# Propositional Lax Logic

Matt Fairtlough     Michael Mendler

Matt Fairtlough
University of Sheffield
Department of Computer Science
Regent Court
Sheffield S1 4DP, UK
Tel.: +44 114 282 5592
Fax.: +44 114 278 0972
Email: m.fairtlough@dcs.shef.ac.uk

Michael Mendler
University of Passau
Department of Computer Science
Innstraße 33
D-94032 Passau, Germany
Tel.: +49 851 509 3096
Fax: +49 851 509 3092
Email: mendler@fmi.uni-passau.de

M. Fairtlough, M. Mendler: Propositional Lax Logic. Information and Computation, Vol.137, No.1, 1997, pp. 1-33.

Proposed Running Head:

Propositional Lax Logic

Correspondence: Matt Fairtlough
University of Sheffield
Department of Computer Science
Regent Court
Sheffield S1 4DP, UK
Tel.: +44 114 282 5592
Fax.: +44 114 278 0972
Email: m.fairtlough@dcs.shef.ac.uk

M. Fairtlough, M. Mendler: Propositional Lax Logic. Information and Computation, Vol.137, No.1, 1997, pp. 1-33.

## Abstract

We investigate a peculiar intuitionistic modal logic, called Propositional Lax Logic (PLL), which has promising applications to the formal verification of computer hardware. The logic has emerged from an attempt to express correctness 'up to' behavioural constraints — a central notion in hardware verification — as a logical modality. As a modal logic it is special since it features a single modal operator $\bigcirc$ that has a flavour both of possibility and of necessity.

In the paper we provide the motivation for PLL and present several technical results. We investigate some of its proof-theoretic properties, presenting a cut-elimination theorem for a standard Gentzen-style sequent presentation of the logic. We go on to define a new class of fallible two-frame Kripke models for PLL. These models are unusual since they feature worlds with inconsistent information; furthermore, the only frame condition imposed is that the $\bigcirc$-frame be a subrelation of the $\supset$-frame. We give a natural translation of these models into Goldblatt's $\mathcal{J}$-space models of PLL. Our completeness theorem for these models yields a Gödel-style embedding of PLL into a classical bimodal theory of type (S4, S4) and underpins a simple proof of the finite model property. We proceed to prove soundness and completeness of several theories for specialized classes of models.

We conclude with a brief exploration of two concrete and rather natural types of model from hardware verification for which the modality $\bigcirc$ models correctness up to timing constraints. We obtain decidability of $\bigcirc$-free fragment of the logic of the first type of model, which coincides with the stable form of Maksimova's intermediate logic $L\Pi$.

M. Fairtlough, M. Mendler: Propositional Lax Logic. Information and Computation, Vol.137, No.1, 1997, pp. 1-33.

# 1 Introduction

The object of this paper is the rather curious modality $\bigcirc$ characterized by the axiom schemes

$$\begin{array}{lcl} \bigcirc R & : & M \supset \bigcirc M \\ \bigcirc M & : & \bigcirc\bigcirc M \supset \bigcirc M \\ \bigcirc S & : & (\bigcirc M \wedge \bigcirc N) \supset \bigcirc(M \wedge N) \end{array}$$

with the inference rule of Modus Ponens and the rule “from $M \supset N$ infer $\bigcirc M \supset \bigcirc N$”. From a classical point of view the combination of these three axioms does not make much sense, however innocent each of these axioms may appear. Indeed, $\bigcirc$ has a flavour of both possibility and of necessity without being one or the other. Axioms $\bigcirc R$ and $\bigcirc M$ are typical of a modality of possibility $\Diamond$ while $\bigcirc S$ is typical for necessity $\Box$. On the other hand, in standard systems, say Lewis' modal system S4 [Chellas, 1980], the axiom $\bigcirc R$ is never adopted for necessity while $\bigcirc S$ never for possibility. In fact, if we add the axiom of the Excluded Middle (EM) and $\neg\bigcirc \mathit{false}$ (which is valid for both $\Diamond$ and $\Box$) to the modal system $\bigcirc R$, $\bigcirc M$, $\bigcirc S$ then $\bigcirc$ becomes trivial. We can derive both $\bigcirc M \supset M$ and $M \supset \bigcirc M$. In other words, there is no classical Kripke semantics for $\bigcirc$. In an intuitionistic setting, however, the situation is different. There, modal operators like $\bigcirc$ arise very naturally in various different ways and under various different names. In the following let us list some of them in order to motivate the interest in $\bigcirc$.

(1) Historically, the earliest appearance of an operator like $\bigcirc$ may have been in Curry's 1948 Notre Dame lectures on *A Theory of Formal Deducibility* published in [Curry, 1957]. These lectures contain some sketchy remarks on a modality endowed with axiom schemata, further refined in [Curry, 1952], that are essentially equivalent to the ones for $\bigcirc$.

(2) Reading implication as an ordering relation, the axioms and rules for $\bigcirc$ specify a class of monotone operators that arise in the study of the lattice-theoretic properties of topological spaces. Such operators were termed *nuclei* by Simmons [Simmons, 1978] and Macnab [Macnab, 1981]. The algebraic structure of nuclei can be generalized to the notion of a *modal operator* on a Heyting algebra [Macnab, 1981]. Goldblatt has shown that these algebras, which he calls *local (Heyting) algebras*, provide an appropriate algebraic semantics for intuitionistic propositional logic with a $\bigcirc$ modality [Goldblatt, 1981]. Goldblatt uses the term *geometric modality* for $\bigcirc$. The algebraic structure further features in category theory as a generalization of Grothendieck topologies. There the modal operator $\bigcirc$ on an Heyting algebra, usually referred to by the symbol $j$, becomes a *topology* on an elementary topos, and the local algebra becomes an *elementary site*. The interested reader is referred to [Goldblatt, 1979].

(3) The algebraic approach essentially characterizes the formal behaviour of $\bigcirc$ internally by the way it relates to implication $\supset$. However, when one is interested in $\bigcirc$ as a logical modality one expects instead to assign external meaning in terms of truth and validity. So, it is natural to try to extend the standard Kripke semantics for intuitionistic logic to encompass the modality as well. In [Goldblatt, 1981] two such classes of intuitionistic Kripke semantics, called $\mathcal{J}$-spaces and $\mathcal{J}$-frames, are presented. In these models an underlying Kripke frame is used to interpret the intuitionistic implication while the modality is

interpreted by some extra data associated with the frame; in the first case this is a notion of neighbourhood and in the second case a notion of closeness of worlds. Both notions are conceived to give $\bigcirc M$ the meaning of "$M$ is locally true".

(4) A different motivation for $\bigcirc$ can be drawn from general type theory. The formal properties of $\bigcirc$ viewed as an unary type constructor give precisely the data of a strong monad familiar from category theory. In fact, the propositions-as-types principle which yields an equivalence between the Intuitionistic Propositional Calculus (IPC) and bi-Cartesian closed categories can be extended to an equivalence between IPC extended by $\bigcirc$ and bi-Cartesian closed categories with a strong monad. This categorical structure is also known as the computational lambda calculus $\lambda_c$ [Moggi, 1991]. Exploiting this connection strong monads have found their way into in functional programming, see *e.g.* their use in Haskell [Thompson, 1996]. The application of $\lambda_c$ as a calculus of proofs has been investigated by Benton *et al.* [Benton et al., 1993], where the logic of $\bigcirc$ is called *computational logic* (CL).

(5) Our interest in the modality stems from a proof-theoretic interpretation of $\bigcirc$ introduced in [Mendler, 1990, Mendler, 1993]. It investigates an application to hardware verification in which the modality $\bigcirc$ formalizes the notion of correctness up to constraints. The corresponding calculi are called *Lax Logics*, where the term 'lax' is chosen to indicate the looseness associated with the notion of correctness up to constraints. The intuitive interpretation of $\bigcirc M$ is "for some constraint $c$, formula $M$ holds under $c$". Clearly, different notions of constraint will have different properties, and thus will give rise to different axioms for $\bigcirc$. The generic interpretation leads to the three axioms $\bigcirc R$, $\bigcirc M$, and $\bigcirc S$. Axiom $\bigcirc R$ says "if $M$ holds outright then it holds under a (trivial) constraint"; $\bigcirc M$ says "if under some constraint, $M$ holds under another constraint, then $M$ holds under an appropriately combined constraint"; finally, $\bigcirc S$ says "if $M$ holds under a constraint, and $N$ holds under a constraint, then the conjunction $M \wedge N$ holds under an appropriately combined constraint". This explains our use of the term *Propositional Lax Logic*, henceforth referred to as PLL, for the logic of $\bigcirc$.

(6) As a concrete instance of the constraint reading for $\bigcirc$ mentioned above (5), $\bigcirc$ can be applied to the timing analysis of combinational circuits. One can establish a direct correspondence between the axioms used in verifying the functional behaviour of a combinational circuit and the computation of data-dependent timing constraints: $\bigcirc R$ corresponds to a wire, which involves zero delay 0; $\bigcirc M$ deals with the sequential composition of circuits, which involves the addition $+$ of delays, and $\bigcirc S$ effects the parallel composition of circuits, which amounts to the maximum operation *max* on delays. In other words, by systematic translation of proofs in PLL into a term over the delay algebra $(\mathbf{Nat}, 0, +, \mathit{max})$, we can extract verification-driven, and thus data-dependent, timing information. This is essentially an interpretation, in the sense of (4), in a concrete $\lambda_c$ calculus. This idea has been worked out in [Mendler, 1996] for a fragment of the logic generated from atomic sentences and the derived implication $M \textit{ leads to } N \;\; =_{\mathit{df}} \;\; M \supset \bigcirc N$. Though the delay algebra $(\mathbf{Nat}, 0, +, \mathit{max})$ may appear rather simple, it is sufficient for a large class of practical timing analyses for discrete dynamic systems [Baccelli et al., 1992].

The previous remarks indicate that however strange $\bigcirc$ may appear as a modality of logic it is a rather natural object well-known from other mathematical contexts. But while its algebraic and type-theoretic ramifications have been investigated its logical aspects seem to be largely unexplored.

This work stresses the logical view of $\bigcirc$ and introduces a novel and rather natural Kripke semantics for $\bigcirc$. The models, called *constraint models*, have two frame relations; one serves to realize the intuitionistic nature of the logic while the other is used to interpret the modality. Based on these models we give a full and faithful embedding of PLL into a classical bimodal theory of type (S4, S4) extending the well-known Gödel translation of intuitionistic logic into S4. This provides a classical explanation of $\bigcirc$ in terms of ordinary modalities.
We will use these constraint models towards a model-theoretic study of our reading of $\bigcirc$ as "under some constraint", which has been introduced previously only in a proof-theoretic sense. In this way we hope to convince the reader of an independent motivation of $\bigcirc$ from hardware verification. We will give two interesting subclasses of constraint models obtaining two concrete constraint interpretations of $\bigcirc$. These concrete models, which are related to (intermediate) intuitionistic logics introduced by Maksimova and Medvedev, verify that PLL has nontrivial expressiveness and illustrate the value of dropping Excluded Middle and $\neg\bigcirc$*false* in concrete cases. We use the structure of the first model to establish the decidability of the stable form of Maksimova's logic and suggest applications of both models in hardware verification.

## 2 Propositional Lax Logic

The formulas of PLL are generated by the grammar

$$M \quad ::= \quad A \mid M \wedge M \mid M \vee M \mid M \supset M \mid \neg M \mid \bigcirc M$$

where $A$ ranges over a countably infinite set of propositional constants pcs $= \{p_0, p_1, \ldots\}$. We will take $\equiv$ to abbreviate bi-implication and use the derived constants *true* and *false*. It is sometimes convenient to consider *false* as primitive and $\neg M$ as an abbreviation for $M \supset$ *false*.
PLL is presented both as a Hilbert and as a Gentzen style calculus. The Hilbert system of PLL takes as axiom schemata all theorems of (or a complete set of axioms for) IPC, plus the modal axiom schemata $\bigcirc R$, $\bigcirc M$, $\bigcirc S$. The inference rules are Modus Ponens and the rule "from $M \supset N$ infer $\bigcirc M \supset \bigcirc N$". The finitary deduction relation induced by these axioms and rules is denoted by $\vdash_{\mathrm{PLL}}$. It is also possible to define PLL as a purely axiomatic extension of IPC.

**Lemma 2.1** *$\Gamma \vdash_{\mathrm{PLL}} M$ iff $M$ can be derived in* IPC *from $\Gamma$ and the single axiom schema $(N \supset \bigcirc K) \equiv (\bigcirc N \supset \bigcirc K)$.*

**Proof:** Let $\vdash^{+}$ be the derivation relation obtained from IPC by adding the scheme $(N \supset \bigcirc K) \equiv (\bigcirc N \supset \bigcirc K)$. One shows that all instances of the three axioms $\bigcirc R$, $\bigcirc M$, $\bigcirc S$ can be derived in $\vdash^{+}$, and further that the rule "from $M \supset N$ infer $\bigcirc M \supset \bigcirc N$" is derivable in the strong form, namely, we have $\vdash^{+} (M \supset N) \supset (\bigcirc M \supset \bigcirc N)$. In the other direction it suffices to show that all instances of $(N \supset \bigcirc K) \equiv (\bigcirc N \supset \bigcirc K)$ can be derived in $\vdash_{\mathrm{PLL}}$. Here $\vdash_{\mathrm{PLL}} (\bigcirc N \supset \bigcirc K) \supset (N \supset \bigcirc K)$ is a consequence of $\bigcirc R$, while for $\vdash_{\mathrm{PLL}} (N \supset \bigcirc K) \supset (\bigcirc N \supset \bigcirc K)$ one invokes all three axioms $\bigcirc R, \bigcirc M$, and $\bigcirc S$. Throughout the proof one makes use of the fact that all IPC theorems, in particular all substitution instances containing $\bigcirc$, are available. ∎

**Proposition 2.2 (Deduction Theorem)** *$\Gamma, M \vdash_{\mathrm{PLL}} N$ implies $\Gamma \vdash_{\mathrm{PLL}} M \supset N$.*

**Proof:** The statement follows immediately from the deduction theorem for IPC (see *e.g.* [Dummett, 1977]) and the fact that PLL is an axiomatic extension of IPC. ∎

The deduction theorem does not hold for the standard Hilbert presentation of ordinary modal logics. For instance in K, T, S4 [Chellas, 1980] we have $M \vdash \Box M$ but $\not\vdash M \supset \Box M$, and $M \supset N \vdash \Diamond M \supset \Diamond N$ but $\not\vdash (M \supset N) \supset (\Diamond M \supset \Diamond N)$.
The Gentzen-style calculus for PLL is presented in terms of ordinary *sequents* $\Gamma \vdash \Delta$, where $\Gamma$ is a finite, possibly empty, list of *hypotheses* and $\Delta$ a finite list of *assertions* with length 0 or 1. The complete set of our sequent rules is listed in figure 1. The inference rules for deriving sequents are the standard ones for IPC plus two special rules $\bigcirc R$ and $\bigcirc L$ which capture the properties of $\bigcirc$ :

$$\frac{\Gamma \vdash M}{\Gamma \vdash \bigcirc M}\,\bigcirc R \qquad\qquad \frac{\Gamma, M \vdash \bigcirc N}{\Gamma, \bigcirc M \vdash \bigcirc N}\,\bigcirc L.$$

These rules are the ones suggested by [Curry, 1957], and may be seen as a sequent-style version of the natural deduction system for $\bigcirc$ used in [Mendler, 1993]. The rules have independently been considered by [Benton et al., 1993]. There are other alternative formalizations of PLL, *e.g.* a tableau calculus has been investigated in [Avellone and Ferrari, 1996].

