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
Technical University of Denmark
Department of Computer Science
Building 344
DK-2800 Lyngby, Denmark
Tel.: +45 4525 3721
Fax: +45 4588 4530
Email: mvm@id.dtu.dk

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

Abstract

We investigate a novel intuitionistic modal logic, called Propositional Lax Logic, with 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. The resulting logic is unorthodox in several respects. 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. As for hardware verification it is special since it is an intuitionistic rather than classical logic which so far has been the basis of the great majority of approaches. Finally, its models are unusual since they feature worlds with inconsistent information and furthermore the only frame condition is that the $\bigcirc$-frame be a subrelation of the $\supset$-frame.

In the paper we will provide the motivation for Propositional Lax Logic and present several technical results. We will investigate some of its proof-theoretic properties, and present a cut-elimination theorem for a standard Gentzen-style sequent presentation of the logic. We further show soundness and completeness for several classes of fallible two-frame Kripke models. In this framework we present a concrete and rather natural class of models from hardware verification such that the modality $\bigcirc$ models correctness up to timing constraints.

Finally, we explore the expressibility of the $\bigcirc$-free fragment of the logic over these concrete constraint models. We obtain decidability of this fragment, which coincides with the stable form of Maksimova's intermediate logic $L\Pi$.

1 Motivation

It is good engineering practice to think of the synthesis of a hardware device as proceeding through numerous levels of abstraction. The attempt to formalize this process in mathematical logic for the purpose of formal verification, however, faces a major obstacle: behavioural abstractions are genuine mathematical abstractions only up to behavioural constraints, *i.e.* under certain restrictions imposed on the device's environment. Timing constraints on input signals form an important class of such restrictions. Since correctness across abstraction levels is only correctness up to constraints, rather than correctness proper, the ambient formalism no longer provides a (uniform) notion of correctness across the abstraction boundary.

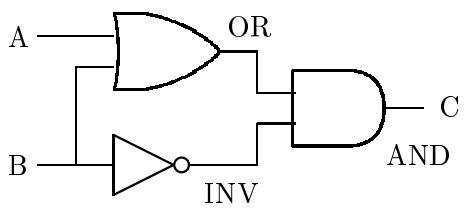

Figure 1: A Simple Combinational Circuit

A concrete example is the common timing abstraction at the gate level. It is convenient to reason about the static behaviour of a combinational circuit in terms of high or low voltage and to abstract away from propagation delays. This makes it possible to analyze large circuits by classical propositional logic and standard Boolean techniques. In this 'ideal' abstract setting the behaviour of the circuit shown in figure 1 may be specified by "if input A is 0 then output C is 0," formally

$$A = 0 \supset C = 0.$$

This abstract formulation elides, of course, much concrete-level detail. As a specification of static behaviour it is valid only as long as gate delays can be ignored. This is, however, not always the case. In the design of real circuits delays can cause considerable grief. *Races*, *hazards*, or *glitches* are delay-related phenomena that may render simple boolean reasoning unsound. In the real circuit corresponding to figure 1 for instance, a $1 \to 0$ transition on input B may produce a $0 \to 1 \to 0$ glitch on C even if A is constant 0, *viz.* whenever the delay through the inverter is sufficiently small compared to that through the or-gate. Thus, in the presence of propagation delays, the above specification is unsound.
So, how can we justify the 'ideal' abstract description in terms of the more concrete level? Well, the best we can expect is that instead of the original specification the 'real' behaviour satisfies but an approximation like

$$B \textit{ stable} \supset (A = 0 \supset (\textit{after some delay} \supset C = 0)),$$

weakened by the stability constraint 'B *stable*' to rule out the glitch, and by the timing constraint *'after some delay'* to account for the input/output propagation delay. The

trouble is that both constraints refer to time and thus belong to the concrete level of timed signals. Thus, the dominant formalism of Boolean algebra, or propositional logic for that matter, is not adequate to capture correctness of the timing abstraction. No problem, one might say, since of course at the low level one can make things precise, say by

$$\begin{array}{l}((\forall\tau.\ B(\tau)=0)\vee(\forall\tau.\ B(\tau)=1))\ \supset\\ \quad(\forall\tau.\ A(\tau)=0)\ \supset\ (\forall\tau.\ \tau\geq\Delta\ \supset\ C(\tau)=0).\end{array}$$

Though the state of the art in formal hardware verification this cannot be the answer as it jeopardizes the crucial distinction between the abstraction levels. We are throwing overboard the abstractness of the Boolean approach, and we are back where we started, entangled in the nitty-gritty details of exact timing verification.
Fortunately, there is a middle way of tackling the problem of approximative and incomplete abstractions: we employ a weakened notion of correctness, *viz. correctness-up-to-constraints*, and formalize it as a logical modality. The example circuit's behaviour then would be specified by

$$\bigcirc(A=0\ \supset\ \bigcirc(C=0)),$$

to be read as "under some constraint, if A is low, then under some constraint, C is 0". Thus, the modality $\bigcirc$ is used to account for the stability and timing constraints, which are no longer part of the specification but of the semantic model and of the correctness proofs. The technical advantages of this idea have been worked out in [Mendler, 1990, Mendler, 1993]. Given the great variety of uses that the notion of 'constraint' finds in hardware engineering, a general advantage of this framework is to provide a precise definition of constraint correctness that permits more or less arbitrary instantiation while yielding useful metamathematical results. To introduce a concrete instance of this framework and to explore some its potentials is the goal of this paper.

2 Propositional Lax Logic

We shall present a concrete formal calculus, *Propositional Lax Logic*, conceived along the lines set out in [Mendler, 1993]. The term 'lax logic' is chosen to indicate the 'looseness' associated with the notion of correctness up to constraints. Propositional Lax Logic, PLL, is an intuitionistic propositional calculus with a single modality $\bigcirc$. 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 following three axioms:

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

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

a (combined) constraint"; finally, $\bigcirc F$ says "if M implies N then if M holds under a constraint, N holds under a (the same) constraint." However innocent each of these axioms may appear in this informal reading, their combination results in a rather strange modality. 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 possibility while $\bigcirc F$ is typical for necessity. On the other hand, in standard systems, say Lewis' modal system $S4$ [Chellas, 1980], the axiom $\bigcirc R$ is never adopted for necessity while $\bigcirc F$ never for possibility, and in fact they would trivialize the modalities.
The second noteworthy feature of PLL is that it is an intuitionistic rather than classical logic which so far has been the basis of the great majority of approaches in the area of hardware verification. In [Mendler, 1990, Mendler, 1993] the intuitionistic nature has been exploited to extract constraints from proofs. Yet, dropping the Excluded Middle is not merely for pragmatic reasons: PLL is essentially intuitionistic in the sense that assuming the Excluded Middle and the axiom $\neg\bigcirc \mathit{false}$ trivializes $\bigcirc$, *i.e.* $\bigcirc M$ becomes provably equivalent to M. This is another indication for the 'strangeness' of $\bigcirc$ in the context of standard classical modal logics. Of course, we hope this paper will convince the reader that the $\bigcirc$ modality is actually a very natural one.

