, by definition of \mathcal{V} we have $x^\Omega \in \mathcal{V}(p)$. Thus $x^\Omega \models_M p$.
- Cases $\mathbb{F}\perp : x \in \mathcal{F}$, $\mathbb{T}\perp : x \in \mathcal{F}$, $\mathbb{F}\top : x$ and $\mathbb{T}\top : x$ are straightforward consequences of the definition of Hintikka CSS and the layered graph semantics.

- Inductive step. We now suppose that (1) and (2) hold for formulæ φ and ψ (IH). We attend only to the cases $\langle \mathbb{T} \rightarrow \rangle$, $\langle \mathbb{T} \blacktriangleright \rangle$ and $\langle \mathbb{T} \blacktriangleright \rangle$ as the others are similar.

- Case $\mathbb{T}\varphi \rightarrow \psi : x \in \mathcal{F}$. Suppose $x^\Omega \leq y^\Omega$. Then $x \leq y \in \overline{C}$ and by Definition 11 property (8) it follows that $\mathbb{F}\varphi : y \in \mathcal{F}$ or $\mathbb{T}\psi : y \in \mathcal{F}$. By (IH) it follows that if $y^\Omega \models_M \varphi$ then $y^\Omega \models_M \psi$ as required.
- Case $\mathbb{T}\varphi \blacktriangleright \psi : x \in \mathcal{F}$. By Definition 11 property (10) there exist labels $c_i, c_j \in \mathcal{D}(C)$ such that $c_i c_j \leq x \in \overline{C}$ and $\mathbb{T}\varphi : c_i \in \mathcal{F}$ and $\mathbb{T}\psi : c_j \in \mathcal{F}$. By (IH) we have $c_i^\Omega \models_M \varphi$ and $c_j^\Omega \models_M \psi$. Further, by definition of Ω we have that $(c_i c_j)^\Omega = c_i^\Omega @_\varepsilon c_j^\Omega \leq x^\Omega$, so $x^\Omega \models_M \varphi \blacktriangleright \psi$.
- Case $\mathbb{T}\varphi \blacktriangleright \psi : x \in \mathcal{F}$. Suppose $x^\Omega \leq y^\Omega$ with $y^\Omega @_\varepsilon z^\Omega \downarrow$ and $z^\Omega \models_M \varphi$. By Lemma 5 we know $y = c_i, z = c_j \in \mathcal{A}(C)$ with $c_i c_j \in \mathcal{D}(C)$. Hence by Definition 11 property 12, either $F\varphi : c_j \in \mathcal{F}$ or $T\psi : c_i c_j \in \mathcal{F}$. By (IH) it follows either $c_j^\Omega \models_M \varphi$ or $(c_i c_j)^\Omega = c_i^\Omega @_\varepsilon c_j^\Omega \models_M \psi$. As we know the former cannot be true, it must be the latter. Hence $x^\Omega \models_M \varphi \blacktriangleright \psi$ as required. \square

Proof (Proposition 4). See [25]. \square

Proof (Proposition 5). See [25]. \square

Proof (Lemma 8). For \subseteq -closure and finite character see [25]. We show the cases $\langle \mathbb{T} \blacktriangleright \rangle$ and $\langle \mathbb{T} \blacktriangleright \rangle$ for saturation: the rest are similar. Let $\langle \mathcal{F}, C \rangle \in \mathcal{P}$

- $\mathbb{T}\varphi \blacktriangleright \psi : x \in \mathcal{F}$. We show $\langle \mathcal{F} \cup \{\mathbb{T}\varphi : c_i, \mathbb{T}\psi : c_j\}, C \cup \{c_i c_j \leq x\} \rangle \in \mathcal{P}$. Let $\langle \mathcal{F}_f, C_f \rangle \subseteq_f \langle \mathcal{F} \cup \{\mathbb{T}\varphi : c_i, \mathbb{T}\psi : c_j\}, C \cup \{c_i c_j \leq x\} \rangle \in \mathcal{P}$. Since, $\mathbb{T}\varphi \blacktriangleright \psi : x \in \mathcal{F}$, by compactness, there exists $C_0 \subseteq_f C$ such that $x \leq x \in \overline{C_0}$. Now define