**Theorem 2.3** *The Hilbert and Gentzen systems for* PLL *are equivalent, i.e. for all formulas $M$, $\vdash_{\mathrm{PLL}} M$ iff $\vdash M$ is derivable.*

**Proof:** One proves a stronger theorem, showing that when $\Gamma$ is finite and $\Delta$ contains at most one formula, the sequent $\Gamma \vdash \Delta$ is derivable iff $\Gamma \vdash_{\mathrm{PLL}} \bigvee \Delta$, where $\bigvee \Delta = M$ if $\Delta = \{M\}$, and $\bigvee \emptyset = \mathit{false}$. Both directions can be established by induction on derivations. ∎

**Theorem 2.4 (Strong Conservativity)** *Let $M$ be a theorem of* PLL*. Then the formula $M'$, where $M'$ is obtained from $M$ by removing all occurrences of $\bigcirc$, is a theorem of* IPC*.*

**Proof:** By induction on the structure of derivations one shows that if $\Gamma \vdash M$ then $\Gamma' \vdash M'$. ∎

Another way of turning theorems of PLL into theorems of IPC is obtained by replacing all sub-formulas prefixed by $\bigcirc$ by *true*. Both results are special instances of the more general

**Logical Rules**

$$\frac{\Gamma \vdash M \qquad \Gamma \vdash N}{\Gamma \vdash M \wedge N}\,\wedge R \qquad\qquad \frac{\Gamma, M, N \vdash \Delta}{\Gamma, M \wedge N \vdash \Delta}\,\wedge L$$

$$\frac{\Gamma, M \vdash \Delta \qquad \Gamma, N \vdash \Delta}{\Gamma, M \vee N \vdash \Delta}\,\vee L$$

$$\frac{\Gamma \vdash M}{\Gamma \vdash M \vee N}\,\vee R_1 \qquad\qquad \frac{\Gamma \vdash N}{\Gamma \vdash M \vee N}\,\vee R_2$$

$$\frac{\Gamma, M \vdash N}{\Gamma \vdash M \supset N}\,\supset\! R \qquad\qquad \frac{\Gamma \vdash M \qquad \Gamma, N \vdash \Delta}{\Gamma, M \supset N \vdash \Delta}\,\supset\! L$$

$$\frac{\Gamma, M \vdash}{\Gamma \vdash \neg M}\,\neg R \qquad\qquad \frac{\Gamma \vdash M}{\Gamma, \neg M \vdash}\,\neg L$$

$$\frac{\Gamma \vdash M}{\Gamma \vdash \bigcirc M}\,\bigcirc R \qquad\qquad \frac{\Gamma, M \vdash \bigcirc N}{\Gamma, \bigcirc M \vdash \bigcirc N}\,\bigcirc L$$

**Structural Rules**

$$\frac{}{M \;\vdash\; M}\,id \qquad\qquad \frac{\Gamma \vdash M \qquad \Gamma, M \vdash \Delta}{\Gamma \vdash \Delta}\,cut$$

$$\frac{\Gamma \vdash \Delta}{\Gamma, M \vdash \Delta}\,weakL \qquad\qquad \frac{\Gamma \vdash}{\Gamma \vdash M}\,weakR$$

$$\frac{\Gamma, M, M \vdash \Delta}{\Gamma, M \vdash \Delta}\,contr \qquad\qquad \frac{\Gamma, M, N, \Gamma' \vdash \Delta}{\Gamma, N, M, \Gamma' \vdash \Delta}\,exch$$

Figure 1: Gentzen Rules for PLL.

result that the translation $\bigcirc M \equiv C \supset M$ preserves provability; for the first take $C \equiv \mathit{true}$ and for the second take $C \equiv \mathit{false}$. From the latter translation we may conclude, for instance, that $\neg \bigcirc \mathit{false}$ and (from the general translation) that $\bigcirc(M \vee N) \supset (\bigcirc M \vee \bigcirc N)$ are not theorems of PLL. This ensures that PLL is nontrivial extension of IPC, in the sense that it is not possible to transform a theorem of IPC into a theorem of PLL by arbitrarily introducing $\bigcirc$s.

**Theorem 2.5 (Strong Extensionality)** PLL *is strongly extensional, i.e. the scheme* $(M \equiv N) \supset (\mathcal{C}[M] \equiv \mathcal{C}[N])$ *is admissible, where* $\mathcal{C}[\_]$ *is an arbitrary syntactic context and* $M, N$ *arbitrary formulas.*

**Proof:** The proof is by induction on the structure of $\mathcal{C}[\_]$. The interesting case, of course, is when $\mathcal{C}[\_] = \bigcirc[\_]$. But $\vdash (M \equiv N) \supset (\bigcirc M \equiv \bigcirc N)$ may be easily derived using rules

$\bigcirc L$ and $\bigcirc R$ (of the Gentzen calculus). ∎

**Theorem 2.6 (Cut Elimination)** *If $\vdash \Delta$ is derivable, then it is derivable without the cut rule.*

**Proof:** The proof uses the same method that works for IPC [Dummett, 1977]. One new reduction step needs to be introduced, as shown in figure 2. Cut elimination has independently been proven by [Benton et al., 1993]. ∎

$$\dfrac{\dfrac{\overset{\Pi_1}{\Gamma \vdash M}}{\Gamma \vdash \bigcirc M}\,\bigcirc R \qquad \dfrac{\overset{\Pi_2}{\Gamma, M \vdash \bigcirc N}}{\Gamma, \bigcirc M \vdash \bigcirc N}\,\bigcirc L}{\Gamma \vdash \bigcirc N}\,\mathit{cut}$$

$$\overset{\mathit{reduce}}{\Longrightarrow} \qquad \dfrac{\overset{\Pi_1}{\Gamma \vdash M} \qquad \overset{\Pi_2}{\Gamma, M \vdash \bigcirc N}}{\Gamma \vdash \bigcirc N.}\,\mathit{cut}$$

Figure 2: Additional Primitive Cut Reduction Step

Direct consequences of cut-elimination are the disjunction and the sub-formula property, and the admissibility of the rule "from $\bigcirc M$ infer $M$", which is the inverse of the necessitation rule of standard modal logics.

**Lemma 2.7**

**(i)** $\vdash_{\mathrm{PLL}} M \vee N$ *implies* $\vdash_{\mathrm{PLL}} M$ *or* $\vdash_{\mathrm{PLL}} N$

**(ii)** $\vdash_{\mathrm{PLL}} \bigcirc M$ *implies* $\vdash_{\mathrm{PLL}} M$

**(iii)** *If $\Gamma \vdash \Delta$ is derivable, then there exists a derivation which involves only sub-formulas of $\Gamma$ and $\Delta$.*

From the sub-formula property (iii) we get the decidability of PLL. This theorem is proven in [Goldblatt, 1981] by semantic methods.

**Theorem 2.8 (Decidability)** PLL *is decidable.*

We have seen that PLL combines a number of properties (in particular deduction theorem and the interpretation $\bigcirc M = \mathit{true}$) which are rather strong for a modal logic. Although from a formal point of view every unary syntactic operator may be called a 'modality' one wonders whether the proof-theoretic properties of $\bigcirc$ are not in fact too strong for it to be an interesting modality in a semantic sense. It turns out that $\bigcirc$ indeed can be given a proper and nontrivial semantics in terms of Kripke models. One necessary condition on a satisfactory notion of Kripke model, of course, is that is should explain the modality $\bigcirc$ in terms of a corresponding semantic accessibility relation. In the following section we present one such type of model.

## 3 Constraint Models for PLL

Kripke-style analyzes have been given for other intuitionistic modal logics, for instance by Simpson [Simpson, 1994] and Plotkin and Stirling [Plotkin and Stirling, 1986] for system IK, by Fischer-Servi [Fischer-Servi, 1980] for the class of $(*)$-IC systems, and by Ewald [Ewald, 1986] for an intuitionistic tense logic. The approach taken here most closely follows [Plotkin and Stirling, 1986] in using one set of worlds but two separate frame relations to interpret $\bigcirc$ and $\supset$. This satisfies our requirement that $\bigcirc$ be given a Kripke-style interpretation. As a result of our approach we obtain a full and faithful embedding of PLL into a classical bimodal (S4, S4) logic. This gives a classical account of PLL which extends the well-known Gödel embedding of IPC, and is different from the embedding of intuitionistic modal logics suggested by Fischer-Servi [Fischer-Servi, 1980]. A quite different kind of semantics was given by Goldblatt [Goldblatt, 1981], in which only the intuitionistic part $\supset$ is represented by a frame relation, while the modality is realized by some extra topological information on the intuitionistic frame.

**Definition 3.1 (Kripke Constraint Model)** *A (Kripke)* constraint model *for* PLL *is a quintuple $\mathcal{C} = (W, R_m, R_i, V, F)$, where $W$ is a non-empty set, $R_m, R_i$ are binary relations on $W$, $F \subseteq W$, and $V$ is a map that assigns to every propositional constant $A$ of* PLL *a subset $V(A) \subseteq W$. These data are subject to the following conditions:*

- *$R_m, R_i$ are preorders, i.e. reflexive and transitive relations, and $R_m \subseteq R_i$,*
- *$F$ and $V$ are hereditary w.r.t. $R_i$, i.e. if $w \; R_i \; v$, then $w \in F$ implies $v \in F$, and $w \in V(A)$ implies $v \in V(A)$,*
- *$V$ is full on $F$, i.e. $F \subseteq V(A)$.*

If $w \; R_m \; v$ then we say that $v$ is a *constraining* of $w$, or $v$ is reachable from $w$ under a *constraint.* Elements of $F$ are *fallible* worlds and if $w \; R_m \; v$ and $v \in F$, then intuitively the constraint leading to $v$ is inconsistent with world $w$. Models with fallible worlds are not a new concept. They have been introduced previously to admit intuitionistic metatheory for intuitionistic logic, see *e.g.* [Troelstra and van Dalen, 1988, Dummett, 1977]. As we will show later on, in our context, fallible worlds arise naturally from the constraint interpretation.

**Definition 3.2 (Validity)** *Let $\mathcal{C} = (W, R_m, R_i, V, F)$ be a constraint model for* PLL. *Given a formula $M$ and $w \in W$, $M$ is* valid *at $w$ in $\mathcal{C}$, written $\mathcal{C}, w \models M$ iff*

- *$M$ is a propositional constant $A$ and $w \in V(A)$;*
- *$M$ is $N \wedge K$ and both $\mathcal{C}, w \models N$ and $\mathcal{C}, w \models K$;*
- *$M$ is $N \vee K$ and $\mathcal{C}, w \models N$ or $\mathcal{C}, w \models K$;*
- *$M$ is true; or $M$ is false and $w \in F$;*

- *$M$ is $N \supset K$ and for all $v \in W$ such that $w\ R_i\ v$, $\mathcal{C}, v \models N$ implies $\mathcal{C}, v \models K$;*
- *$M$ is of form $\bigcirc N$ and for all $v \in W$, $w\ R_i\ v$, there exists $u \in W$ with $v\ R_m\ u$ such that $\mathcal{C}, u \models N$.*

*A formula $M$ is* valid in $\mathcal{C}$*, written $\mathcal{C} \models M$, if for all $w \in W$, $M$ is valid at $w$ in $\mathcal{C}$; $M$ is* valid*, written $\models M$, if $M$ is valid in any constraint model $\mathcal{C}$.*

Disregarding the fallible worlds, for modal-free formulas validity is defined exactly as for intuitionistic logic on the underlying frame $(W, R_i, V)$. Validity behaves as in ordinary intuitionistic logic, *viz.* it is hereditary with respect to the accessibility relations. Formally, if $w \models M$ and $w\ R_i\ v$, then $v \models M$. This is due to the transitivity of $R_i$. Since $R_m$ is a subrelation of $R_i$, validity is hereditary with respect to $R_m$ too. Worlds $w, v$ with $w\ R_i\ v$ and $v\ R_i\ w$ validate the same formulas and can thus be identified. Hence, it is no restriction to assume that the relation $R_i$ is a partial order, *i.e.* antisymmetric. Note that $\bigcirc$ is hereditary w.r.t. the intuitionistic frame $R_i$ without further imposing a confluence frame condition as in the models for IK [Plotkin and Stirling, 1986].

Some remarks concerning our definition of validity are in order. Observe that the clause for validity of $\bigcirc N$ is a $\forall\exists$ statement. This endows $\bigcirc$ with properties of both possibility and of necessity. Secondly, one notes that fallible worlds validate all formulas and that $\neg \bigcirc \mathit{false}$ is not valid in general. Also, our semantics of $\bigcirc$ does not validate the scheme $\bigcirc(M \vee N) \supset \bigcirc M \vee \bigcirc N$, a fact that is important if the semantics is to capture the proof-theoretic properties of PLL. Both this scheme and $\neg \bigcirc \mathit{false}$ are generally adopted for modality $\Diamond$, even for intuitionistic logics such as IK and apparently also by the class $(*)$-IC of logics considered by Fischer-Servi in [Fischer-Servi, 1980]. We will present concrete constraint models falsifying as well as validating these axioms. Finally notice that there is no point in defining a 'necessity' modality, in contrast to IK. Its definition

$$w \models \Box M \quad \text{iff} \quad \forall v, u.\ w\ R_i\ v\ \ \&\ \ v\ R_m\ u \Rightarrow u \models M$$

yields nothing new because of the frame condition $R_m \subseteq R_i$.

**Theorem 3.3 (Soundness)** *If $\vdash_{\mathrm{PLL}} M$ then $\models M$.*

**Proof:** We lift the notion of validity to sequents in the following way: A sequent $\Gamma \vdash K$ is *valid in* model $\mathcal{C}$ if for all $w$, whenever all hypotheses $M \in \Gamma$ are valid at $w$ in $\mathcal{C}$, then the assertion $K$ is valid at $w$ in $\mathcal{C}$; a sequent $\Gamma \vdash$ is valid in $\mathcal{C}$ if the only worlds at which all hypotheses $M \in \Gamma$ are valid in $\mathcal{C}$ are fallible worlds.

One then shows by induction on derivations that if $\Gamma \vdash \Delta$ is derivable then $\Gamma \vdash \Delta$ is valid in all models. The hereditariness of validity, and thus transitivity of $R_i$ and inclusion $R_m \subseteq R_i$, is used for the rules $\supset R$, $\neg R$, $\bigcirc R$, and $\bigcirc L$. The reflexivity of $R_i$ is used to show soundness of $\supset L$, $\neg L$, $\bigcirc L$. Finally, the reflexivity of $R_m$ is exploited for $\bigcirc R$, and transitivity of $R_m$ for $\bigcirc L$. ∎

Another type of models for PLL are the $\mathcal{J}$-frames and $\mathcal{J}$-spaces of Goldblatt [Goldblatt, 1981]. Just as in our work, these models are built on an intuitionistic frame

$(W, R_i)$. However, they do not have fallible worlds $F$ and in place of our modal frame relation $R_m$ some topological structure on $(W, R_i)$ is used. We will now give a rather natural semantics-preserving translation of constraint models into $\mathcal{J}$-spaces, that preserves the underlying intuitionistic frame. The other direction and the connection with $\mathcal{J}$-frames, which are not considered here, are left as open problems.
We first recall the definitions given in [Goldblatt, 1981]. An *intuitionistic Kripke model* (IKM) is a triple $(W, R_i, V)$ where $W$ is a nonempty set, $R_i$ a partial ordering on $W$ and $V$ a valuation, *i.e.* an assignment of hereditary subsets of $W$ to propositional constants.