So, just what kind of modality is $\bigcirc$? Why should it be interesting at all and how does it relate to correctness-up-to constraints? In [Mendler, 1990, Mendler, 1993] $\bigcirc$ is motivated by a proof-theoretic interpretation. The present paper attempts to justify the axioms and their constraint interpretation by model-theoretic means. We will show that PLL has a natural class of Kripke models for which it is sound and complete. Two concrete subclasses of such models will be presented obtaining two concrete constraint interpretations of $\bigcirc$. These concrete models verify that PLL has nontrivial expressiveness and illustrate the benefit of dropping Excluded Middle and $\neg\bigcirc \mathit{false}$. But before we get to the technical results it may be appropriate to give some general justification of $\bigcirc$.

(1) Consider the most simple constraint interpretation, *viz.* $\bigcirc M \equiv C \supset M$, where C is an arbitrary but fixed constraint. Under this encoding all three axioms $\bigcirc R$, $\bigcirc M$, $\bigcirc F$ become tautologies of (intuitionistic) propositional logic. With modification, this generalizes to a set $\mathcal{C}$ of constraints: $\bigcirc M \equiv \Sigma C \in \mathcal{C}.\ C \supset M$ (see [Mendler, 1990]). The single constraint interpretation is precisely Curry's system LJZ [Curry, 1952]. PLL itself appears to have occurred for the first time in Curry's 1948 Notre Dame lectures on *A Theory of Formal Deducibility* [Curry, 1957]. These lectures contain some sketchy remarks on a $\Diamond$ modality endowed with axiom schemata that are essentially equivalent to the ones we are adopting for $\bigcirc$. The present paper may be seen as giving a model-theoretic account of Curry's proof-theoretic $\Diamond$ and in particular of LJZ.
(2) A second motivation for $\bigcirc$ can be drawn from general type theory. The formal properties of $\bigcirc$ viewed as an unary type constructor are precisely the data of a strong closure operator, or 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 PLL and bi-Cartesian closed categories with a strong monad. This categorical structure is also known as the computational lambda calculus λ_c [Moggi, 1989]. The application of λ_c as

a calculus of proofs for PLL has been investigated by Benton *et al.* [Benton et al., 1993] (there the logic is called CL).
(3) The third motivation for $\bigcirc$ is the possibility of a timing analysis of combinational circuits. In an equivalent presentation of PLL we can replace $\bigcirc F$ by the axiom

$$\bigcirc S : (\bigcirc M \wedge \bigcirc N) \supset \bigcirc(M \wedge N)$$

and the additional inference rule "from $M \supset N$ infer $\bigcirc M \supset \bigcirc N$". One may now establish a direct correspondence between the axioms used in verifying the functional behaviour of a combinational circuit and the computation of a data-dependent timing constraint: $\bigcirc R$ 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 $(\mathbf{Nat}, 0, +, max)$ we can extract verification-driven, and thus data-dependent, timing information. This is essentially an interpretation, in the sense of (2), in a concrete λ_c calculus.
The previous remarks point out that however strange $\bigcirc$ may appear as a modality of logic it is a rather natural object well-known from other mathematical contexts. While in the shape of strong monads $\bigcirc$ already has proven a very useful tool in the semantics of functional programming languages it is relatively unexplored qua logic. This work takes a logical approach and provides an independent motivation of $\bigcirc$ from hardware verification. Based on this concrete interpretation the analysis given in this paper heads off in new directions.

3 The Logic

The formulas of PLL are generated by the grammar

$$\begin{array}{rcl} M & ::= & A \mid \mathit{true} \mid \mathit{false} \mid M \wedge M \mid \\ & & M \vee M \mid M \supset M \mid \neg M \mid \bigcirc M \end{array}$$

where A ranges over a countably infinite set of propositional constants $\mathrm{pcs} = \{p_0, p_1, \ldots\}$. We will sometimes also use $\equiv$ to abbreviate bi-implication.
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 IPC, plus the axiom schemata $\bigcirc R$, $\bigcirc M$, $\bigcirc F$, and Modus Ponens as the only inference rule. The finitary deduction relation induced by this axiom system is denoted by $\vdash_{\mathrm{PLL}}$.

Lemma 3.1 (Deduction Theorem) $?, M \vdash_{\mathrm{PLL}} N$ *implies* $? \vdash_{\mathrm{PLL}} M \supset N$.

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 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* $? \vdash \Delta$, where $?$ is a finite, possibly empty, list of *hypotheses* and Δ a finite list of *assertions* with length 0 or 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 $\bigcirc$:

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

The complete set of rules is listed in figure 2.

Logical Rules

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

$$\frac{?, M \vdash \Delta \quad ?, N \vdash \Delta}{?, M \vee N \vdash \Delta}\vee L$$

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

$$\frac{?, M \vdash N}{? \vdash M \supset N}\supset R \qquad \frac{? \vdash M \quad ?, N \vdash \Delta}{?, M \supset N \vdash \Delta}\supset L$$

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

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

Structural Rules

$$\frac{}{M \vdash M}\,id \qquad \frac{? \vdash M \quad ?, M \vdash \Delta}{? \vdash \Delta}\,cut$$

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

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

Figure 2: Gentzen Rules for PLL.

Theorem 3.2 *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 one can simulate both the sequent turnstile and the rule bar by implication: A rule

$$\frac{?_0 \vdash \Delta_0 \qquad \cdots \qquad ?_n \vdash \Delta_n}{? \vdash \Delta}$$

is derivable *iff*

$$\vdash_{\mathrm{PLL}} ((\bigwedge ?_0 \supset \bigvee \Delta_0) \wedge \cdots \wedge (\bigwedge ?_n \supset \bigvee \Delta_n)) \supset (\bigwedge ? \supset \bigvee \Delta),$$

where $\bigwedge ?$ and $\bigvee \Delta$ abbreviate finite conjunction and disjunction of the formulas in $?$ and Δ, respectively. For the degenerate cases one takes *true* in the former and *false* in the latter case. ∎

Theorem 3.3 (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 $? \vdash M$ then $?' \vdash M'$. ∎

Another way of translating 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 result that the translation $\bigcirc M \equiv C \supset M$ preserves provability; for the first take $C \equiv$ *true* and for the second take $C \equiv$ *false*. From the latter translation we may conclude, for instance, that $\neg \bigcirc$*false* is not a theorem of PLL. This ensures that PLL is not a trivial 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. Note also that both $\neg \Diamond$ *false* and $\neg \Box$ *false* are theorems of standard modal logics with reflexive accessibility such as S4.