$$\mathcal{F}'_f = (\mathcal{F}_f \setminus \{\mathbb{T}\varphi : c_i, \mathbb{T}\psi : c_j\}) \cup \{\mathbb{T}\varphi \blacktriangleright \psi : x\}$$

$$C'_f = C_f \cup C_0$$

- Then $\langle \mathcal{F}'_f, C'_f \rangle$ is a CSS and $\langle \mathcal{F}'_f, C'_f \rangle \subseteq_f \langle \mathcal{F}, C \rangle$ so it is consistent. We have that $[\langle \mathcal{F}'_f \cup \{\mathbb{T}\varphi : c_i, \mathbb{T}\psi : c_j\}, C'_f \cup \{c_i c_j \leq x\} \rangle]$ is a tableau for $\langle \mathcal{F}'_f, C'_f \rangle$. Thus if it is possible for $\langle \mathcal{F}'_f \cup \{\mathbb{T}\varphi : c_i, \mathbb{T}\psi : c_j\}, C'_f \cup \{c_i c_j \leq x\} \rangle$ to be closed then so too is it for $\langle \mathcal{F}'_f, C'_f \rangle$: a contradiction. Hence it is consistent. We have that $\langle \mathcal{F}_f, C_f \rangle \subseteq \langle \mathcal{F}'_f \cup \{\mathbb{T}\varphi : c_i, \mathbb{T}\psi : c_j\}, C'_f \cup \{c_i c_j \leq x\} \rangle$ so $\langle \mathcal{F}_f, C_f \rangle$ is consistent by Proposition 5.
- $\mathbb{T}\varphi \blacktriangleright \psi : x \in \mathcal{F}$ and $x \leq y, yz \leq yz \in \overline{C}$. Suppose neither $\langle \mathcal{F} \cup \{\mathbb{F}\varphi : z\}, C \rangle \in \mathcal{P}$ nor $\langle \mathcal{F} \cup \{\mathbb{T}\psi : yz\}, C \rangle \in \mathcal{P}$. Then there exist $\langle \mathcal{F}_f^A, C_f^A \rangle \subseteq_f \langle \mathcal{F} \cup \{\mathbb{F}\varphi : z\}, C \rangle$ and $\langle \mathcal{F}_f^B, C_f^B \rangle \subseteq_f \langle \mathcal{F} \cup \{\mathbb{T}\psi : yz\}, C \rangle$ that are inconsistent. By compactness, there exist $C_0, C_1 \subseteq C$ such that $z \leq z \in C_0$ and $yz \leq yz \in C_1$. Thus we define $\mathcal{F}'_f = (\mathcal{F}_f^A \setminus \{\mathbb{F}\varphi : z\}) \cup (\mathcal{F}_f^B \setminus \{\mathbb{T}\psi : yz\}) \cup \{\mathbb{T}\varphi \blacktriangleright \psi : x\}$ and $C'_f = C_f^A \cup C_f^B \cup C_0 \cup C_1$. Then $\langle \mathcal{F}'_f, C'_f \rangle$ is a finite CSS and $[\langle \mathcal{F}'_f \cup \{\mathbb{F}\varphi : z\}, C'_f \rangle; \langle \mathcal{F}'_f \cup \{\mathbb{T}\psi : yz\}, C'_f \rangle]$ is a tableau for it. We have $\langle \mathcal{F}_f^A, C_f^A \rangle \subseteq_f \langle \mathcal{F}'_f \cup \{\mathbb{F}\varphi : z\}, C'_f \rangle$ and $\langle \mathcal{F}_f^B, C_f^B \rangle \subseteq_f \langle \mathcal{F}'_f \cup \{\mathbb{T}\psi : yz\}, C'_f \rangle$ so by \subseteq -closure of consistency $\langle \mathcal{F}'_f, C'_f \rangle$ and $\langle \mathcal{F}_f^B, C_f^B \rangle$ are inconsistent: respectively let \mathcal{T}_A and \mathcal{T}_B be closed tableaux for them. Then $\mathcal{T}_A \oplus \mathcal{T}_B$ is a closed tableau for $\langle \mathcal{F}'_f, C'_f \rangle$ and the CSS is inconsistent: contradicting $\langle \mathcal{F}'_f, C'_f \rangle \subseteq_f \langle \mathcal{F}, C \rangle \in \mathcal{P}$. \square