**Definition 3.4** *An* $\mathcal{J}$-space *is given by an IKM* $\mathcal{S} = (W, R_i, V)$ *together with a map* $\gamma$ *that assigns to every* $w \in W$ *a collection* $\gamma(w) \subseteq 2^W$ *of* $R_i$*-hereditary subsets of* $W$*, with the following properties:*

**(N1)** $w \; R_i \; v$ *implies* $\gamma(w) \subseteq \gamma(v)$

**(N2)** $R \in \gamma(w)$ *and* $S \in \gamma(w)$ *implies* $R \cap S \in \gamma(w)$

**(N3)** $R \in \gamma(w)$ *and* $S$ *a* $R_i$*-hereditary subset of* $W$ *such that* $R \subseteq S$ *imply* $S \in \gamma(w)$

**(N4)** $[w) = \{\, v \mid w \; R_i \; v \,\} \in \gamma(w)$

**(N5)** *For any* $R_i$*-hereditary subset* $S \subseteq W$*, if* $\{\, v \mid S \in \gamma(v) \,\} \in \gamma(w)$*, then* $S \in \gamma(w)$

Strictly, in [Goldblatt, 1981] the term *$\mathcal{J}$-spaces* is applied only to the underlying structure $(W, R_i, \gamma)$ not including the valuation $V$. For modal-free formulas validity on $\mathcal{J}$-spaces, denoted by $\models_s$, is defined just like that for intuitionistic logic, on the underlying IKM. Validity for formulas $\bigcirc M$ is given by the clause

$$w \models_s \bigcirc M \quad \text{iff} \quad \exists S \in \gamma(w).\, \forall v \in S.\, v \models_s N.$$

**Remark:** Condition (N1) is to ensure hereditariness of validity. (N2) deals with the axiom $\bigcirc M \wedge \bigcirc N \supset \bigcirc(M \wedge N)$, (N3) with the rule that $\vdash M \supset N$ entails $\vdash \bigcirc M \supset \bigcirc N$, (N4) is for the axiom $M \supset \bigcirc M$, and finally (N5) ensures validity of $\bigcirc\bigcirc M \supset \bigcirc M$.

**Theorem 3.5** *Let* $\mathcal{C} = (W, R_i, R_m, F, V)$ *be a non-trivial constraint model (i.e, one where* $W \neq F$*) and let* $(W^0, {R_i}^0, V^0)$ *be the underlying non-fallible IKM obtained from* $(W, R_i, V)$ *by restriction to the set* $W \setminus F$*. Then, there exists* $\gamma$ *such that* $\mathcal{S} = (W^0, {R_i}^0, \gamma, V^0)$ *is a* $\mathcal{J}$*-space such that for all* $M$*,*

$$\mathcal{C} \models M \quad \textit{iff} \quad \mathcal{S} \models_s M.$$

**Proof:** A subset $S \subseteq W$ is called *$R_m$-cofinal* for $w \in W$ iff $S$ is $R_i$-hereditary and for all $u \in W$ such that $w \; R_i \; u$, there exists a $v \in S$ with $u \; R_m \; v$. In other words, $S$ is $R_m$-cofinal for $w$ if from every $R_i$-reachable successor of $w$ the set $S$ is $R_m$-reachable. For all $w \in W^0$ we take $\gamma(w)$ to be the set of all $R_m$-cofinal sets for $w$, restricted to $W^0$. We leave it to the reader to check the properties (N1)–(N5) and preservation of truth, *i.e.* that for all $w \in W^0$, $\mathcal{C}, w \models M$ iff $\mathcal{S}, w \models_s M$. ∎

## 4 Completeness

In this section we prove completeness of PLL with respect to Kripke constraint models. If we had a method of translating Goldblatt's $\mathcal{J}$-spaces into equivalent constraint models, then completeness for constraint models would follow immediately from the following theorem.

**Theorem 4.1 (Goldblatt)** $\vdash_{\text{PLL}} M$ *iff* $M$ *is valid on all* $\mathcal{J}$*-spaces.*

Rather than searching for such a translation of models we give a separate completeness proof. We will follow the standard idea of constructing a counter model for every formula that is not derivable. The counter model employs a suitable generalization of the Lindenbaum construction, in which worlds are triples

$$(\Gamma, \Delta, \Theta)$$

of sets of formulas, called *theories*, subject to an abstract consistency condition which reflects the semantic rôle of its components (*cf.* [Fitting, 1983]).
The model will be set up so that at a world $w = (\Gamma, \Delta, \Theta)$ the formulas in $\Gamma$ are validated at $w$, the formulas in $\Delta$ are falsified at $w$, and the formulas in $\Theta$ are falsified at every world $R_m$-reachable from $w$. The sets $\Theta$ are a special feature of our completeness proof and of PLL. They are introduced to make up for the fact that falsity of a formula $\bigcirc M$ cannot be expressed by including $M$ (or a sub-formula of $M$) in $\Gamma$ or $\Delta$. We need to keep track of these separately.
Another special feature of the proof is the notion of consistency. A theory $(\Gamma, \Delta, \Theta)$ is *consistent* if for every choice of formulas $N_1, \dots, N_n \in \Delta$, and $K_1, \dots, K_k \in \Theta$, such that $n + k \geq 1$, it is *not* the case that

$$\Gamma \ \vdash \ N_1 \vee \cdots \vee N_n \ \vee \ \bigcirc(K_1 \vee \cdots \vee K_k)$$

This definition is somewhat weaker than one might expect as it excludes the case $k = n = 0$. The disjunction on the right must always be nonempty, with the effect that the theories $(\Gamma, \emptyset, \emptyset)$, for any choice of $\Gamma$, are consistent for trivial reasons. The point here is that we take the empty disjunction to be the empty formula rather than *false*.
A consistent theory is *maximally consistent* if there is no proper consistent extension, under component-wise subset ordering. For instance, the distinguished theory $(\bot, \emptyset, \emptyset)$, where $\bot$ denotes the set of all formulas, is maximally consistent. Observe that if $(\Gamma, \Delta, \Theta)$ is maximally consistent, then *false* $\in \Gamma$ iff $\Delta = \Theta = \emptyset$.

**Lemma 4.2**

- *Every consistent theory has a maximally consistent extension.*
- *If* $(\Gamma, \Delta, \Theta)$ *is a maximally consistent theory then the following properties hold:*
  - **(i)** $\Gamma$ *is deductively closed*
  - **(ii)** *If* $M \vee N \in \Gamma$ *then* $M \in \Gamma$ *or* $N \in \Gamma$

**(iii)** *If* $M \supset N \in \Gamma$ *then* $M \in \Delta$ *or* $N \in \Gamma$

**(iv)** *If* $M \vee N \in \Delta$ *then* $M \in \Delta$ *and* $N \in \Delta$

**(v)** *If* $M \wedge N \in \Delta$ *then* $M \in \Delta$ *or* $N \in \Delta$

**(vi)** $\Theta \subseteq \Delta$

**(vii)** $M \in \Gamma$ *iff* $M \notin \Delta$

**Proof:** Let $(\Gamma, \Delta, \Theta)$ be a consistent theory. We obtain a maximally consistent extension $(\Gamma^*, \Delta^*, \Theta^*)$ in the usual way by enumerating all formulas

$$B_0, B_1, \ldots, B_n, B_{n+1}, \ldots$$

and by building up a hierarchy of consistent theories

$$(\Gamma_0, \Delta_0, \Theta_0) \subseteq (\Gamma_1, \Delta_1, \Theta_1) \subseteq \cdots \subseteq (\Gamma_n, \Delta_n, \Theta_n) \subseteq (\Gamma_{n+1}, \Delta_{n+1}, \Theta_{n+1}) \subseteq \cdots$$

starting with $(\Gamma_0, \Delta_0, \Theta_0) = (\Gamma, \Delta, \Theta)$ and such that $(\Gamma_{n+1}, \Delta_{n+1}, \Theta_{n+1}) = (\Gamma_n \cup \{B_n\}, \Delta_n, \Theta_n)$ if it is consistent, otherwise $(\Gamma_{n+1}, \Delta_{n+1}, \Theta_{n+1}) = (\Gamma_n, \Delta_n \cup \{B_n\}, \Theta_n \cup \{B_n\})$ if it is consistent, otherwise $(\Gamma_{n+1}, \Delta_{n+1}, \Theta_{n+1}) = (\Gamma_n, \Delta_n \cup \{B_n\}, \Theta_n)$. Then,

$$(\Gamma^*, \Delta^*, \Theta^*) \overset{df}{=} (\bigcup_{n \in \omega} \Gamma_n, \bigcup_{n \in \omega} \Delta_n, \bigcup_{n \in \omega} \Theta_n).$$

$(\Gamma^*, \Delta^*, \Theta^*)$ is a maximally consistent theory. Note, if $\Gamma \vdash \mathit{false}$, then by consistency of $(\Gamma, \Delta, \Theta)$ we must have $\Delta = \Theta = \emptyset$, in which case the above construction will produce the maximally consistent extension $(\bot, \emptyset, \emptyset)$.

The second part of the lemma is not hard to verify. It uses the properties of the sequent calculus for $\vdash$, in particular the following two derived rules

$$\frac{\Gamma \vdash \bigvee X \ \vee\ \bigcirc \bigvee Y}{\Gamma \vdash \bigvee X' \ \vee\ \bigcirc \bigvee Y'}\ X \subseteq X' \text{ and } Y \subseteq Y' \qquad\qquad \frac{\Gamma \vdash M \vee N \qquad \Gamma, M \vdash N}{\Gamma \vdash N}$$

In the first rule $X', Y'$ are finite sets of formulas and $\bigvee\{M_1, \ldots, M_n\}$ abbreviates $M_1 \vee \cdots \vee M_n$. When $Z$ is empty then the corresponding disjunct $\bigvee Z$ in the first rule is dropped. The second rule is derivable from the structural rules (in particular the *cut* rule), $\vee L$, and *id*, whereas the first one also involves $\vee R_1, \vee R_2, \bigcirc R$, and $\bigcirc L$. The application of both these derived rules, as well as the structural rules, will be referred to as "structural reasoning" in the following. The seven claims in the second part of the lemma are now handled as follows:

(i) If $\Gamma \vdash M$ and $M \notin \Gamma$, then by maximality $\Gamma, M \vdash \bigvee \Delta' \vee \bigcirc \bigvee \Theta'$ for some finite subsets $\Delta' \subseteq \Delta$ and $\Theta' \subseteq \Theta$. By structural reasoning this implies $\Gamma \vdash \bigvee \Delta' \vee \bigcirc \bigvee \Theta'$, contradicting the consistency of $(\Gamma, \Delta, \Theta)$. The remaining cases follow a similar pattern.

(ii) If neither $M$ nor $N$ are members of $\Gamma$, then $(\Gamma \cup \{M\}, \Delta, \Theta)$ and $(\Gamma \cup \{N\}, \Delta, \Theta)$ are inconsistent, by maximality. Thus, for some $\Delta_M, \Delta_N \subseteq \Delta$ and $\Theta_M, \Theta_N \subseteq \Theta$, we get associated — let us call them the "maximality" — proofs for $\Gamma, M \vdash \bigvee \Delta_M \;\vee\; \bigcirc \bigvee \Theta_M$ and $\Gamma, N \vdash \bigvee \Delta_N \;\vee\; \bigcirc \bigvee \Theta_N$. Applying structural reasoning and the $\vee L$ rule to the associated maximality proofs, we obtain the inconsistency of $(\Gamma \cup \{M \vee N\}, \Delta, \Theta)$, and hence $M \vee N \notin \Gamma$.

(iii) If $M \notin \Delta$ and $N \notin \Gamma$ we apply structural reasoning and the $\supset L$ rule to the associated maximality proofs to establish the inconsistency of $(\Gamma \cup \{M \supset N\}, \Delta, \Theta)$.

(iv) If $M \notin \Delta$ or $N \notin \Delta$, we may apply structural reasoning and $\vee R_1$ or $\vee R_2$ to the associated maximality proofs to establish the inconsistency of $(\Gamma, \Delta \cup \{M \vee N\}, \Theta)$; we might boil this argument down to the even more compact formulation "by maximality and $\vee R_1$";

(v) follows by maximality and $\wedge R$;

(vi) follows by maximality and the theorem $K \vee \bigcirc L \supset \bigcirc(K \vee L)$;

(vii) follows by maximality.

■

We can now proceed to define a generic Kripke constraint model

$$\mathcal{C}^* = (W^*, R_m^*, R_i^*, V^*, F^*)$$

which falsifies all unprovable formulas. As the elements in $W^*$ we take the maximally consistent theories $\mathcal{T} = (\Gamma, \Delta, \Theta)$. The accessibility relation $R_i^*$ is simply the subset relation on the first component, *i.e.*

$$(\Gamma, \Delta, \Theta)\ R_i^*\ (\Gamma', \Delta', \Theta') \quad \overset{df}{\equiv} \quad \Gamma \subseteq \Gamma'$$

and constraint accessibility $R_m^*$ is the subset relation in the first *and* third component:

$$(\Gamma, \Delta, \Theta)\ R_m^*\ (\Gamma', \Delta', \Theta') \quad \overset{df}{\equiv} \quad \Gamma \subseteq \Gamma' \quad \& \quad \Theta \subseteq \Theta'.$$

Valuation $V^*$ and fallible nodes $F^*$ are defined such that

$$\begin{aligned} V^*(A) \quad &\overset{df}{\equiv} \quad \{\, (\Gamma, \Delta, \Theta) \mid A \in \Gamma \,\} \\ F^* \quad &\overset{df}{\equiv} \quad \{(\bot, \emptyset, \emptyset)\}. \end{aligned}$$

It is not hard to verify that these data indeed constitute a constraint Kripke model. The following properties make $\mathcal{C}^*$ a canonical model for PLL:

**Lemma 4.3** *Let $\mathcal{T} = (\Gamma, \Delta, \Theta)$ be a maximally consistent theory. Then,*

- $M \in \Gamma$ *implies* $\mathcal{T} \models M$

- *$M \in \Delta$ implies $\mathcal{T} \not\models M$*
- *$M \in \Theta$ implies that for all $\mathcal{T}'$ such that $\mathcal{T}\ R_m^*\ \mathcal{T}'$, $\mathcal{T}' \not\models M$.*