Theorem 3.4 (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 $\vdash_{\mathrm{PLL}} (M \equiv N) \supset (\bigcirc M \equiv \bigcirc N)$ may easily be derived using axiom $\bigcirc F$. ∎

Theorem 3.5 (Cut Elimination) *If $\vdash \Delta$ is derivable, then it is derivable without the cut rule.*

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

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

Figure 3: Additional Primitive Cut Reduction Step

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 3. ∎

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

Lemma 3.6

(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* $? \vdash \Delta$ *is derivable, then there exists a derivation which involves only sub-formulas of* $?$ *and* Δ.

From the sub-formula property (iii) we get the decidability of PLL.

Theorem 3.7 (Decidability) PLL *is decidable.*

We have seen that PLL combines a number of properties (in particular deduction theorem and the interpretation $\bigcirc M = true$) 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 semantical sense. In the next section we show that $\bigcirc$ indeed can be given a proper and nontrivial semantics in terms of Kripke models.

4 Kripke 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 $\supset$.

Here we identify a natural class of Kripke models for which PLL is sound and complete. The models are two-frame Kripke models with a single frame relation and fallible worlds.

Definition 4.1 (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* aR_ib*, then* $a \in F$ *implies* $b \in F$*, and* $a \in V(A)$ *implies* $b \in V(A)$*,*
- V *is full on* F*, i.e.* $F \subseteq V(A)$*.*

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

Definition 4.2 (Validity) *Let* $\mathcal{C} = (W, R_m, R_i, V, F)$ *be a constraint model for* PLL*. Given a formula* M *and* $c \in W$*,* M *is* valid *at* c *in* $\mathcal{C}$*, written* $\mathcal{C}, c \models M$ *iff*

- M *is a propositional constant* A *and* $c \in V(A)$*;*
- M *is* $N \wedge K$ *and both* $\mathcal{C}, c \models N$ *and* $\mathcal{C}, c \models K$*;*
- M *is* $N \vee K$ *and* $\mathcal{C}, c \models N$ *or* $\mathcal{C}, c \models K$*;*
- M *is true; or* M *is false and* $c \in F$*;*
- M *is* $N \supset K$ *and for all* $a \in W$ *such that* cR_ia*,* $\mathcal{C}, a \models N$ *implies* $\mathcal{C}, a \models K$*;*
- M *is of form* $\bigcirc N$ *and for all* $b \in W$*,* cR_ib*, there exists* $a \in W$ *with* bR_ma *such that* $\mathcal{C}, a \models N$*.*

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

Validity behaves as in ordinary intuitionistic logic, *viz.* it is hereditary w.r.t. the accessibility relations. Formally, If $c \models M$ and cR_ib, then $b \models M$. Since R_m is a subrelation of R_i, validity is hereditary w.r.t. R_m too. Worlds w, v with wR_iv and vR_iw validate the same formulas and can thus be identified. Hence, it is no restriction to assume that the relation R_i is a proper ordering, *i.e.* antisymmetric.
Some remarks concerning our definition of validity are in order. First, one notes that fallible worlds validate all formulas and that $\neg\bigcirc \mathit{false}$ is not valid in general. Second, the

clause for validity of $\bigcirc N$ is a $\forall\exists$ statement. This endows $\bigcirc$ with properties of both possibility and of necessity. A direct consequence is 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]. Another consequence is that this semantics of $\bigcirc$ does not validate the scheme $\bigcirc(M \vee N) \supset \bigcirc M \vee \bigcirc N$. 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

$$w \models \Box M \quad \mathit{iff} \quad \forall w', v'.\ wR_i w' \ \&\ w'R_m v' \Rightarrow v' \models M$$

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

Theorem 4.3 (Soundness) *If* $\vdash_{\mathrm{PLL}} M$ *then* $\models M$.

Proof: We lift the notion of validity to sequents in the following way: A sequent $? \vdash K$ is *valid in* model $\mathcal{C}$ if for all c, whenever all hypotheses $M \in ?$ are valid at c in $\mathcal{C}$, then the assertion K is valid at c in $\mathcal{C}$; a sequent $? \vdash$ is valid in $\mathcal{C}$ if the only worlds c under which all hypotheses $M \in ?$ are valid in $\mathcal{C}$ are fallible worlds.
One then shows by induction on derivations that if $? \vdash \Delta$ is derivable then $? \vdash \Delta$ is valid in all models. ∎

We now proceed to prove completeness of PLL w.r.t. Kripke constraint models. 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

$$(?, \Delta, \Theta)$$

of sets of formulas, called *theories*, subject to an abstract consistency condition which reflects the semantical rôle of its components (*cf.* [Fitting, 1983]).
The model will be set up so that at a world $w = (?, \Delta, \Theta)$ the formulas in $?$ are validated at w, the formulas in Δ are falsified at w, and the formulas in Θ are falsified at every world R_m reachable from w. The sets Θ 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 $?$ or Δ. We need to keep track of these separately.
Another special feature of the proof is the notion of consistency. A theory $(?, \Delta, \Theta)$ is *consistent* if for every choice of formulas $N_1, \ldots, N_n \in \Delta$, and $K_1, \ldots, K_k \in \Theta$, such that $n + k \geq 1$, it is *not* the case that

$$? \quad \vdash_{\mathrm{PLL}} \quad N_1 \vee \cdots \vee N_m \ \vee\ \bigcirc(K_1 \vee \cdots \vee K_k)$$

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

$(?, \emptyset, \emptyset)$, for any choice of $?$, 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 $(\perp, \emptyset, \emptyset)$, where $\perp$ denotes the set of all formulas is maximally consistent. Observe that if $(?, \Delta, \Theta)$ is maximally consistent, then *false* $\in ?$ *iff* $\Delta = \Theta = \emptyset$.