Proof (Proposition 6). Only 2 is non-trivial. and we prove it by induction on i . The base case $i = 0$ is given by our initial assumption. Now for the inductive hypothesis (IH) we have that $\langle \mathcal{F}_i, C_i \rangle \in \mathcal{P}$. Then the inductive step is an immediate consequence of Lemma 8 for the non-trivial cases. \square

Proof (Proposition 7).

1. First note that $\langle \mathcal{F}_\infty, C_\infty \rangle$ is a CSS since each stage of construction satisfies (Ref) and by our choice of constants throughout the construction (Contra) and (Freshness) are satisfied. Further, it is open since otherwise there would be some stage $\langle \mathcal{F}_k, C_k \rangle$ at which the offending closure condition is satisfied, which would contradict that each $\langle \mathcal{F}_i, C_i \rangle$ is consistent. Now let $\langle \mathcal{F}_f, C_f \rangle \subseteq_f \langle \mathcal{F}_\infty, C_\infty \rangle$. Then there exists $k \in \mathbb{N}$ such that $\langle \mathcal{F}_f, C_f \rangle \subseteq_f \langle \mathcal{F}_k, C_k \rangle$. By Proposition $\langle \mathcal{F}_k, C_k \rangle \in \mathcal{P}$ so it follows $\langle \mathcal{F}_f, C_f \rangle \in \mathcal{P}$. As \mathcal{P} is of finite character, we thus have $\langle \mathcal{F}_\infty, C_\infty \rangle \in \mathcal{P}$.
2. First note that $\langle \mathcal{F}_\infty \cup \{\mathbb{S}\varphi : x\}, C_\infty \rangle$ is a CSS so (Contra) and (Freshness) are satisfied when the label x is introduced. By compactness, there exists finite $C_0 \subseteq C_\infty$ such that $x \leq x \in \overline{C_0}$. As it is finite, there exists $k \in \mathbb{N}$ such that $C_0 \subseteq C_k$ and by fairness there exists $l \geq k$ such that $\mathbb{S}_l \chi_l : (x_l) \equiv \mathbb{S}\varphi : x$. Since (Freshness) and (Contra) are fulfilled with respect to \mathcal{F}_∞ they are also fulfilled with respect to $\mathcal{F}_l \cup \{\mathbb{S}\varphi : x\}$ so $\langle \mathcal{F}_{l+1}, C_{l+1} \rangle = \langle \mathcal{F}_l \cup \{\mathbb{S}\varphi : x\}, C_l \rangle \in \mathcal{P}$ and $\langle \mathcal{F}_{l+1}, C_{l+1} \rangle = \langle \mathcal{F}_l \cup \{\mathbb{S}\varphi : x\} \cup \mathcal{F}_e, C_l \cup C_e \rangle$. Hence $\mathbb{S}\varphi : x \in \mathcal{F}_\infty$. \square

Proof (Lemma 9). For properties (1)–(3) we have that $\langle \mathcal{F}_\infty, C_\infty \rangle$ is open. For the other conditions, the saturation property of the oracle \mathcal{P} and 2. of Proposition 7 suffice. \square

Proof (Theorem 2). Suppose there exists no proof for the formula φ . Then by Lemma 9 we can construct the Hintikka CSS $\langle \mathcal{F}_\infty, \mathcal{C}_\infty \rangle$ from $\mathcal{T}_0 = [\langle \{\mathbb{F}\varphi : c_0\}, \{c_0 \leq c_0\} \rangle]$ as outlined above, with $\mathbb{F}\varphi : c_0 \in \mathcal{F}_\infty$. Then by Lemma 7, $\Omega(\langle \mathcal{F}_\infty, \mathcal{C}_\infty \rangle)$ is a countermodel for φ . That is, φ is not valid.