**Proof:** The lemma is proven by induction on the formula $M$. Here only the cases $M \equiv \bigcirc N$ and $M \equiv N \supset K$ will be treated, as they are the ones that drive the model along $R_i^*$ and $R_m^*$. All other cases are achieved 'on-the-spot' using lemma 4.2.
It will be convenient to express the consistency condition for theories $(\Gamma, \Delta, \Theta)$ in more concise but less precise form as

$$\Gamma \not\vdash_{\mathrm{PLL}} \bigvee \Delta \ \vee\ \bigcirc \bigvee \Theta,$$

noting that if the right hand side is the empty formula then the statement is trivially true.
• Suppose $\bigcirc N \in \Gamma$ and $\mathcal{T}_1$ is such that $\mathcal{T}\ R_i^*\ \mathcal{T}_1$. Then $\mathcal{T}_1 = (\Gamma_1, \Delta_1, \Theta_1)$ and $\Gamma \subseteq \Gamma_1$. We consider the theory $(\Gamma_1 \cup \{N\}, \emptyset, \Theta_1)$. We claim that this theory is consistent. Assume otherwise, then we must have $\Gamma_1, N \vdash_{\mathrm{PLL}} \bigcirc \bigvee \Theta_1$ and further by the deduction theorem, $\Gamma_1 \vdash_{\mathrm{PLL}} N \supset \bigcirc \bigvee \Theta_1$. Since we can prove

$$(N \supset \bigcirc \bigvee \Theta_1) \supset (\bigcirc N \supset \bigcirc \bigvee \Theta_1)$$

in PLL (by lemma 2.1) we conclude that $\Gamma_1, \bigcirc N \vdash_{\mathrm{PLL}} \bigcirc \bigvee \Theta_1$. But since $\bigcirc N \in \Gamma \subseteq \Gamma_1$ this contradicts the consistency of $\mathcal{T}_1$. By lemma 4.2 we can now find a maximally consistent extension $\mathcal{T}' = (\Gamma', \Delta', \Theta')$ of $(\Gamma_1 \cup \{N\}, \emptyset, \Theta_1)$. By definition, $\mathcal{T}_1\ R_m^*\ \mathcal{T}'$, and by the induction hypothesis on $N$, $\mathcal{T}' \models N$. Thus we have $\mathcal{T} \models \bigcirc N$.
• Suppose $\bigcirc N \in \Delta$. Consider the theory $(\Gamma, \emptyset, \{N\})$, which must be consistent for otherwise $\Gamma \vdash_{\mathrm{PLL}} \bigcirc N$, which contradicts consistency of $\mathcal{T}$. Now take a maximally consistent extension $\mathcal{T}' = (\Gamma', \Delta', \Theta')$ of $(\Gamma, \emptyset, \{N\})$. We claim that for all $\mathcal{T}_1$, $\mathcal{T}'\ R_m^*\ \mathcal{T}_1$, $\mathcal{T}_1 \not\models N$. Let $\mathcal{T}_1 = (\Gamma_1, \Delta_1, \Theta_1)$. By construction of $\mathcal{T}'$ and definition of $R_m^*$, $N \in \Theta' \subseteq \Theta_1$. By induction hypothesis on $N$, $\mathcal{T}_1 \not\models N$. This completes the proof that $\mathcal{T} \not\models \bigcirc N$.
• Suppose $N \supset K \in \Gamma$ and $\mathcal{T}_1 = (\Gamma_1, \Delta_1, \Theta_1)$ such that $\mathcal{T}\ R_i^*\ \mathcal{T}_1$. By definition of $R_i^*$, $N \supset K \in \Gamma \subseteq \Gamma_1$. By lemma 4.2 (iii) we have $N \in \Delta_1$ or $K \in \Gamma_1$. By induction hypothesis we infer that if $\mathcal{T}_1 \models N$ then $\mathcal{T}_1 \models K$. Thus, $\mathcal{T} \models N \supset K$.
• Suppose $N \supset K \in \Delta$. Consider the theory $(\Gamma \cup \{N\}, \{K\}, \emptyset)$. It must be consistent since otherwise $\Gamma, N \vdash_{\mathrm{PLL}} K$, whence by the deduction theorem $\Gamma \vdash_{\mathrm{PLL}} N \supset K$ which contradicts consistency of $\mathcal{T}$. Now take a maximally consistent extension $\mathcal{T}' = (\Gamma', \Delta', \Theta')$ of $(\Gamma \cup \{N\}, \{K\}, \emptyset)$. We have $\mathcal{T}\ R_i^*\ \mathcal{T}'$, $N \in \Gamma'$, and $K \in \Delta'$. By induction hypothesis, $\mathcal{T}' \models N$ and $\mathcal{T}' \not\models K$. But this means $\mathcal{T} \not\models N \supset K$.
• To prove the last statement of the lemma the cases $M \in \Theta$ are all treated in the same way: suppose $M \in \Theta$ and $\mathcal{T}_1 = (\Gamma_1, \Delta_1, \Theta_1)$ such that $\mathcal{T}\ R_m^*\ \mathcal{T}_1$. By definition of $R_m^*$, and the properties of maximally consistent theories, lemma 4.2 (vi), $M \in \Theta \subset \Theta_1 \subset \Delta_1$. Thus, we can appeal to the proofs above to conclude $\mathcal{T}_1 \not\models M$. ∎

**Theorem 4.4 (Completeness)** *If $\models M$ then $\vdash_{\mathrm{PLL}} M$.*

**Proof:** Suppose $\not\vdash_{\mathrm{PLL}} M$. Then $(\emptyset, \{M\}, \emptyset)$ is consistent. By lemma 4.2 there is a maximally consistent extension $\mathcal{T}$, and by lemma 4.3 $\mathcal{T} \not\models M$ in the constraint Kripke model $\mathcal{C}^*$. ∎

Three examples of counter models, one falsifying $\neg \bigcirc \mathit{false}$, one falsifying $\bigcirc(A \vee B) \supset (\bigcirc A \vee \bigcirc B)$ and one falsifying $\models (\bigcirc A \supset \bigcirc B) \supset \bigcirc(A \supset B)$, are shown in figure 3, where the dashed arrows represent $R_i$ and the solid arrows $R_m$.

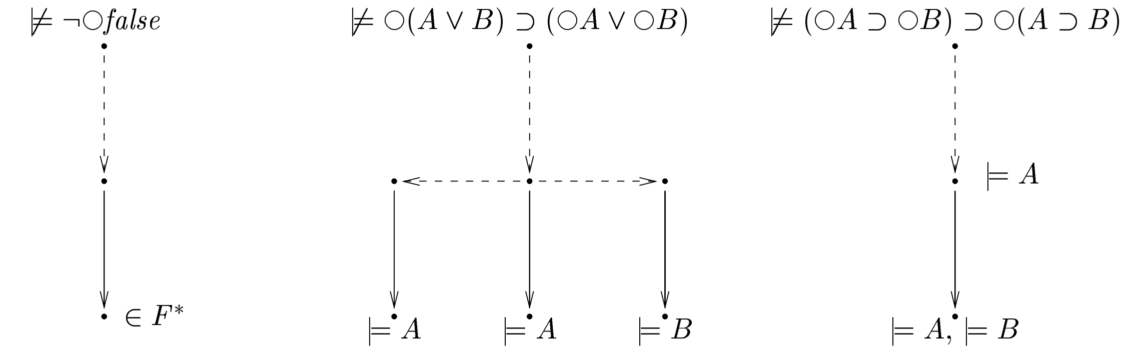
$\not\models \neg\bigcirc \mathit{false}$
$\in F^*$
$\not\models \bigcirc(A \vee B) \supset (\bigcirc A \vee \bigcirc B)$
$\models A$
$\models A$
$\models B$
$\not\models (\bigcirc A \supset \bigcirc B) \supset \bigcirc(A \supset B)$
$\models A$
$\models A, \models B$

Figure 3: Three Counter Models

In section 6 we will discuss special cases of concrete constraint models validating the axiom schemes $\neg \bigcirc \mathit{false}$ and $\bigcirc(M \vee N) \supset (\bigcirc M \vee \bigcirc N)$. It turns out that these classes can be characterized as follows:

**Theorem 4.5**

- PLL $+ \neg \bigcirc \mathit{false}$ *is sound and complete for the class of constraint models with* $F = \emptyset$.
- PLL $+ \bigcirc(M \vee N) \supset (\bigcirc M \vee \bigcirc N)$ *is sound and complete for the class of constraint models where* $R_m$ *and* $R_i$ *are* mutually confluent, *i.e. if* $x\ R_m\ w$ *and* $x\ R_i\ v$*, then there exists* $u$ *such that* $w\ R_i\ u$ *and* $v\ R_m\ u$.

**Proof:** Soundness of $\neg \bigcirc \mathit{false}$ is obvious if $F = \emptyset$. Soundness of the second axiom perhaps is not so obvious. For mutually confluent frame relations one first proves by induction on the structure of $M$ that for all worlds $w$,

$$w \models \bigcirc M \quad \text{iff} \quad \exists u.\, w\ R_m\ u \ \ \&\ \ u \models M.$$

From this soundness of $\bigcirc(M \vee N) \supset (\bigcirc M \vee \bigcirc N)$ then follows directly.
The proof of completeness in both cases is obtained by simple specialization of the completeness proof for PLL (theorem 4.4).
• Suppose $M$ is not derivable in PLL $+ \neg \bigcirc \mathit{false}$. Then the theory $(\{\neg \bigcirc \mathit{false}\}, \{M\}, \emptyset)$ is consistent and thus we can find a maximally consistent theory $\mathcal{T} = (\Gamma, \Delta, \Theta)$ so that $\neg \bigcirc \mathit{false} \in \Gamma$ and $M \in \Delta$. We know that $\mathcal{T} \nvDash M$ in the sub-model of $\mathcal{C}^*$ generated by all theories $\mathcal{T}'$ such that $\mathcal{T}\ R_i^*\ \mathcal{T}'$. Though being a counter model for $M$ it does contain

the fallible theory $(\bot, \emptyset, \emptyset)$ and thus is not of the desired form. However, one can show that by throwing out $(\bot, \emptyset, \emptyset)$ from the (counter) model we do not change validity of any formula. A sufficient condition for this is that $(\bot, \emptyset, \emptyset)$ cannot be accessed by $R_m^*$. In fact, one shows that $\neg \bigcirc \mathit{false} \in \Gamma$ and $(\Gamma, \Delta, \Theta)\ R_m^*\ (\Gamma', \Delta', \Theta')$ implies $\mathit{false} \notin \Gamma'$. For assume otherwise, then $(\Gamma', \Delta', \Theta') = (\bot, \emptyset, \emptyset)$ whence by definition of $R_m^*$ we have $\Theta = \emptyset$. Since $(\Gamma, \Delta, \Theta)$ is maximally consistent this implies that $\Gamma \vdash_{\mathrm{PLL}} \bigvee \Delta\ \vee\ \bigcirc \mathit{false}$ since the proper extension $(\Gamma, \Delta, \{\mathit{false}\})$ cannot be consistent. Now we use the assumption that $\neg \bigcirc \mathit{false} \in \Gamma$ (and the properties of deduction in the logic) to conclude that $\Gamma \vdash_{\mathrm{PLL}} \bigvee \Delta$ which contradicts the consistency of $(\Gamma, \Delta, \Theta)$. Thus, from the assumption that $M$ is not a theorem of $\mathrm{PLL} + \neg \bigcirc \mathit{false}$ we can construct a model without fallible nodes in which $M$ is falsified. This proves the completeness statement for $\mathrm{PLL} + \neg \bigcirc \mathit{false}$.

• Suppose that $M$ is not derivable in $\mathrm{PLL} + \bigcirc(X \vee Y) \supset (\bigcirc X \vee \bigcirc Y)$. Again we consider the canonical counter model generated by a maximally consistent theory $\mathcal{T} = (\Gamma, \Delta, \Theta)$ such that $M \in \Delta$ and such that $\Gamma$ contains all substitution instances of the axiom scheme $\bigcirc(X \vee Y) \supset (\bigcirc X \vee \bigcirc Y)$. We are done if we can show that in the sub-model given by the maximally consistent theories $(\Gamma', \Delta', \Theta')$ with $\Gamma \subseteq \Gamma'$, $R_i^*$ and $R_m^*$ are mutually confluent. The first step is to observe that both $\Delta'$ and $\Theta'$ are uniquely determined by $\Gamma'$ as follows:

$$\Delta' = \complement(\Gamma') \quad \text{and} \quad \Theta' = \delta\Delta',$$

where $\complement(\Gamma')$ is the complement of $\Gamma'$ and $\delta\Delta' = \{ N \mid \bigcirc N \in \Delta' \}$. The first part was proven already in lemma 4.2. The second part is a consequence of the extra axioms in $\Gamma'$ and seen as follows. Let $K \in \delta\Delta'$, *i.e.* $\bigcirc K \in \Delta'$, but $K \notin \Theta'$. Then, since $(\Gamma', \Delta', \Theta')$ is maximally consistent, we get $\Gamma' \vdash_{\mathrm{PLL}} \bigvee \Delta'\ \vee\ \bigcirc(\bigvee \Theta' \vee K)$. Now, by assumption, $\Gamma'$ contains the axiom $\bigcirc(\bigvee \Theta' \vee K) \supset \bigcirc \bigvee \Theta' \vee \bigcirc K$, whence from both facts together we get $\Gamma' \vdash_{\mathrm{PLL}} \bigvee \Delta'\ \vee\ \bigcirc K\ \vee\ \bigcirc \bigvee \Theta'$ which contradicts consistency of $(\Gamma', \Delta', \Theta')$. Thus, $\delta\Delta' \subseteq \Theta'$. The other direction is obtained similarly, using the fact that $(\bigcirc N \vee \bigcirc K) \supset \bigcirc(N \vee K)$ is derivable in PLL.

The second step is to observe that $(\Gamma', \Delta', \Theta')\ R_m^*\ (\Gamma'', \Delta'', \Theta'')$ is equivalent to the condition $\Gamma' \subseteq \Gamma'' \subseteq \delta\Gamma'$. Assume $\Gamma' \subseteq \Gamma'' \subseteq \delta\Gamma'$. Then $\Theta' = \delta\Delta' = \delta(\complement(\Gamma')) = \delta\delta(\complement(\Gamma')) = \delta(\complement(\delta\Gamma')) \subseteq \delta(\complement(\Gamma'')) = \delta\Delta'' = \Theta''$, where the equation $\delta\delta X = \delta X$ holds generally for all deductively closed sets $X$, by virtue of the rule $\bigcirc M$. Thus, $(\Gamma', \Delta', \Theta')\ R_m^*\ (\Gamma'', \Delta'', \Theta'')$. Vice versa, if $(\Gamma', \Delta', \Theta')\ R_m^*\ (\Gamma'', \Delta'', \Theta'')$ we have $\Gamma' \subseteq \Gamma''$ and $\Gamma'' \subseteq \complement(\Theta'') \subseteq \complement(\Theta') = \complement(\delta\Delta') = \delta(\complement(\Delta')) = \delta\Gamma'$.