Lemma 4.4

- *Every consistent theory has a maximally consistent extension.*
- *If* $(?, \Delta, \Theta)$ *is a maximally consistent theory then the following properties hold:*

  (i) $?$ *is deductively closed*

  (ii) *If* $M \vee N \in ?$ *then* $M \in ?$ *or* $N \in ?$

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

  (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) $M \in ?$ *iff* $M \notin \Delta$

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

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

and by building up a hierarchy of consistent theories

$$(?_0, \Delta_0, \Theta_0) \subseteq (?_1, \Delta_1, \Theta_1) \subseteq \cdots \subseteq (?_n, \Delta_n, \Theta_n) \subseteq (?_{n+1}, \Delta_{n+1}, \Theta_{n+1}) \subseteq \cdots$$

starting with $(?_0, \Delta_0, \Theta_0) = (?, \Delta, \Theta)$ and such that $(?_{n+1}, \Delta_{n+1}, \Theta_{n+1}) = (?_n \cup \{B_n\}, \Delta_n, \Theta_n)$ if it is consistent, otherwise $(?_{n+1}, \Delta_{n+1}, \Theta_{n+1}) = (?_n, \Delta_n \cup \{B_n\}, \Theta_n \cup \{B_n\})$ if it is consistent, otherwise $(?_{n+1}, \Delta_{n+1}, \Theta_{n+1}) = (?_n, \Delta_n \cup \{B_n\}, \Theta_n)$. Then,

$$(?^*, \Delta^*, \Theta^*) \stackrel{df}{=} (\bigcup_{n\in\omega} ?_n, \bigcup_{n\in\omega} \Delta_n, \bigcup_{n\in\omega} \Theta).$$

$(?^*, \Delta^*, \Theta^*)$ is a maximally consistent theory. Note, if $? \vdash$ *false*, then by consistency of $(?, \Delta, \Theta)$ we must have $\Delta = \Theta = \emptyset$, in which case the above construction will produce the maximally consistent extension $(\perp, \emptyset, \emptyset)$.
The second part of the lemma is not hard to verify. It uses the properties of the deduction relation $\vdash_{\mathrm{PLL}}$. ∎

We can now proceed to define a generic Kripke constraint model

$$\mathcal{C}^* = (C^*, R^*_m, R^*_i, V^*, F^*)$$

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

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

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

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

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

$$\begin{array}{rcl} V^*(A) & \stackrel{df}{\equiv} & \{\, (?, \Delta, \Theta) \mid A \in ?\, \} \\ F^* & \stackrel{df}{\equiv} & \{(\bot, \emptyset, \emptyset)\}. \end{array}$$

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

- *$M \in ?$ 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 4.4.
It will be convenient to express the consistency condition for theories $(?, \Delta, \Theta)$ in more concise but less precise form as

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

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

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

in PLL(from axiom schemes $\bigcirc\bigcirc A \supset \bigcirc A$ and $(A \supset B) \supset (\bigcirc A \supset \bigcirc B)$) we conclude that $?_1, \bigcirc N \vdash_{\mathrm{PLL}} \bigcirc \bigvee \Theta_1$. But since $\bigcirc N \in ? \subseteq ?_1$ this contradicts the consistency of $\mathcal{T}_1$. By lemma 4.4 we can now find a maximally consistent extension $\mathcal{T}' = (?', \Delta', \Theta')$ of

$(?_1 \cup \{N\}, \emptyset, \Theta_1)$. 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 $(?, \emptyset, \{N\})$, which must be consistent for otherwise $? \vdash_{\mathrm{PLL}} \bigcirc N$, which contradicts consistency of $\mathcal{T}$. Now take a maximally consistent extension $\mathcal{T}' = (?', \Delta', \Theta')$ of $(?, \emptyset, \{N\})$. We claim that for all $\mathcal{T}_1$, $\mathcal{T}' R_m^* \mathcal{T}_1$, $\mathcal{T}_1 \not\models N$. Let $\mathcal{T}_1 = (?_1, \Delta_1, \Theta_1)$. 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 $N \supset K \in ?$ and $\mathcal{T}_1 = (?_1, \Delta_1, \Theta_1)$ such that $\mathcal{T} R_i^* \mathcal{T}_1$. By definition of R_i^*, $N \supset K \in ? \subseteq ?_1$. By lemma 4.4 (iii) we have $N \in \Delta_1$ or $K \in ?_1$. 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 $(? \cup \{N\}, \{K\}, \emptyset)$. It must be consistent since otherwise $?, N \vdash_{\mathrm{PLL}} K$, whence by the deduction theorem $? \vdash_{\mathrm{PLL}} N \supset K$ which contradicts consistency of $\mathcal{T}$. Now take a maximally consistent extension $\mathcal{T}' = (?', \Delta', \Theta')$ of $(? \cup \{N\}, \{K\}, \emptyset)$. We have $\mathcal{T} R_i^* \mathcal{T}'$, $N \in ?'$, and $K \in \Delta'$. By induction hypothesis, $\mathcal{T}' \models N$ and $\mathcal{T}' \not\models K$. But this means nothing but $\mathcal{T} \not\models N \supset K$.

• 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 $\mathcal{T}_1 = (?_1, \Delta_1, \Theta_1)$ such that $\mathcal{T} R_m^* \mathcal{T}_1$. By definition of R_m^*, and the properties of maximally consistent theories, lemma 4.4 (vi), $M \in \Theta \subset \Theta_1 \subset \Delta_1$. Thus, we can appeal to the proofs above to conclude $\mathcal{T}_1 \not\models M$. Notice, this recursing to the Δ cases does not introduce circularity in the proof because any subsequent reduction to the Θ case (namely $\bigcirc N \in \Theta$) strictly reduces the complexity of the formula M. ∎

Theorem 4.6 (Completeness) *If* $\models M$ *then* $\vdash_{\mathrm{PLL}} M$.

Proof: Suppose $\nvdash_{\mathrm{PLL}} M$. Then $(\emptyset, \{M\}, \emptyset)$ is consistent. By Lemma 4.4 there is a maximally consistent extension $\mathcal{T}$, and by Lemma 4.5 $\mathcal{T} \not\models M$ in the constraint Kripke model $\mathcal{C}^*$. ∎

Two examples of counter models, one falsifying $\neg \bigcirc \mathit{false}$ and the other falsifying $\bigcirc(A \vee B) \supset (\bigcirc A \vee \bigcirc B)$, are shown in figure 4, where the solid arrows represent R_i^* and the dashed lines R_m^*. Both counter models (which may be further simplified by dropping the initial R_i^* steps) may be seen to be constructed from $\mathcal{C}^*$.

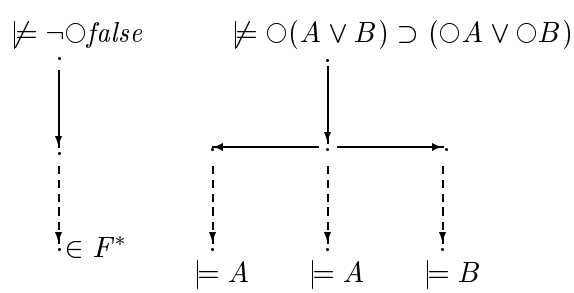

Figure 4: Two Counter Models

As we shall see in section 5 there are special cases of concrete constraint models which validate 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 4.7

- 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* aR_mb *and* aR_ic*, then there exists* d *such that* bR_id *and* cR_md.