Now we can prove mutual confluence. Suppose we are given three maximally consistent theories $(\Gamma', \Delta', \Theta')$, $(\Gamma_1, \Delta_1, \Theta_1)$, and $(\Gamma_2, \Delta_2, \Theta_2)$ such that $\Gamma \subseteq \Gamma' \cap \Gamma_1 \cap \Gamma_2$ and such that

$$(\Gamma', \Delta', \Theta')\ R_i^*\ (\Gamma_1, \Delta_1, \Theta_1) \quad \text{and} \quad (\Gamma', \Delta', \Theta')\ R_m^*\ (\Gamma_2, \Delta_2, \Theta_2).$$

We need to find a $\mathcal{T}'$ such that $(\Gamma_1, \Delta_1, \Theta_1)\ R_m^*\ \mathcal{T}'$ and $(\Gamma_2, \Delta_2, \Theta_2)\ R_i^*\ \mathcal{T}'$. We claim that any maximally consistent extension $\mathcal{T}'$ of the theory $(\delta\Gamma_1, \emptyset, \Theta_1)$ will do. For such a $\mathcal{T}'$ to exist $(\delta\Gamma_1, \emptyset, \Theta_1)$ must be consistent. Suppose it is not, then $\delta\Gamma_1 \vdash_{\mathrm{PLL}} \bigcirc \bigvee \Theta_1$ which, by the properties of the logic, implies that $\Gamma_1 \vdash_{\mathrm{PLL}} \bigcirc \bigvee \Theta_1$ contradicting consistency of $(\Gamma_1, \Delta_1, \Theta_1)$. Thus, let $\mathcal{T}' = (\Gamma_3, \Delta_3, \Theta_3)$ be a maximally consistent extension of

$(\delta\Gamma_1, \emptyset, \Theta_1)$. One verifies $\Gamma_1 \subseteq \delta\Gamma_1 \subseteq \Gamma_3$ and $\Theta_1 \subseteq \Theta_3$, hence $(\Gamma_1, \Delta_1, \Theta_1)\ R_m^*\ \mathcal{T}'$ as desired. Further, $\Gamma_2 \subseteq \delta\Gamma'$ by the second observation above and thus $\Gamma_2 \subseteq \delta\Gamma' \subseteq \delta\Gamma_1 \subseteq \Gamma_3$. Thus, $(\Gamma_2, \Delta_2, \Theta_2)\ R_i^*\ \mathcal{T}'$ which completes the proof that the presence of the axioms $\bigcirc(X \vee Y) \supset (\bigcirc X \vee \bigcirc Y)$ forces $R_m^*$ and $R_i^*$ in the canonical model to be mutually confluent. ∎

Our proof of completeness is classical, *i.e.* nonconstructive. It does not yield an effective method of constructing a counter model for unprovable sequents. However, from the work of Avellone and Ferrari [Avellone and Ferrari, 1996], which uses a different, tableau-based presentation of PLL it is clear that a constructive proof of completeness for our constraint models is possible. In fact, PLL has the finite model property for our class of constraint models.

**Theorem 4.6 (Finite Model Property)** $\vdash_{\mathrm{PLL}} M$ *iff* $\mathcal{C} \models M$ *for all finite constraint models* $\mathcal{C}$.

**Proof:** Soundness is obvious. Completeness hinges on the fact that, as in intuitionistic logic, the validity or refutation of a formula $M$ at a given world $w$ of a constraint model only depends on the validity or refutation of all of its proper subformulas at $w$ and at all $v$ that are $R_i$-reachable from $w$. So, at each world only a finite amount of information is relevant for $M$. Using this one can devise a suitable quotient (filtration) of a given counter model for $M$, that preserves the refutation of $M$ but has only a finite number of elements.

Concretely, let $\mathit{Sf}(M)$ be the set of subformulas of $M$ (we consider *false* as a subformula of every formula), and $\mathcal{C} = (W, R_i, R_m, V, F)$ a refutation model for $M$. In our constraint models two kinds of information are relevant of a given world $w$. Firstly, as in the intuitionistic case, we need to preserve the set $T(w)$ of subformulas that are validated at $w$, *i.e.* the set

$$T(w) \quad := \quad \{ N \in \mathit{Sf}(M) \mid w \models N \}.$$

Secondly, we need to preserve the set of subformulas that are refuted on all $R_m$-reachable successors of $w$, *i.e.* the set

$$F_m(w) \quad := \quad \{ N \in \mathit{Sf}(M) \mid \forall v.\ w\ R_m\ v \ \Rightarrow\ v \not\models N \}.$$

This part of the information captures the semantic behaviour of the modality $\bigcirc$. We then define an equivalence relation on $W$ as follows:

$$w \equiv v \quad \text{iff} \quad T(w) = T(v) \quad \& \quad F_m(w) = F_m(v).$$

Since $\mathit{Sf}(M)$ is finite it is clear that there are only a finite number of equivalence classes $[w]_\equiv$. We now define the filtration model

$$\mathcal{C}_\equiv \quad = \quad (W|_\equiv, R_i|_\equiv, R_m|_\equiv, V|_\equiv, F|_\equiv)$$

over the set $W|_\equiv$ of equivalence classes, by stipulating $[w]_\equiv\ R_i|_\equiv\ [v]_\equiv$ iff $T(w) \subseteq T(v)$; $[w]_\equiv\ R_m|_\equiv\ [v]_\equiv$ iff $T(w) \subseteq T(v)$ and $F_m(w) \subseteq F_m(v)$; $[w]_\equiv \in V_\equiv(A)$ iff $A \notin \mathit{Sf}(M)$ or

$w \in V(A)$; $[w]_\equiv \in F|_\equiv$ iff $w \in F$. One verifies that this construction yields a well-defined finite constraint model that validates exactly the same $M$-subformulas as $\mathcal{C}$. Thus, if $\not\vdash_{\mathrm{PLL}} M$ we can apply this filtration to the canonical counter model $\mathcal{C}^*$ constructed in the proof of the completeness theorem 4.4 to get a finite counter model $\mathcal{C}^*|_\equiv$ for $M$. ∎

## 5 Embedding of PLL in Classical Modal Logic

It is well-known that intuitionistic logic can be encoded in the classical modal logic S4, using Gödel's translation [Gödel, 1932]. In fact, the completeness of intuitionistic logic for the standard intuitionistic Kripke semantics can be seen as a corollary of the faithfulness of Gödel's translation. The main result of this section is to show that for the intuitionistic modal logic PLL too a faithful translation into classical modal logic can be obtained from the Kripke semantics presented in the previous section. We shall embed PLL into a classical bimodal theory of type (S4, S4).

Classical bimodal logic has the usual propositional connectives together with two dual pairs of modalities $\Box_i, \Diamond_i, \Box_m, \Diamond_m$. A bimodal *model* is a Kripke structure $\mathcal{M} = (W, R_m, R_i, V)$ where $W$ is a nonempty set, $R_i$, $R_m$ are binary relations on $W$, and $V$ is a map that assigns to every propositional constant $A$ a subset $V(A) \subseteq W$. The notion of validity in bimodal models is as usual and assumed to be understood (see *e.g.* [Popkorn, 1994]).
A bimodal logic of type (S4, S4) has as axioms the standard propositional ones plus the modal schemes

$$\begin{array}{rcl@{\qquad}rcl} T_i & : & \Box_i M \supset M & T_m & : & \Box_m M \supset M \\ 4_i & : & \Box_i M \supset \Box_i \Box_i M & 4_m & : & \Box_m M \supset \Box_m \Box_m M \\ K_i & : & \Box_i (M \supset N) \supset \Box_i M \supset \Box_i N & K_m & : & \Box_m (M \supset N) \supset \Box_m M \supset \Box_m N \end{array}$$

and Modus Ponens together with necessitation

$$\vdash M \;\Rightarrow\; \vdash \Box_i M \qquad\qquad \vdash M \;\Rightarrow\; \vdash \Box_m M$$

as rules of inference. As usual the necessity modalities $\Box_i$, $\Box_m$ are taken as primitive and the possibilities are introduced as their classical duals, *i.e.* $\Diamond_i M = \neg\Box_i\neg M$ and $\Diamond_m M = \neg\Box_m\neg M$. The bimodal theory we are interested in is obtained from bimodal logic of type (S4, S4) by adding the axiom scheme

$$Sub \;:\; \Box_i M \supset \Box_m M.$$

The resulting theory we denote by [S4, S4], where the square brackets are meant to indicate the presence of the axiom *Sub*. A [S4, S4]-*model* is a bimodal model $\mathcal{M} = (W, R_m, R_i, V)$ where $R_i$, $R_m$ are reflexive, transitive, and satisfy $R_m \subseteq R_i$. It is straightforward to show from results in [Popkorn, 1994] that the theory [S4, S4] is sound and (Kripke) complete for the class of [S4, S4]-models.

Let $f$ be a distinguished propositional constant in the following. We translate every formula $M$ of PLL into a bimodal formula $M^g$ as follows:

$$\mathit{false}^g \;=\; \Box_i f$$

$$\begin{aligned} A^g &= \Box_i(A \vee f) \\ (M \wedge N)^g &= M^g \wedge N^g \\ (M \vee N)^g &= M^g \vee N^g \\ (M \supset N)^g &= \Box_i(M^g \supset N^g) \\ (\bigcirc M)^g &= \Box_i \Diamond_m M^g, \end{aligned}$$

where $A$ ranges over propositional constants.

**Theorem 5.1** *Let $M$ be a formula of* PLL *that does not contain the propositional constant $f$. Then, $\vdash_{\mathrm{PLL}} M$ iff* [S4, S4] $\vdash M^g$.

**Proof:** The theorem is a direct consequence of soundness and completeness of the respective logics, and the close relationship between their models. There is a natural way to translate both types of models into each other preserving the validity of formulas. All we need to do is to translate the valuation part, the bimodal structure remains the same.

($\Rightarrow$) Let $\mathcal{M} = (W, R_m, R_i, V)$ be a [S4, S4]-model and $\mathcal{M}_g = (W, R_m, R_i, V_g, F_g)$ the induced Kripke constraint model with $V_g(A) = \{ w \in W \mid \forall v \in W.\ w\ R_i\ v \Rightarrow v \in V(A) \cup V(f) \}$ and $F_g = V_g(f)$. We prove by structural induction that for all formulas $M$ of PLL that do not contain $f$,

$$\mathcal{M}, w \models M^g \quad \Leftrightarrow \quad \mathcal{M}_g, w \models M,$$

where $\models$ on the left is classical validity in [S4, S4]-models, while $\models$ on the right is intuitionistic validity in constraint models. From this it follows that if $M$ is valid in all constraint models then $M^g$ is valid in all [S4, S4]-models. Hence, by completeness of [S4, S4], $\vdash_{\mathrm{PLL}} M$ implies [S4, S4] $\vdash M^g$.

• $\mathcal{M}, w \models \mathit{false}^g$ iff $\mathcal{M}, w \models \Box_i f$ iff $\forall v.\ w\ R_i\ v \Rightarrow \mathcal{M}, v \models f$, iff $w \in V_g(f)$ iff $\mathcal{M}_g, w \models \mathit{false}$.

• $\mathcal{M}, w \models A^g$ iff $\mathcal{M}, w \models \Box_i(A \vee f)$ iff $w \in V_g(A)$ iff $\mathcal{M}_g, w \models A$.

• Conjunction $M \wedge N$ and disjunction $M \vee N$ present no difficulties.

• $\mathcal{M}, w \models (M \supset N)^g$ iff $\mathcal{M}, w \models \Box_i(M^g \supset N^g)$. This is equivalent to the statement that for all $v$ with $w\ R_i\ v$, $\mathcal{M}, v \models M^g$ implies $\mathcal{M}, v \models N^g$. By induction hypothesis this is equivalent to $\mathcal{M}_g, v \models M$ implies $\mathcal{M}_g, v \models N$. Hence, $\mathcal{M}, w \models (M \supset N)^g$ is equivalent to $\mathcal{M}_g, w \models M \supset N$.

• $\mathcal{M}, w \models (\bigcirc M)^g$ iff $\mathcal{M}, w \models \Box_i \Diamond_m M^g$. Using the induction hypothesis for $M$, this is readily seen to be the same as the statement $\mathcal{M}_g, w \models \bigcirc M$.

($\Leftarrow$) Let $\mathcal{C} = (W, R_m, R_i, V, F)$ be a constraint model and $\mathcal{C}^g = (W, R_m, R_i, V^g)$ the induced [S4, S4]-model obtained by putting $V^g(A) = V(A)$ if $A \neq f$ and $V^g(f) = F$. We claim that for all formulas $M$ that do not contain $f$,

$$\mathcal{C}, w \models M \quad \Leftrightarrow \quad \mathcal{C}^g, w \models M^g.$$

From this it follows that if $M^g$ is valid in all [S4, S4]-models then $M$ is valid in all constraint models, which by completeness of PLL means that [S4, S4] $\vdash M^g$ implies $\vdash_{\mathrm{PLL}} M$.

- $\mathcal{C}, w \models \mathit{false}$ iff $w \in F$. By hereditariness of $F$ this is equivalent to $\forall v.\ w\ R_i\ v \Rightarrow v \in F$ which is the same as $\mathcal{C}^g, w \models \mathit{false}^g$ since by definition $V^g(f) = F$ and $\mathit{false}^g = \Box_i f$.

- We only need to consider propositional constants $A$ different from $f$. $\mathcal{C}^g, w \models A^g$ iff $\mathcal{C}^g, w \models \Box_i(A \vee f)$. Since $V^g(A) \cup V^g(f) = V(A) \cup F = V(A)$, this is equivalent to the statement that for all $v$ with $w\ R_i\ v$, $v \in V(A)$, which by hereditariness of $V(A)$ is the same as $\mathcal{C}, w \models A$.

- Again, conjunction $M \wedge N$ and disjunction $M \vee N$ are trivial.

- $\mathcal{C}^g, w \models (M \supset N)^g$ iff $\mathcal{C}^g, w \models \Box_i(M^g \supset N^g)$. Using the induction hypothesis for $M, N$ this is nothing but the semantic condition for $\mathcal{C}, w \models M \supset N$.

- $\mathcal{C}^g, w \models (\bigcirc M)^g$ iff $\mathcal{C}^g, w \models \Box_i \Diamond_m M^g$. Again, with reference to the induction hypothesis, this is equivalent to the semantic condition for $\mathcal{C}, w \models \bigcirc M$. ∎

Theorem 5.1 gives a classical account of PLL by a simple bimodal variant of the Gödel translation. This is an interesting result which falls out directly from the special structure of our constraint models, *viz.* their essential bimodal nature.
Note how falsity (and hence negation) of PLL is captured in the translated classical formula with the help of a distinguished propositional constant $f$. This trick is borrowed from Johansson who used it to embed intuitionistic logic into minimal logic [Johansson, 1936]. The naive translation $\mathit{false}^g = \mathit{false}$ would not be faithful, since then $(\neg\bigcirc \mathit{false})^g = \Box_i \neg \Box_i \Diamond_m \mathit{false}$, which is a theorem of [S4, S4] while $\neg\bigcirc\mathit{false}$ is not a theorem of PLL. Observe also that the requirement that $f$ not appear in $M$ is crucial: For instance, $f \supset A$ is not valid in PLL but $(f \supset A)^g = \Box_i(\Box_i f \supset \Box_i(A \vee f))$ is valid in [S4, S4].

# 6 Some Abstract Constraint Models

We give two variants of concrete models for PLL. The first class of models, discussed in this section, is characterized by formulas of the kind $\bigcirc M \equiv \mathcal{C}[M]$ where $\mathcal{C}[\_]$ is one of a family of possible *contexts*, for example $\mathcal{C}_1[M] \equiv C \supset M$ where $C$ is a fixed proposition. As mentioned this is precisely Curry's system LJZ [Curry, 1952] and a special case of the quite general constraint interpretation according to which $\bigcirc M$ means $\gamma \supset M$, where $\gamma$ is taken from a predefined set of distinguished propositions representing constraints. Other possible contexts are $\mathcal{C}_2[M] \equiv C \vee M$ or $\mathcal{C}_3[M] \equiv (M \supset C) \supset C$. These three contexts $\mathcal{C}_i[\_]$ are closely related to the modal operators $v$, $u$, and $w$ considered by Simmons [Simmons, 1978] and Macnab [Macnab, 1981], which have a distinguished status in the algebraic theory. Here we give a constraint interpretation and characterization in terms of constraint models, albeit in case of $\mathcal{C}_3[\_]$ only for $C = \mathit{false}$.

Let PLL$^C$ be the (syntactic) theory

$$\mathrm{PLL}\ +\ \bigcirc M \equiv (C \supset M),$$

where $C$ is an arbitrary but fixed proposition, and $\mathbf{M}^C$ the class of (antisymmetric) Kripke constraint models validating PLL$^C$. We might call these the *Curry* models for constraint $C$. The PLL$^C$ interpretation of $\bigcirc$ provides us with a class of models for which the axiom schemata $\neg \bigcirc \mathit{false}$ and $\bigcirc(M \vee N) \supset (\bigcirc M \vee \bigcirc N)$ are unsound, in general. The former is valid iff $\models \neg\neg C$.

**Proposition 6.1** *$\forall w.\ \exists u.\ w\ R_m\ u\ \ \&\ \ u \models C$, and (ii) $\forall w, u.\ (w \models C\ \ \&\ \ w\ R_m\ u) \ \Rightarrow\ w = u$.*

Strictly speaking, the two conditions are not pure 'frame' conditions as they involve the validity of $C$ and thus the valuation. By 'characterized' we mean that the class of models satisfying the given conditions is the largest class of models for PLL$^C$ closed under any change of valuation that does not modify the validity of $C$.

**Proof:** The first condition says that from every world $w$ there is a $C$-validating world reachable via $R_m$. This is necessary and sufficient to ensure validity of $(C \supset M) \supset \bigcirc M$ (for necessity put $M = C$). The second condition says that if $w$ already validates $C$ then $w$ is a terminal with respect to $R_m$. This is necessary and sufficient to ensure the other direction $\bigcirc M \supset (C \supset M)$ (for necessity put $M = A$ where $A$ is a propositional constant not occurring in $C$). ∎

With the semantic characterization at hand we can now try to construct concrete models for PLL$^C$. Let $\mathcal{M} = (W, R_i, V)$ be an arbitrary intuitionistic Kripke model for IPC. We obtain a suitable constraint Kripke model $\mathcal{M}^C = (W^C, R_i^C, R_m^C, V^C, F^C)$ by the following definitions:

- $W^C = W \cup \{\bot\}$ where $\bot$ is a new element not already in $W$,
- $V^C(A) = V(A) \cup \{\bot\}$,
- $F^C = \{\bot\}$,
- $w\ R_i^C\ v$ iff $w\ R_i\ v$ or $v = \bot$,
- $w\ R_m^C\ v$ iff $\mathcal{M}, w \not\models C$ and $v = \bot$, or $w = v$.

Thus, the model $\mathcal{M}^C$ is obtained from $\mathcal{M}$ by adding a single fallible element $\bot$ and connecting all worlds not satisfying $C$ to it, via $R_m$. It is not hard to verify that $\mathcal{M}^C$ fulfills the requirements of a constraint Kripke model, in particular that $R_m^C$ is a reflexive and transitive subrelation of $R_i^C$. Moreover, one checks that $\mathcal{M}^C$ has the properties (i) and (ii) of proposition 6.1. Thus, $\mathcal{M}^C$ is a model of PLL$^C$. Note that the models $\mathcal{M}^C$ actually are a rather restricted subclass of $\mathbf{M}^C$ satisfying the stronger property that if $w \neq v$, then $w\ R_m\ v$ iff $\mathcal{M}^C, w \not\models C$ and $v \in F$.

**Proposition 6.2 (Curry Models)** PLL$^C$ *is complete for the class of $\mathcal{M}^C$ models and, a fortiori, for the class of models satisfying the frame condition of proposition 6.1.*

**Proof:** Let formula $M$ be given such that for all intuitionistic Kripke models $\mathcal{M}$, $\mathcal{M}^C \models M$. Since $\mathcal{M}^C$ validates the axioms $\bigcirc K \equiv C \supset K$, we get $\mathcal{M}^C \models M^C$, where $M^C$ is obtained from $M$ by replacing all occurrences of sub-formulas $\bigcirc K$ by $C \supset K$. But now $M^C$ is a modal-free formula for which validity in $\mathcal{M}^C$ and $\mathcal{M}$ coincide. Thus, $\mathcal{M} \models M^C$, for all intuitionistic models $\mathcal{M}$. Then, by completeness of IPC, there is a derivation of $M^C$ in IPC. Since IPC is a subcalculus of PLL we have $\vdash_{\mathrm{PLL}} M^C$. From this, by extensionality of PLL it is easy to conclude that PLL $+ \bigcirc M \equiv (C \supset M)$ derives $M$. ∎

On might wonder whether PLL proper is complete for the class of all Curry models, *i.e.* for $\mathbf{M} = \bigcup_C \mathbf{M}_C$. This is not the case. For instance, the axiom scheme $(\bigcirc M \supset \bigcirc N) \supset \bigcirc(M \supset N)$ is valid in $\mathbf{M}$ but is not a theorem of PLL (see the counter model in figure 3). So, there is more to say about constraints than what is covered by the Curry contexts. Intuitively, Curry's constraint interpretation $\bigcirc M \equiv C \supset M$ involves a 'positive' constraint $C$: "*if* $C$ *then* $M$". But what about the 'negative' version "*if not* $C$ *then* $M$"? It is, of course, intuitionistically not the same as "*if* $\neg C$ *then* $M$", whence it cannot be reduced to the positive version with a negated constraint. We need a new constraint context, and in fact this negative constraint can be formalized by the axiom $\bigcirc M \equiv (C \vee M)$. Let

$$\mathrm{PLL}_C \;:=\; \mathrm{PLL} \;+\; \bigcirc M \equiv (C \vee M),$$

where again $C$ is fixed, and let $\mathbf{M}_C$ be the class of (antisymmetric) Kripke constraint models validating $\mathrm{PLL}_C$. Then we get the following result:

**Proposition 6.3**

- $\mathbf{M}_C$ *is characterized by the frame conditions (i)* $\forall w.\, w \models C \;\Rightarrow\; \exists u.\, w\, R_m\, u \;\;\&\;\; u \in F$, *and (ii)* $\forall w, u.\, (w \not\models C \;\;\&\;\; w\, R_m\, u) \;\Rightarrow\; w = u$, *and*
- $\mathrm{PLL}_C$ *is complete for this class of models.*

**Proof:** The first frame condition says that from every world $w$ validating $C$ a fallible world is accessible via $R_m$. This is necessary and sufficient for validity of $(C \vee M) \supset \bigcirc M$ (for necessity put $M = \mathit{false}$). The second condition says that if $w$ is not validating $C$ then it is a terminal with respect to $R_m$. This is necessary and sufficient to ensure the other direction $\bigcirc M \supset (C \vee M)$ (for necessity put $M = A$ where $A$ is a pc not occurring in $C$).

The argument for completeness proceeds along similar lines as for $\mathrm{PLL}^C$. By adjoining a single new fallible node $\perp$ one constructs for every intuitionistic Kripke model $\mathcal{M}$ a constraint model $\mathcal{M}_C$ such that for $w \neq v$, $w\, R_m^C\, v$ iff $\mathcal{M}, w \models C$ and $v = \perp$. This model is constructed to satisfy the frame condition and the condition that for modal-free $K$, $\mathcal{M}_C, w \models K$ iff $\mathcal{M}, w \models K$. The rest is as in the proof of proposition 6.2, where instead of $M^C$ we take $M_C$ obtained from $M$ by replacing every occurrence of a sub-formula $\bigcirc K$ by $C \vee K$. ∎

The reader may check that this second constraint interpretation of $\bigcirc$ provides us with a class of models in which the axiom scheme $\bigcirc(M \vee N) \supset (\bigcirc M \vee \bigcirc N)$ is always valid, while

$\neg\bigcirc\mathit{false}$ is strongly incompatible in the sense that if we add it to $\mathrm{PLL}_C$ then $\bigcirc M \equiv M$ becomes derivable. Furthermore, the axiom scheme $(\bigcirc M \supset \bigcirc N) \supset \bigcirc(M \supset N)$ is invalid. It is equivalent to the axiom $C \vee \neg C$, *i.e.* the assumption that constraint $C$ is "classical," in which case $C \vee M \equiv \neg C \supset M$, so that the positive and negative constraint contexts are interdefinable.

The last interpretation we wish to consider is given by the theory

$$\mathrm{PLL}^* \quad := \quad \mathrm{PLL} \; + \; \bigcirc M \equiv ((M \supset \mathit{false}) \supset \mathit{false}),$$

in which $\bigcirc M$ can be read as '$M$ holds classically'. Notice, $\mathrm{PLL}^*$ contains the axioms $\neg\bigcirc\mathit{false}$ and $(\bigcirc M \supset \bigcirc N) \supset \bigcirc(M \supset N)$, but not $\bigcirc(M \vee N) \supset (\bigcirc M \vee \bigcirc N)$.

**Proposition 6.4**

- $\mathrm{PLL}^*$ *is sound and complete for the class of constraint models satisfying* $R_m = R_i$ *and* $F = \emptyset$.

**Proof:** Soundness is easy to verify. For completeness we exploit completeness of IPC as before. Given an intuitionistic Kripke model $\mathcal{M} = (W, R_i, V)$ we consider the constraint model $\mathcal{M}^*$ obtained from $\mathcal{M}$ by taking $R_m = R_i$ and $F = \emptyset$. Then, $\mathcal{M} \models M$ iff $\mathcal{M}^* \models M^*$ where $M^*$ is obtained from $M$ by replacing all occurrences of $\bigcirc$ by double negation. ∎

One might wonder in which sense $\bigcirc M \equiv \neg\neg M$ is a constraint interpretation, or more precisely what notion of constraint is involved in the statement '$M$ holds classically'. The answer is simple, the constraint is the Excluded Middle (or some equivalent classical principle):

**Proposition 6.5** *Let $M$ be a formula of* IPC *and $pcs(M)$ the set of propositional constants in $M$. Then,*

$$\neg\neg M \equiv ((\bigwedge_{A \in \mathrm{pcs}(M)} A \vee \neg A) \supset M)$$

*is a theorem of* IPC.

**Proof:** One can construct a derivation verifying the statement by induction on $M$. Alternatively, one uses the fact that IPC is complete for the class of *finite* intuitionistic Kripke models (see *e.g.* [Dummett, 1977]) and shows that on finite models the equivalence is valid semantically. ∎

Proposition 6.5 implies that the theory of $\bigcirc M \equiv \neg\neg M$ is equivalent to the theory of $\bigcirc M \equiv ((\bigwedge_{A \in \mathrm{pcs}(M)} A \vee \neg A) \supset M)$, or — in second-order propositional logic — to the theory

$$\bigcirc M \equiv (\forall p.\, p \vee \neg p) \supset M.$$

In other words, $\mathrm{PLL}^*$ is a constraint interpretation of $\bigcirc$ of the Currian form $\mathrm{PLL}^C$, where the constraint $C$ is of second-order nature.

# 7 Two Concrete Classes of Constraint Models

In this section we present two concrete classes of constraint models that arise naturally in hardware verification. In both cases the modality $\bigcirc$ is interpreted to express truth up to stabilization constraints. They are obtained from the dynamic behaviour of combinational circuits under explicit modelling of propagation delays, so that $\bigcirc M$ means there exists a timing constraint $d$ such that the circuit stabilizes in state $M$ after time delay $d$. The two types of models represent two different ways of formalizing this idea. The first one, discussed in section 7.1, is related to the intermediate logic of Maksimova [Maksimova, 1986] and the second one, which will be discussed in section 7.2 is related to an intermediate logic due to Kolmogorov and Medvedev [Medvedev, 1966].

## 7.1 Combinational Circuits I

The standard way of interpreting propositional logic on circuits is to associate propositional constants with input and output signals of combinational gates, so that the truth values correspond to *high* and *low* voltages. The PLL models to be investigated in this section are set up such that for a propositional constant $A$

$$\left.\begin{array}{r} A \\ \neg A \\ \bigcirc A \\ \bigcirc\neg A \end{array}\right\} \quad \text{means} \quad \left\{\begin{array}{l} \text{`}A \text{ is stable } \textit{high}\text{'} \\ \text{`}A \text{ is stable } \textit{low}\text{'} \\ \text{`}A \text{ is going to stabilize to } \textit{high}\text{'} \\ \text{`}A \text{ is going to stabilize to } \textit{low.}\text{'} \end{array}\right.$$

In this way we wish to retain the ideal 'static' interpretation of truth values while safely keeping track of the offset to the real signals caused by propagation delays.

Formally, signals may be conceived as Boolean-valued functions over the time domain $\mathbb{N}$ of natural numbers, the Boolean values $\mathbb{B}$ being denoted by 1 and 0. A circuit interpretation of PLL then is given by a map $\mathcal{I}$, called a *timing diagram*, assigning to each propositional constant $A$ a function $\mathcal{I}(A) : \mathbb{N} \to \mathbb{B}$.

Given a timing diagram $\mathcal{I}$ we will construct a constraint model $\mathcal{M}(\mathcal{I})$, so that the induced semantics for PLL complies with the informal reading of formulas given above. The worlds of $\mathcal{M}(\mathcal{I})$ are closed-open time intervals obtained from breaking the signal waveform $\mathcal{I}$ into pieces. We adopt a Leibnizian view of time which takes the process of time to be given by events, *i.e.* state changes. This means that the only intervals we can form for a given $\mathcal{I}$ are the $[s, t)$, where both $s$ and $t$ mark a signal change. A time $t + 1$ marks a signal change if there exists $A$ such that $\mathcal{I}(A)(t) \neq \mathcal{I}(A)(t + 1)$. Let us call these intervals the *Leibniz* intervals of $\mathcal{I}$. As special cases of Leibniz intervals $[s, t)$ we allow $s, t = 0$, $t = \infty$ and empty intervals with $s = t$. An example can be seen in figure 4. It depicts two signals $\mathcal{I}(A)$ and $\mathcal{I}(B)$ with their signal changes at times $t_0 = 0, t_1, \ldots, t_7$. The Leibniz intervals, then, are $[t_i, t_j)$, and $[t_i, \infty)$, $i, j = 0, \ldots 7$, $i \leq j$.

Given a timing diagram $\mathcal{I}$, a constraint model

$$\mathcal{M}(\mathcal{I}) \quad \overset{df}{=} \quad (W(\mathcal{I}), R_i(\mathcal{I}), R_m(\mathcal{I}), V(\mathcal{I}), F(\mathcal{I}))$$

is constructed as follows:

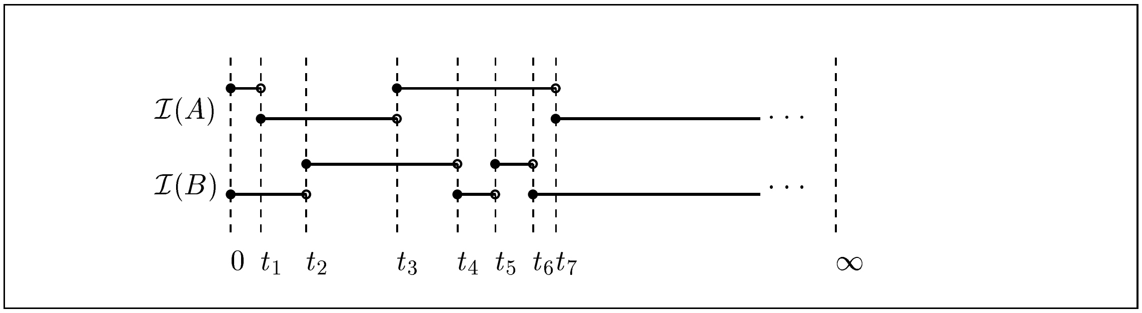

Figure 4: An Example Interpretation.