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,

$$w \models \bigcirc M \quad \textit{iff} \quad \exists u.\ wR_mu \ \&\ u \models M.$$

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 4.6).
• 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 $\mathcal{T} = (?, \Delta, \Theta)$ so that $\neg\bigcirc \mathit{false} \in ?$ and $M \in \Delta$. We know that $\mathcal{T} \not\models M$ 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 $\neg\bigcirc \mathit{false} \in ?$ and $(?, \Delta, \Theta)R_m^*(?', \Delta', \Theta')$ implies $\mathit{false} \notin ?'$. For assume otherwise, then $(?', \Delta', \Theta') = (\bot, \emptyset, \emptyset)$ whence by definition of R_m^* we have $\Theta = \emptyset$. Since $(?, \Delta, \Theta)$ is maximally consistent this implies that $? \vdash_{\mathrm{PLL}} \bigvee \Delta \ \vee\ \bigcirc \mathit{false}$ since the proper extension $(?, \Delta, \{\mathit{false}\})$ cannot be consistent. Now we use the assumption that $\neg\bigcirc \mathit{false} \in ?$ (and the properties of deduction in the logic) to conclude that $? \vdash_{\mathrm{PLL}} \bigvee \Delta$ which contradicts the consistency of $(?, \Delta, \Theta)$. Thus, from the assumption that M is not a theorem of PLL $+ \neg\bigcirc \mathit{false}$ we can construct a model without fallible nodes in which M is falsified. This proves the completeness statement for PLL $+ \neg\bigcirc \mathit{false}$.
• Suppose that M is not derivable in PLL $+ \bigcirc(X \vee Y) \supset (\bigcirc X \vee \bigcirc Y)$. Again we consider the canonical counter model generated by a maximally consistent theory $\mathcal{T} = (?, \Delta, \Theta)$ such that $M \in \Delta$ and such that $?$ 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 $(?', \Delta', \Theta')$ with $? \subseteq ?'$, R_i^* and R_m^* are mutually confluent. The first step is to observe that both Δ' and Θ' are uniquely determined by $?'$ as follows:

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

where $\complement(?')$ is the complement of $?'$ and $\delta\Delta' = \{\, N \mid \bigcirc N \in \Delta' \,\}$. The first part was proven already in Lemma 4.4. The second part is a consequence of the extra axioms in

$?'$ and seen as follows. Let $K \in \delta\Delta'$, *i.e.* $\bigcirc K \in \Delta'$, but $K \notin \Theta'$. Then, since $(?', \Delta', \Theta')$ is maximally consistent, we get $?' \vdash_{\mathrm{PLL}} \bigvee \Delta' \ \vee \ \bigcirc(\bigvee \Theta' \vee K)$. Now, by assumption, $?'$ contains the axiom $\bigcirc(\bigvee \Theta' \vee K) \supset \bigcirc \bigvee \Theta' \vee \bigcirc K$, whence from both facts together we get $?' \vdash_{\mathrm{PLL}} \bigvee \Delta' \ \vee \ \bigcirc K \ \vee \ \bigcirc \bigvee \Theta'$ which contradicts consistency of $(?', \Delta', \Theta')$. 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 $(?', \Delta', \Theta') R^*_m (?'', \Delta'', \Theta'')$ is equivalent to the condition $?' \subseteq ?'' \subseteq \delta ?'$. Assume $?' \subseteq ?'' \subseteq \delta ?'$. Then $\Theta' = \delta\Delta' = \delta(\mathsf{C}(?')) = \delta\delta(\mathsf{C}(?')) = \delta(\mathsf{C}(\delta ?')) \subseteq \delta(\mathsf{C}(?'')) = \delta\Delta'' = \Theta''$, where the equation $\delta\delta X = \delta X$ holds generally for all deductively closed sets X, by virtue of the rule $\bigcirc M$. Thus, $(?', \Delta', \Theta') R^*_m (?'', \Delta'', \Theta'')$. Vice versa, if $(?', \Delta', \Theta') R^*_m (?'', \Delta'', \Theta'')$ we have $?' \subseteq ?''$ and $?'' \subseteq \mathsf{C}(\Theta'') \subseteq \mathsf{C}(\Theta') = \mathsf{C}(\delta\Delta') = \delta(\mathsf{C}(\Delta')) = \delta ?'$.

Now we can prove mutual confluence. Suppose we are given three maximally consistent theories $(?', \Delta', \Theta')$, $(?_1, \Delta_1, \Theta_1)$, and $(?_2, \Delta_2, \Theta_2)$ such that $? \subseteq ?' \cap ?_1 \cap ?_2$ and such that

$$(?', \Delta', \Theta') R^*_i (?_1, \Delta_1, \Theta_1) \quad \text{and} \quad (?', \Delta', \Theta') R^*_m (?_2, \Delta_2, \Theta_2).$$

We need to find a $\mathcal{T}'$ such that $(?_1, \Delta_1, \Theta_1) R^*_m \mathcal{T}'$ and $(?_2, \Delta_2, \Theta_2) R^*_i \mathcal{T}'$. We claim that any maximally consistent extension $\mathcal{T}'$ of the theory $(\delta ?_1, \emptyset, \Theta_1)$ will do. For such a $\mathcal{T}'$ to exist $(\delta ?_1, \emptyset, \Theta_1)$ must be consistent. Suppose it is not, then $\delta ?_1 \vdash_{\mathrm{PLL}} \bigcirc \bigvee \Theta_1$ which, by the properties of the logic, implies that $?_1 \vdash_{\mathrm{PLL}} \bigcirc \bigvee \Theta_1$ contradicting consistency of $(?_1, \Delta_1, \Theta_1)$. Thus, let $\mathcal{T}' = (?_3, \Delta_3, \Theta_3)$ be a maximally consistent extension of $(\delta ?_1, \emptyset, \Theta_1)$. One verifies $?_1 \subseteq \delta ?_1 \subseteq ?_3$ and $\Theta_1 \subseteq \Theta_3$, hence $(?_1, \Delta_1, \Theta_1) R^*_m \mathcal{T}'$ as desired. Further, $?_2 \subseteq \delta ?'$ by the second observation above and thus $?_2 \subseteq \delta ?' \subseteq \delta ?_1 \subseteq ?_3$. Thus, $(?_2, \Delta_2, \Theta_2) R^*_i \mathcal{T}'$ 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.

∎

5 Three General Constraint Models

In this paper we give two variants of concrete models for PLL. The first class of models 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 $\mathcal{C}[M] \equiv C \supset M$ where C is an arbitrary but 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 γ is taken from a predefined set of distinguished propositions representing constraints. Other possible contexts are $\mathcal{C}[M] \equiv C \vee M$ or $\mathcal{C}[M] \equiv (M \supset C) \supset C$.

Let PLL^C be the theory

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

and $\mathcal{M}^C$ the class of (antisymmetric) Kripke constraint models validating PLL^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*

$\models \neg\neg C$ and the latter whenever $[\![C]\!] = \{\, w \mid w \models C \,\}$ is a principal ideal, *i.e.* for some z, $[\![C]\!] = \{\, w \mid zR_i w \,\}$.

Lemma 5.1 *$\mathcal{M}^C$ is characterized by the frame conditions (i) $\forall w.\ \exists u.\ wR_m u\ \&\ u \models C$, and (ii) $\forall w, u.\ (w \models C\ \&\ wR_m u)\ \Rightarrow\ w = u$.*

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 conditions 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 is already validating C then w is a terminal w.r.t. 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). Note that the restriction to antisymmetric constraint Kripke models is not a severe one, as every constraint Kripke model is (elementarily) equivalent to an antisymmetric one. ∎

With the semantical characterization at hand we can now try to construct concrete models for PLL^C. Let $\mathcal{M} = (W, \sqsubseteq, V)$ 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,
- $V^C(A) = V(A) \cup \{\bot\}$,
- $F^C = \{\bot\}$,
- $wR_i^C v$ *iff* $w \sqsubseteq v$ or $v = \bot$,
- $wR_m^C v$ *iff* $\mathcal{M}, w \not\models C$ and $v = \bot$, or $w = v$.

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 lemma 5.1. Thus, $\mathcal{M}^C$ is a model of PLL^C. Note that the $\mathcal{M}^C$ actually are a rather restricted class of models satisfying the stronger property that if $w \neq v$, then $wR_m v$ iff $\mathcal{M}^C, w \not\models C$ and $v \in F$.

Lemma 5.2 (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 lemma 5.1.*

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 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. ∎

The constraint interpretation $\bigcirc M \equiv C \supset M$ involves a 'positive' constraint C: "*if C then M*". There is also the 'negative' version "*if not C then M*", which, of course, intuitionistically is not the same as "*if* $\neg C$ *then M*". This negative constraint can be formalized by the axiom $\bigcirc M \equiv (C \vee M)$. Let

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

and $\mathcal{M}_C$ the class of (antisymmetric) Kripke constraint models validating PLL_C. Then we get the following results:

Lemma 5.3

- *$\mathcal{M}_C$ is characterized by the frame conditions (i) $\forall w.\ w \models C \ \Rightarrow\ \exists u.\, wR_m u \ \ \&\ \ u \in F$, and (ii) $\forall w, u.\ (w \not\models C \ \ \&\ \ wR_m u) \ \Rightarrow\ w = u$, and*
- 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 suffient 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 w.r.t. 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 pcs not occurring in C).
The argument for completeness proceeds along similar lines as for 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 $w \neq v$, $wR^C_m v$ iff $\mathcal{M}, w \models C$ and $v = \perp$. This model is so that it satisfies 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 lemma 5.2, 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 PLL_C then $\bigcirc M \equiv M$ becomes derivable.

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, this theory PLL^* contains the axiom $\neg\bigcirc \mathit{false}$ but not $\bigcirc(M \vee N) \supset (\bigcirc M \vee \bigcirc N)$.

Lemma 5.4

- 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 $\mathcal{M} = (W, \sqsubseteq, V)$ we consider the constraint model $\mathcal{M}^*$ obtained from $\mathcal{M}$ by taking $R_m = R_i = \sqsubseteq$ 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):

Lemma 5.5 *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. ∎

Lemma 5.5 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, PLL* is a constraint interpretation of $\bigcirc$ of the Currian form PLL^C, where the constraint C is of second-order nature.

6 Combinational Circuits

The second type of models to be investigated are still more concrete. 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. Concretely, the circuit models are set up such that for a propositional constant A

$$\left.\begin{array}{r} A \\ \neg A \\ \bigcirc A \\ \bigcirc\neg A \end{array}\right\} \quad \text{means} \quad \left\{\begin{array}{l} \text{'}A \text{ is stable at 1'} \\ \text{'}A \text{ is stable at 0'} \\ \text{'}A \text{ is going to stabilize to 1'} \\ \text{'}A \text{ is going to stabilize to 0.'} \end{array}\right.$$

This allows us to retain the ideal 'static' interpretation of truth values while safely keeping track of the offset to the real signals caused by propagation delays. For instance, the example circuit mentioned in the introductory section (1) can now be specified by

$$(B \vee \neg B) \ \supset \ (\neg A \supset \bigcirc \neg C).$$

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* voltage. Signals are 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 $\mathcal{I}(\mathcal{A}) : \mathbb{N} \to \mathbb{B}$.
Given a timing diagram $\mathcal{I}$ we will construct a constraint Kripke model $\mathcal{MI}$, so that the induced semantics for PLL complies with the informal reading of formulas given above. The worlds of $\mathcal{MI}$ are closed-open time intervals obtained from breaking the signal waveform $\mathcal{I}$ into pieces. We adopt Leibniz' 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 $\mathcal{I}(\mathcal{A})(\sqcup) \neq \mathcal{I}(\mathcal{A})(\sqcup + \infty)$. 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 5. It depicts two signals $\mathcal{I}(\mathcal{A})$ and $\mathcal{I}(\mathcal{B})$ with their signal changes at times $t_0 = 0, t_1, \ldots, t_7$. The Leibniz intervals, then, are $[t_i, t_j)$, and $[t_i, \infty)$, $i, j = 0, \ldots 7$, $i \leq j$.

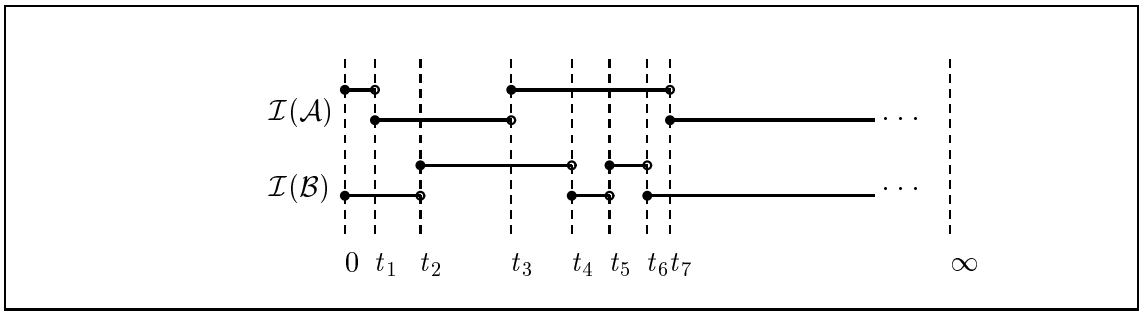

Figure 5: An Example Interpretation.