- $W(\mathcal{I})$ is the set of Leibniz intervals for $\mathcal{I}$
- $[s,t)\ R_i(\mathcal{I})\ [s',t')$ if $[s',t')$ is a subinterval of $[s,t)$
- $[s,t)\ R_m(\mathcal{I})\ [s',t')$ if $[s',t')$ is a final subinterval of $[s,t)$, *i.e.* $t = t'$ and $s \leq s'$
- $[s,t) \in V(\mathcal{I})(A)$ if $\mathcal{I}(A)$ is constant 1 throughout $[s,t)$, *i.e.* $\forall x.\ s \leq x < t, \mathcal{I}(A)(x) = 1$
- $F(\mathcal{I})$ is the set of empty intervals $[s,s)$.

The set $W(\mathcal{I})$ is clearly nonempty, as it always contains the pairs $[0,0)$ and $[0,\infty)$. The other properties of a constraint Kripke model are easily verified. Also, as this model is confluent, it satisfies the axiom $\bigcirc(M \vee N) \supset (\bigcirc M \vee \bigcirc N)$. Let us write $\mathcal{I} \models M$ instead of $\mathcal{M}(\mathcal{I}) \models M$ from now on.

**Proposition 7.1** *Let $A$ be an atomic proposition.*

- $\mathcal{I} \models A$ *iff* $\mathcal{I}(A)$ *is constant* 1.
- $\mathcal{I} \models \neg A$ *iff* $\mathcal{I}(A)$ *is constant* 0.
- $\mathcal{I} \models \bigcirc A$ *iff* $\mathcal{I}(A)$ *stabilizes eventually to* 1*, i.e. there is a* $k \geq s$ *such that* $\forall x \geq k.\mathcal{I}(A)(x) = 1$.
- $\mathcal{I} \models \bigcirc\neg A$ *iff* $\mathcal{I}(A)$ *stabilizes eventually to* 0.

**Proof:** Easy. ∎

Thus, the semantics of the basic modalities is as anticipated at the beginning of this section. In particular, we notice that in this interpretation the intuitionistic nature of PLL is intimately tied up with transient behaviour: $\mathcal{I} \models A \vee \neg A$ iff $\mathcal{I}(A)$ is stable.

In analyzing the meaning of formulas it is helpful to realize that $t < \infty$ implies $[s,t) \models \bigcirc M$ for any $M$, *i.e.* finite intervals validate any $\bigcirc$-formula. This is a consequence of the fact that from finite intervals there is always the empty final subinterval reachable through

$R_m(\mathcal{I})$. Intuitively, a finite Leibniz interval does not carry stability information, as it represents an intermediate phase of the circuit's execution.
With this in mind we may unroll the semantics of some formulas to find that we can express various types of stabilization behaviour:

**Proposition 7.2** *Let $A, B$ be propositional constants.*

- $\mathcal{I} \models \bigcirc(A \vee \neg A)$ *iff* $\mathcal{I}(A)$ *stabilizes eventually.*
- $\mathcal{I} \models \neg \bigcirc \mathit{false}$ *iff all signals are constant in* $\mathcal{I}$.
- $\mathcal{I} \models (A \vee \neg A) \supset \bigcirc \mathit{false}$ *iff* $\mathcal{I}(A)$ *oscillates indefinitely.*
- $\mathcal{I} \models \bigcirc A \supset \neg B$ *iff whenever* $\mathcal{I}(B)$ *switches to* $1$ *all signals have become stable for good and* $\mathcal{I}(A)$ *rests at* $0$.

**Proof:** Easy. ∎

It can be seen that if the circuit stabilizes completely at some time $s$, then both $\mathcal{I}, [s, \infty) \models A \vee \neg A$ and $\mathcal{I}, [s, \infty) \models \bigcirc A \equiv A$ for all $A$. Thus, after stabilization, the theory reduces to ordinary classical Boolean algebra, which is what one expects.
We might specify the falling output transition of an invertor by the formula $A \supset \bigcirc \neg B$, "if $\mathcal{I}(A)$ becomes stable 1 for good then eventually $\mathcal{I}(B)$ becomes stable 0 for good". Similarly, $\neg A \supset \bigcirc B$ would capture the rising output transition. Given this axiomatization we might consider a ring circuit consisting of an odd number of invertors. Then, if $A$ represents any one of the signals within the ring our logic would derive the formula $(A \supset \bigcirc \neg A) \wedge (\neg A \supset \bigcirc A)$ which says precisely that $\mathcal{I}(A)$ oscillates. This is much closer to the behaviour of the real circuit than the classical theory of the invertor ring leading to $A \equiv \neg A$, which is plainly inconsistent.
One can show that the $\bigcirc$-free fragment also allows us to specify nontrivial dynamic behaviour: it is possible to specify state and transition invariants, say that two signals may never be 1 at the same time, or in a certain state never switch at the same time.

Let us call the theory induced by the circuit models $\mathcal{M}(\mathcal{I})$, for arbitrary timing diagrams $\mathcal{I}$, *Circuit*-PLL. Now, in view of its nontrivial expressibility it is natural to ask whether one can find a (finite) complete axiomatization for Circuit-PLL. Though some axioms are known this question remains open at the time of writing. The following axiom schemes are valid in (but not complete for) Circuit-PLL:

- $\bigcirc(M \vee N) \supset (\bigcirc M \vee \bigcirc N)$
- $\neg \bigcirc \mathit{false} \supset (M \vee \neg M)$
- $(((L \supset M \vee N) \supset M \vee N) \;\wedge\; ((M \supset L \vee N) \supset L \vee N)$
  $\wedge\; ((N \supset L \vee M) \supset L \vee M)) \;\supset\; L \vee M \vee N$
- $((\neg\neg M \supset M) \supset M \vee \neg M) \supset \neg M \vee \neg\neg M$
- $\neg\neg A \supset A$ for propositional constants $A$

The first axiom scheme has been noted before and stems from the confluence of both accessibility relations in the circuit models. The second axiom scheme we have encountered implicitly in the semantic discussions above. It shows how $\bigcirc$ depends upon the fallible nature of the models: if the axiom $\neg\bigcirc \mathit{false}$ excluding fallible nodes is added, Circuit-PLL becomes equivalent to classical propositional logic. Thus, although its semantics involves time the modal operator $\bigcirc$ is rather different from a temporal operator such as 'eventually'. The third axiom scheme is Gabbay and DeJongh's binary tree formula $D_1$ [Gabbay and DeJongh, 1974] and the fourth Scott's axiom [Kreisel and Putnam, 1957]. Both follow directly from the structure of the circuit models' accessibility relation $R_i(\mathcal{I})$. The last axiom is easy to verify; it reflects the stability of the truth valuation for propositional constants. Note that this axiom does not hold as a scheme since for instance $\neg\neg(A \vee B) \supset A \vee B$ is not valid. This means that Circuit-PLL is a *nonstandard* logic, *i.e.* not closed under substitution. We might point out that this feature, of not being closed under substitution, parallels the characteristics of dynamic systems. The functional behaviour of an asynchronous circuit, for instance, is not preserved when substituting a composite circuit for a functionally equivalent primitive subcomponent. Replacing a multi-input AND gate by a cascade of 2-input ANDs, say, may introduce critical hazards that corrupt the functional operation.

Finally, it should be mentioned that the $\bigcirc$-free fragment of Circuit-PLL, *i.e.* the intuitionistic base of Circuit-PLL, deserves some attention in itself. For it coincides with the *regular* form of Maksimova's intermediate logic $L\Pi$ [Maksimova, 1986], more precisely we have

$$\bigcirc\text{-free Circuit-PLL} \quad = \quad L\Pi + \{\, \neg\neg A \supset A \mid A \text{ propositional constant}\,\}.$$

This follows from the fact that both theories are generated by essentially by the same class of Kripke models, *viz.* finite nonempty sequences of bit-vectors. For $L\Pi + \{\neg\neg A \supset A\}$ this can be deduced from the definition of $L\Pi$ and the semantics of the regularity axioms $\neg\neg A \supset A$. For Circuit-PLL this can be seen as follows. We first observe that in the $\bigcirc$-free fragment we can restrict ourselves to finite timing diagrams, *i.e.* those with a finite number of signals which all eventually stabilize: a $\bigcirc$-free formula is valid iff it is valid in all finite timing diagrams. We can then further simplify the interpretation noting that validity does not depend on the absolute length of an interval. Thus, we may identify a finite timing diagram over $n$ pcs with its underlying sequence of $n$-bit states. For instance, the finite interval $[t_2, t_6)$ in figure 4 corresponds to the state sequence $01, 11, 10, 11$ where the first bit corresponds to propositional constant $A$ and the second to $B$. Since the validity of formulas in the $\bigcirc$-free fragment is unaffected by the presence of empty intervals, we may as well restrict ourselves to non-empty sequences. This shows that the models for $\bigcirc$-free Circuit-PLL can be reduced to nonempty finite sequences of bit-vectors. This observation leads to a simple proof of the following:

**Proposition 7.3** *$\bigcirc$-free Circuit-*PLL*, or regular $L\Pi$, is decidable.*

**Proof:** Let $\Sigma^+$ denote the set of all non-empty sequences of $n$-bit vectors and for two such sequences $w$, $v$, let $w \sqsubseteq v$ if there exist $v_1, v_2$, possibly empty, such that $v = v_1 w v_2$. Now to every formula $M$ whose propositional constants are among $p_1, \ldots, p_n$ we may assign a subset $[\![M]\!]$ of $\Sigma^+$ in the following way:

$$\begin{array}{lcl}
[\![\mathit{true}]\!] & = & \Sigma^+ \\
[\![\mathit{false}]\!] & = & \emptyset \\
[\![p_i]\!] & = & \{\, s_0 s_1 \cdots s_m \in \Sigma^+ \mid \forall j \leq m.\ (s_j)(i) = 1 \,\} \\
[\![M \wedge N]\!] & = & [\![M]\!] \cap [\![N]\!] \\
[\![M \vee N]\!] & = & [\![M]\!] \cup [\![N]\!] \\
[\![M \supset N]\!] & = & \{\, w \in \Sigma^+ \mid \forall u \sqsubseteq w.\ u \in [\![M]\!] \Rightarrow u \in [\![N]\!] \,\} \\
[\![\neg M]\!] & = & \{\, w \in \Sigma^+ \mid \forall u \sqsubseteq w.\ u \notin [\![M]\!] \,\}.
\end{array}$$

It is straightforward to show that for every timing diagram $\mathcal{I}$ and every formula $M$, $\mathcal{I} \in [\![M]\!]$ iff $\mathcal{I} \models M$; it is almost as straightforward to show that $[\![M]\!]$ is a regular language, from which decidability follows immediately. ∎

### 7.2 Combinational Circuits II

We now discuss a second type of constraint models for combinational circuits that uses $\bigcirc$ to account for propagation delays. In contrast to the previous model we will now distinguish between signal values and truth values. A propositional constant $A$ represents an atomic statement about the stabilization behaviour of an associated signal $a$. For a Boolean signal $a$ there are two atomic statements we are interested in: "$a$ is stable *high*," which may be written $a = 1$, and "$a$ is stable *low*," written $a = 0$. In this vein, we assume that the propositional constants of PLL are of the form $a = 1$ or $a = 0$ where $a$ ranges over a countably infinite number of signals $\mathbb{S} = \{a, b, c, c_1, c_2, \cdots\}$. A timing diagram, now, is a function $V : \mathbb{S} \to \mathbb{N} \to \mathbb{B}$ that maps every signal $a \in \mathbb{S}$ to a function $V(a) : \mathbb{N} \to \mathbb{B}$. We will interpret PLL over sets of timing diagrams rather than single timing diagrams. More precisely, a *circuit* in this section is conceived as a *time-invariant* subset $C \subseteq \mathbb{S} \to \mathbb{N} \to \mathbb{B}$. Here $C$ is called time invariant if $C^d \subseteq C$ for all $d \in \mathbb{N}$, where $C^d$ is obtained from $C$ by shifting all $V \in C$ left by an amount of $d$. Formally, we define $V^d$ such that $V^d(a)(t) = V(a)(t + d)$, and then $C^d = \{\, V^d \mid V \in C \,\}$. Each element $V \in C$ represents a possible waveform for $C$, called an *observable behaviour*, or *execution* of $C$.

Given the circuit $C$, a constraint Kripke model

$$\mathcal{M}(C) \quad \overset{df}{=} \quad (W(C), R_i(C), R_m(C), V(C), F(C))$$

is constructed as follows:

- $W(C)$ is the set of pairs $(D, s)$ where $D \subseteq C$ is time invariant and $s \in \mathbb{N}$
- $(D, s)\ R_i(C)\ (E, t)$ if $E \subseteq D$ and $t \geq s$
- $(D, s)\ R_m(C)\ (E, t)$ if $E = D$ and $t \geq s$
- $(D, s) \in V(C)(a = 1)$ if for all $V \in D$, $V(a)$ stabilizes to 1 before time $s$, *i.e.* $\forall x \geq s.\ V(a)(x) = 1$

- $(D, s) \in V(C)(a = 0)$ if for all $V \in D$, $V(a)$ stabilizes to 0 before time $s$, *i.e.* $\forall x \geq s.\, V(a)(x) = 0$
- $F(C) = \{\, (\emptyset, s) \mid s \in \mathbb{N} \,\}$.

The set $W(C)$ is clearly nonempty, and the other properties of a constraint Kripke model are easily verified, too. Note also that this model is confluent, *i.e.* it satisfies the axiom $\bigcirc(M \vee N) \supset (\bigcirc M \vee \bigcirc N)$. Furthermore one checks that $\neg\bigcirc \mathit{false}$ is valid as well, which suggests that fallible worlds are redundant in this model. In fact, they could be removed without changing the semantics of formulas, but keeping the empty sets is technically convenient.

The constraint models $\mathcal{M}(C)$ induce an interesting semantics of bounded stabilization for PLL. Let us write $C \models M$ instead of $\mathcal{M}(C) \models M$ to denote validity with respect to this class of models. Propositional constants are atomic stabilization predicates: $C \models a = i$ states that signal $a$ is constant $i$ in all executions $V \in C$. It will be useful to introduce $(a = i)^{\downarrow}(V, t)$ as an abbreviation for the semantic stabilization condition $\forall x \geq t.\, V(a)(x) = i$. If $A$ is a propositional constant, then $(D, s) \models A$ is the same as $\forall V \in D.\, A^{\downarrow}(V, s)$.