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

$$\mathcal{MI} \ \stackrel{df}{=} \ (W(\mathcal{I}), \mathcal{R}_{\rangle}(\mathcal{I}), \mathcal{R}_{\Updownarrow}(\mathcal{I}), \mathcal{V}(\mathcal{I}), \mathcal{F}(\mathcal{I}))$$

is constructed as follows:

- $W(\mathcal{I})$ is the set of Leibniz intervals for $\mathcal{I}$.
- $[s, t) R_i [s', t')$ if $[s', t')$ is a subinterval of $[s, t)$,
- $[s, t) R_m [s', t')$ if $[s', t')$ is a final subinterval of $[s, t)$, *i.e.* $t = t'$ and $s \leq s'$.

- $[s,t) \in V(\mathcal{I})(\mathcal{A})$ if $\mathcal{I}(\mathcal{A})$ is constant 1 throughout $[s,t)$, *i.e.* $\forall x.\ s \leq x < t$, $\mathcal{I}(\mathcal{A})(\S) = \infty$.

- $F(\mathcal{I})$ 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 $\bigcirc(M \vee N) \supset (\bigcirc M \vee \bigcirc N)$.

Lemma 6.1 *Let A be an atomic proposition.*

- $\models A$ *iff* $\mathcal{I}(\mathcal{A})$ *is constant* 1.

- $\models \neg A$ *iff* $\mathcal{I}(\mathcal{A})$ *is constant* 0.

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

- $\models \bigcirc\neg A$ *iff* $\mathcal{I}(\mathcal{A})$ *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 delay behaviour: $\models A \vee \neg A$ iff $\mathcal{I}(\mathcal{A})$ 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 carries inconsistent stability information. It represents an intermediate phase of the circuit's execution with a potential for glitches.
With this in mind we may unroll the semantics of some formulas to find that we can express various types of stabilization behaviour:

Lemma 6.2 *Let A, B be propositional constants.*

- $\models \bigcirc(A \vee \neg A)$ *iff* $\mathcal{I}(\mathcal{A})$ *stabilizes eventually.*

- $\models \neg\bigcirc$*false iff all signals are constant.*

- $\models (A \vee \neg A) \supset \bigcirc$*false iff* $\mathcal{I}(\mathcal{A})$ *oscillates indefinitely.*

- $\models \bigcirc A \supset \neg B$ *iff whenever* B *switches to* 1 *all signals have become stable for good and* A *rests at* 0.

Proof: Easy. ∎

It can be seen that if the circuit stabilizes completely at some time s, then both $[s, \infty) \models A \vee \neg A$ and $[s, \infty) \models \bigcirc A \equiv A$ for all A. Thus, after stabilization, the theory reduces to ordinary classical Boolean algebra, which is what we expected.
Aiming at a concrete application we might specify the falling output transition of an invertor by the formula $A \supset \bigcirc\neg B$, "if $\mathcal{I}(\mathcal{A})$ becomes stable 1 for good then eventually $\mathcal{I}(\mathcal{B})$ 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 nothing but that $\mathcal{I}(\mathcal{A})$ oscillates. In contrast, the classical theory of the invertor ring would lead 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. The expressiveness, which ranges from a set of states with arbitrary transitions to no transitions at all, will be investigated in the next section.

Let us call the theory induced by the circuit models $\mathcal{MI}$, 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 present state. The following axiom schemes are valid in (but not complete for) Circuit-PLL:

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

The first axiom scheme has been noted before, it stems from the confluence of both accessibility relations in the circuit models. The second axiom scheme we have encountered implicitly in the semantical 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 boolean algebra. Thus, although the circuit models $\mathcal{MI}$ involve 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, is characteristic for 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.

7 Expressibility of the ○-free fragment of Circuit-PLL

We have seen that with the modality ○ we can specify oscillation and termination behaviour in Circuit-PLL. In this section we present some results which show that already the ○-free fragment can specify nontrivial dynamic behaviour. We also give an upper bound on expressiveness and as a corollary obtain the decidability of ○-free Circuit-PLL.

At this point it deserves mention that ○-free Circuit-PLL, *i.e.* the intuitionistic base of Circuit-PLL, coincides with the stable form of Maksimova's intermediate logic $L\Pi$ [Maksimova, 1986], more precisely

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

This follows from the fact that both theories are generated by effectively the same class of Kripke models. Thus, the results of this section are also results about stable $L\Pi$. In particular from decidability of ○-free Circuit-PLL (corollary 7.4 below) the decidability of stable $L\Pi$ can be inferred. This connection, however, will not be pursued further in this paper.

In the ○-free fragment we can restrict ourselves to finite timing diagrams, *i.e.* those with a finite number of signals which all eventually stabilize: A ○-free formula is valid iff it is valid in all finite timing diagrams. We can 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 5 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 ○-free fragment is unaffected by the presence of empty intervals, we may as well restrict ourselves to non-empty sequences. In order to simplify the analysis further we will restrict ourselves to a finite number of propositional constants $p_0, \ldots, p_{pcs-1}$, and henceforth all formulas are assumed to be ○-free formulas built from these atoms.
With these observations we may adopt the following more compact interpretation of the ○-free fragment of Circuit-PLL: Let $\Sigma = \mathbb{B}^{pcs}$ be the set of bit vectors of length *pcs*, called *states*. Formulas (○-free with pcs in $p_0, \ldots, p_{pcs-1}$) are interpreted on non-empty sequences of states without repetitions (*i.e.* no 'stuttering'), called *traces*. The set of traces is denoted by Σ^+, and $\sqsubseteq$ will denote the sub-trace relationship, *i.e.* $w \sqsubseteq v$ if there exist v_1, v_2, possibly empty, such that $v = v_1 w v_2$. Every formula now is assigned a subset $[\![M]\!]$

of traces in the following way:

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

Lemma 7.1 (Soundness of $[\![_]\!]$) *Let I be a finite timing diagram. Then $I \in [\![M]\!]$ iff $I \models M$.*

Proof: A routine induction on the structure of M. ∎

The lemma provides an equivalent interpretation in terms of traces in which the expressibility of the $\bigcirc$-free fragment of Circuit-PLL may be conveniently studied. For $w \in \Sigma^+$ we will write $w \models M$ rather than $w \in [\![M]\!]$.