**Proposition 7.4** *Let $A, B$ be propositional constants. Then, $C \models A \supset \bigcirc B$ iff there exists $d \in \mathbb{N}$ such that for all $V \in C$ and $t \in \mathbb{N}$, $A^{\downarrow}(V, t)$ implies $B^{\downarrow}(V, t + d)$.*

**Proof:** $C \models A \supset \bigcirc B$ is equivalent to $(C, 0) \models A \supset \bigcirc B$ since $(C, 0)$ is the least element in $\mathcal{M}(C)$. Unrolling the semantical definitions this is equivalent to

$$\forall D \subseteq C.\, \forall t \geq 0.\, (\forall V \in D.\, A^{\downarrow}(V, t)) \Rightarrow (\exists d \geq t.\, \forall V \in D.\, B^{\downarrow}(V, d)), \tag{1}$$

where $D$ is time-invariant. In particular consider the time-invariant subset $D^* = \{\, V \in C \mid A^{\downarrow}(V, 0) \,\}$ of $C$, so that $\forall V \in D^*.\, A^{\downarrow}(V, 0)$ is trivially true. If we instantiate $D$ in (1) by $D^*$ and $t$ by 0, then (1) reduces to $\exists d \geq 0.\, \forall V \in D^*.\, B^{\downarrow}(V, d)$, which is the same as $\exists d.\, \forall V \in C.\, A^{\downarrow}(V, 0) \Rightarrow B^{\downarrow}(V, d)$. Making use of the time invariance of $C$ this finally gives us

$$\exists d.\, \forall V \in C.\, \forall t \in \mathbb{N}.\, A^{\downarrow}(V, t) \Rightarrow B^{\downarrow}(V, t + d). \tag{2}$$

The converse can be shown too, *viz.* that (2) implies (1). ∎

Thus, a formula like $a = 1 \supset \bigcirc(b = 1)$ comes down to a boundedly-gives-rise-to statement: "there exists a stabilization bound $d$ so that whenever $a$ becomes stable 1, $b$ will become stable 1 with a maximal delay $d$". More generally, $A \supset \bigcirc B$ specifies a bounded transition from $A$ to $B$. Note that the ordering of quantifiers in the statement of proposition 7.4 is crucial: $\exists d\ \forall V$ means that the delay $d$ is a *uniform* bound for *all* executions of $C$. In contrast, swapping the quantifiers to $\forall V\ \exists d$ would permit the delay to depend on the particular execution, and in particular to be unbounded over all $V \in C$. We may call $d$ a *uniform stabilization bound* for the transition $A \supset \bigcirc B$ and $\forall V \in C.\, \forall t \in \mathbb{N}.\, A^{\downarrow}(V, t) \Rightarrow B^{\downarrow}(V, t+d)$ the *stabilization refinement* of $A \supset \bigcirc B$ by $d$. More formally, we may introduce $(A \supset \bigcirc B)^{\downarrow}(V, d)$ as an abbreviation for $\forall t.\, A^{\downarrow}(V, t) \Rightarrow B^{\downarrow}(V, t+d)$. With this notation we may restate proposition 7.4 as follows: $C \models A \supset \bigcirc B$ iff there exists a stabilization bound $d \in \mathbb{N}$ such that for all $V \in C$, the stabilization refinement $(A \supset \bigcirc B)^{\downarrow}(V, d)$ is true. We omit the proof of

**Proposition 7.5** *Let $A_1, A_2, B_1, B_2$ be propositional constants. Then, $C \models (A_1 \supset \bigcirc B_1) \supset (A_2 \supset \bigcirc B_2)$ iff there exists $f : \mathbb{N} \to \mathbb{N}$ such that for all $V \in C$ and $d \in \mathbb{N}$, $(A_1 \supset \bigcirc B_1)^{\downarrow}(V, d)$ implies $(A_2 \supset \bigcirc B_2)^{\downarrow}(V, f\, d)$.*

It turns out that the structure brought up by propositions 7.4 and 7.5 can be lifted to arbitrary formulas. One can assign to every formula $M$ of PLL a set $[\![M]\!]$ of stabilization bounds and for every $d \in [\![M]\!]$ construct a stabilization refinement $M^{\downarrow}(V, d)$ of $M$ by $d$. It can be shown that in this way an equivalent characterization of the Kripke constraint models introduced in this section can be obtained, *viz.* that $C \models M$ iff there exists a $d \in [\![M]\!]$ such that $M^{\downarrow}(V, 0)$ is true for all $V \in C$. This refinement semantics can be viewed essentially as a set-theoretic realizability semantics for PLL, which can be used for the extraction of data-dependent timing information [Mendler, 1996, Mendler and Fairtlough, 1996].

To finish off this section let us mention some distinguished special situations contained in this type of constraint models. First we notice that if $C = \{V\}$ consists of a single constant execution $V$ (*i.e.* one in which all signals are constant), then validity coincides with ordinary classical validity. Such $C$ satisfies the axioms $M \vee \neg M$ and $\bigcirc M \equiv M$, and we have $C \models M$ iff $M$ is classically valid for $V$, where an atomic sentence $a = i$, is read as "signal $a$ is constant $i$". This special case corresponds to the usual *static* two-valued model of circuits.

Another way in which the classical two-valued reasoning can be embedded into the semantics is the following one: as one verifies readily, for arbitrary $C$, $C \models \neg\neg M$ iff $M$ is classically valid on all $V \in C$, where $a = i$ is read as "signal $a$ will stabilize to $i$". This means that double negated formulas are classical statements about the *stationary* state of a circuit. To be more precise, these are classical statements in a three-valued setting in which a signal $a$ can be stable 1, stable 0, or oscillate. The latter value is represented by the formula $\neg(a = 1) \wedge \neg(a = 0)$. If $C$ is a circuit in which all signals eventually stabilize, then $C \models \neg\neg(a = 1 \vee a = 0)$ and we get back, under double negation, the classical two-valued model of the final stable state.

A third interesting special case are the constant circuits $C$ consisting of an arbitrary subset of constant executions. In such circuits the time dimension is completely eliminated and $\bigcirc M$ is equivalent to $M$. Assuming that we are interested in the validity of formulas containing an arbitrary but fixed finite number of signals $a_1, a_2, \ldots, a_n$, every execution $V \in C$ can be reduced to a finite vector $V \in \mathbb{B}^n$ in the apparent way. Thus, every constant circuit $C$ can be identified with a subset $C \subseteq \mathbb{B}^n$ of Boolean vectors. Validity in the set of all constant circuits then coincides with ordinary intuitionistic validity in the lattice $L_n = (\wp(\mathbb{B}^n), \supseteq)$ with regular valuations and $\emptyset$ as fallible element. A valuation is regular if for all propositional constants $A$ and $D \subseteq \mathbb{B}^n$, $D \models A$ iff $\forall V \in D.\ \{V\} \models A$. The regular intuitionistic theory of the lattices $L_n$ (with $\emptyset$ fallible), and hence the theory of all constant circuits, can be shown to coincide with Medvedev's intermediate logic of *singleton problems* [Medvedev, 1966]. A complete axiomatization for Medvedev's singleton problems has been given by [Miglioli et al., 1989], where the theory is called $F_{cl}$.

# 8 Conclusion

We have presented a new viewpoint on a little-explored intuitionistic modal logic, PLL, which is a conservative extension of the standard intuitionistic propositional calculus by a single modal operator $\bigcirc$. We show that, besides representing a notion of "local truth" or playing a rôle as the type theory of the computational $\lambda$-calculus, $\bigcirc$ can be used to capture the notion of 'correctness-up-to-constraints'. The advantage of the framework we present here is that it provides a precise definition of constraint correctness that permits more or less arbitrary instantiation while enjoying an intriguing yet tractable meta-theory.

The main result is that PLL has a natural class of two-frame Kripke models for which it is sound and complete, and moreover the finite model property holds. This provides a satisfactory model-theoretic account of the modality $\bigcirc$ in an intuitionistic setting. In particular, the Kripke models allow us to establish an embedding of PLL in a classical bimodal theory that extends Gödel's translation. On the proof-theoretic side it is shown that PLL, despite being a modal logic, inherits many of the properties of intuitionistic logic, *viz.* deduction theorem, a simple cut-free sequent calculus, the disjunction property, and strong extensionality.

We have given a number of concrete models for PLL, two of them motivated from hardware verification. In these we interpret PLL over timing diagrams in two different ways such that $\bigcirc$ expresses truth up to stabilization. The first of these models is related to Maksimova's logic $L\Pi$ and the second to Medvedev's intermediate constructive logic of singleton problems. We have used our characterisation of the first model to find a simple proof of the decidability of the regular form of $L\Pi$.

For circuits where delays do not invalidate functional correctness, such as synchronous circuits, it is often necessary or advantageous to combine functional and timing analysis so as to derive the exact data-dependent delay of combinational circuitry. We believe that PLL can be used to do this with standard proof extraction techniques based on a concrete computational lambda calculus as mentioned in the introduction. The applicability of PLL to hardware verification and constraint handling still deserves to be explored in more detail. The first results obtained by the authors, however, are very promising indeed.

# 9 Acknowledgements

Rod Burstall and Terry Stroup have had decisive influence on the development and presentation of this work. Michael Mendler is indebted to Rod for his encouragement and stimulating supervision of the author's Ph.D. research, on which this work is built.
Thanks are also due to Roy Dyckhoff for his interest and for providing useful references to the literature. The authors are grateful to Nick Benton for discussions on the computational interpretation of PLL, to Pierangelo Miglioli for pointing out the connection with Maksimova's intermediate logic, and to the two anonymous referees for their helpful comments and suggestions.
Michael Mendler was supported by a Human Capital and Mobility fellowship in the *EuroForm* network, and by the *Deutsche Forschungsgemeinschaft.*

## References

[Avellone and Ferrari, 1996] Avellone, A. and Ferrari, M. (1996). Almost duplication-free tableau calculi for propositional lax logics. In Miglioli, P., Moscato, U., Mundici, D., and Ornaghi, M., editors, *Proceedings of the 5th International Workshop on Theorem Proving with Analytic Tableaux and Related Methods*. Springer LNAI 1071.

[Baccelli et al., 1992] Baccelli, F., Cohen, G., Olsder, G. J., and Quadrat, J.-P. (1992). *Synchronization and Linearity*. John Wiley and Sons.

[Benton et al., 1993] Benton, N., Bierman, G., and de Paiva, V. (1993). Computational types from a logical perspective I. Technical Report, Computer Laboratory University of Cambridge, U.K.

[Chellas, 1980] Chellas, B. (1980). *Modal Logic*. Cambridge University Press.

[Curry, 1952] Curry, H. B. (1952). The elimination theorem when modality is present. *Journal of Symbolic Logic*, 17:249–265.

[Curry, 1957] Curry, H. B. (1957). *A Theory of Formal Deducibility*, volume 6 of *Notre Dame Mathematical Lectures*. Notre Dame, Indiana, second edition.

[Dummett, 1977] Dummett, M. (1977). *Elements of Intuitionism*. Clarendon Press, Oxford.

[Ewald, 1986] Ewald, W. B. (1986). Intuitionistic tense and modal logic. *Journal of Symbolic Logic*, 51.

[Fischer-Servi, 1980] Fischer-Servi, G. (1980). Semantics for a class of intuitionistic modal calculi. In Chiara, M. L. D., editor, *Italian Studies in the Philosophy of Science*, pages 59–72. Reidel.

[Fitting, 1983] Fitting, M. (1983). *Proof Methods for Modal and Intuitionistic Logics*. Reidel.

[Gabbay and DeJongh, 1974] Gabbay, D. M. and DeJongh, D. H. J. (1974). A sequence of decidable finitely axiomatizable intermediate logics with the disjunction property. *Journal of Symbolic Logic*, 39(1):67–78.

[Gödel, 1932] Gödel, K. (1932). Zum Intuitionistischen Aussagenkalkül. *Akademie der Wissenschaften in Wien, Mathematisch-Naturwissenschaftliche Klasse. Anzeiger.*, 69:65–66.

[Goldblatt, 1979] Goldblatt, R. I. (1979). *Topoi: The Categorical Analysis of Logic*. North Holland.

[Goldblatt, 1981] Goldblatt, R. I. (1981). Grothendieck topology as geometric modality. *Zeitschrift für mathematische Logik und Grundlagen der Mathematik*, 27:495–529.

[Johansson, 1936] Johansson, I. (1936). Der Minimalkalkül, ein reduzierter intuitionistischer Formalismus. *Compositio Math.*, 4:119–136.

[Kreisel and Putnam, 1957] Kreisel, G. and Putnam, H. (1957). Eine Unableitbarkeitsbeweismethode für den intuitionistischen Aussagenkalkül. *Archiv für Mathematische Logik und Grundlagenforschung*, 3:74–78.

[Macnab, 1981] Macnab, D. S. (1981). Modal operators on Heyting algebras. *Algebra Universalis*, 12:5–29.

[Maksimova, 1986] Maksimova, L. L. (1986). On maximal intermediate logics with the disjunction property. *Studia Logica*, 45:69–45.

[Medvedev, 1966] Medvedev, J. T. (1966). Interpretation of logical formulas by means of finite problems. *Soviet Math. Dokl.*, 7(4):857–860.

[Mendler, 1990] Mendler, M. (1990). Constrained proofs: A logic for dealing with behavioural constraints in formal hardware verification. In Jones, G. and Sheeran, M., editors, *Designing Correct Circuits*, pages 1–28. Springer.

[Mendler, 1993] Mendler, M. (1993). *A Modal Logic for Handling Behavioural Constraints in Formal Hardware Verification.* PhD thesis, Edinburgh University, Department of Computer Science, ECS-LFCS-93-255.

[Mendler, 1996] Mendler, M. (1996). Timing refinement of intuitionistic proofs and its application to the timing analysis of combinational circuits. In Miglioli, P., Moscato, U., Mundici, D., and Ornaghi, M., editors, *Proceedings of the 5th International Workshop on Theorem Proving with Analytic Tableaux and Related Methods*, pages 261–277. Springer LNAI 1071.

[Mendler and Fairtlough, 1996] Mendler, M. and Fairtlough, M. (1996). Ternary simulation: A refinement of binary functions or an abstraction of real-time behaviour? In Sheeran, M. and Singh, S., editors, *Proceedings of the 3rd Workshop on Designing Correct Circuits (DCC96).* Springer. Springer Electronic Workshops in Computing.

[Miglioli et al., 1989] Miglioli, P., Moscato, U., Ornaghi, M., Quazza, S., and Usberti, G. (1989). Some results on intermediate constructive logics. *Notre Dame Journal of Formal Logic*, 30(4):543–562.

[Moggi, 1991] Moggi, E. (1991). Notions of computation and monads. *Information and Computation*, 93:55–92.

[Plotkin and Stirling, 1986] Plotkin, G. and Stirling, C. (1986). A framework for intuitionistic modal logics. In *Theoretical aspects of reasoning about knowledge*, pages 399–406, Monterey.

[Popkorn, 1994] Popkorn, S. (1994). *First Steps in Modal Logic.* Cambridge University Press.

[Simmons, 1978] Simmons, H. (1978). A framework for topology. In Macintyre, A., Pacholski, L., and Paris, J., editors, *Logic Colloqium'77*, pages 239–251. North-Holland.

[Simpson, 1994] Simpson, A. (1994). *The Proof Theory and Semantics of Intuitionistic Modal Logic.* PhD thesis, University of Edinburgh, Department of Computer Science.

[Thompson, 1996] Thompson, S. (1996). *Haskell — The Craft of Functional Programming.* Addison-Wesley.

[Troelstra and van Dalen, 1988] Troelstra, A. S. and van Dalen, D. (1988). *Constructivism in Mathematics*, volume II. North-Holland.

M. Fairtlough, M. Mendler: Propositional Lax Logic. Information and Computation, Vol.137, No.1, 1997, pp. 1-33.