7.1 A Lower bound on expressibility

First note that conjunctions of literals specify states, so that, for example, the conjunct $N := p_0 \wedge \neg p_1 \wedge p_2$ means "p_0 and p_2 are stable at 1, p_1 is stable at 0, *i.e.* $[\![N]\!] = \{101\}$. This means that for any $s = b_0 \cdots b_{pcs-1} \in \Sigma$ we can find a formula $M(s)$ such that $[\![M(s)]\!] = \{s\}$, by setting

$$M(s) = \bigwedge_{0 \leq i < pcs} \neg^{(1-b_i)} p_i,$$

so that, with N as above, we have $N = M(101)$. A disjunction D of such states (a classical disjunctive normal form) then expresses that the system must be in exactly one of a finite number of states, with *no* signal changes allowed. We might call D a *static state invariant*. In contrast, the formula $\neg\neg D$ is a *dynamic state invariant*. It says "at any single point in time, the system must be in one of the states in D"; here *any* signal changes are permitted provided they do not take the system outside D. The formulas D and $\neg\neg D$ are two extreme cases of a general *transition invariant* (ti) given by a pair (S, T) where $S \subseteq \Sigma$ is a set of states and $T \subseteq S \times S$ an irreflexive, symmetric relation on S. A ti (S, T) can be viewed as an undirected graph, whose vertices are (uniquely labelled by) members of Σ, and whose paths specify a subset $P(S, T)$ of traces.

Lemma 7.2 *For every ti G there exists a formula M such that $[\![M]\!] = P(G)$.*

Proof: Let the ti $G = (S, T)$ be given. Then the formula

$$\neg\neg \bigvee_{s \in S} M(s) \quad \wedge \quad \bigwedge_{(s,t) \notin T} (\neg\neg(M(s) \vee M(t)) \supset (M(s) \vee M(t)))$$

does the job. The first conjunct specifies the complete graph over the carrier set S of G, from which the second conjunct selectively removes those edges (s,t) that do not occur in T. ∎

Example *For illustration, figure 6 displays three examples of simple transition invariants over* $\Sigma = \mathbb{B}^2$ *given by the formulas* $D := (\neg p_0 \wedge \neg p_1) \vee (p_0 \wedge \neg p_1) \vee (\neg p_0 \wedge p_1)$, $\neg\neg D$ *and* $p_0 \supset (p_1 \vee \neg p_1)$.

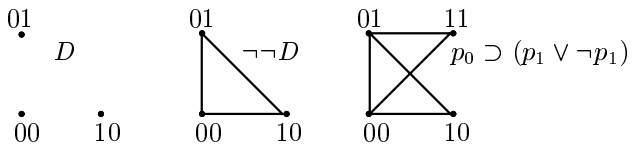

Figure 6: Three Transition Invariants

To take a more interesting example let us consider a binary 3*-bit up/down counter with outputs modelled by the pcs* p_0, p_1, p_2*, where* p_0 *is the least significant and* p_2 *the most significant bit. The counter passes through all of the* 8 *possible states but takes only* 8 *of the possible* 28 *(undirected) transitions between these states. The corresponding transition invariant* $G_{\mathrm{CNT}} = (S_{\mathrm{CNT}}, T_{\mathrm{CNT}})$ *is given by* $S_{\mathrm{CNT}} = \mathbb{B}^3$ *and*

$$T_{\mathrm{CNT}} \quad = \quad \{\, (i, i+1), (i+1, i) \mid i = 0, 1, \ldots, 6 \,\} \cup \{(7,0), (0,7)\}.$$

Under the binary encoding of states we can capture the permitted transitions by four conditions on the switching of the counter's signals:

Whenever p_1 *switches* p_0 *must switch too*	*(1)*
Whenever p_2 *switches* p_1 *must switch too*	*(2)*
Whenever p_2 *switches then before or after both* p_1, p_0 *are in the same state*	*(3)*
Whenever p_1, p_0 *switch in the same direction then* p_2 *switches, too.*	*(4)*

The reader is invited to check that these conditions precisely specify T_{CNT} *and further that they can be expressed by the formula*

$$\begin{aligned} \textit{CNT-Spec} \quad = \quad & (p_0 \vee \neg p_0) \supset (p_1 \vee \neg p_1) && (1) \\ \wedge\ & (p_1 \vee \neg p_1) \supset (p_2 \vee \neg p_2) && (2) \\ \wedge\ & \neg(p_0 \equiv p_1) \supset (p_2 \vee \neg p_2) && (3) \\ \wedge\ & (p_2 \vee \neg p_2) \supset \neg(p_0 \equiv p_1) && (4) \end{aligned}$$

∎

Lemma 7.2 shows that in the propositional fragment of Circuit-PLL we can express non-trivial dynamic behaviour. It is evident that this lower bound is not tight. Take the formula $p_0 \vee p_1$, for instance. It states essentially that at any time "at least one of p_0 or p_1 must be 1, and if both are 1 only that bit may switch that has not switched before". This does not correspond to any transition invariant (as defined above) since the behaviour in

state 11 depends on the previous history. Thus, in general, our formulas specify dynamic behaviour with some form of internal memory. In fact, the dynamic behaviour expressible is much richer and includes higher-order transition invariants, as will be seen later in section 8. Yet we cannot expect to express arbitrary memory and some limitations are mentioned in the next section.

7.2 Upper bound on expressibility

An upper bound to the expressibility in the $\bigcirc$-free fragment of Circuit-PLL is given by the regular languages closed under subsequence and insensitive to local reversal, as we now show.
Closure under subsequences is immediate from the intuitionistic nature of our interpretation. To see that, for every M, $[\![M]\!]$ is a regular language we first observe that $[\![\mathit{true}]\!]$ and $[\![\mathit{false}]\!]$ are regular, as well as $[\![p_i]\!]$ where $p_i \in$ pcs. Further, one verifies that by definition of $[\![_]\!]$ all binary connectives can be expressed by binary union, intersection, complement, and concatenation of regular languages. The nontrivial case here is implication for which one shows:

$$[\![M \supset N]\!] \;=\; \{\, w \in \Sigma^+ \mid \forall u \sqsubseteq w.\; u \in [\![M]\!] \Rightarrow u \in [\![N]\!] \,\} \;=\; \complement(\Sigma^+ \cdot \complement(\complement[\![M]\!] \cup [\![N]\!]) \cdot \Sigma^+),$$

where $\complement$ is the complement and $\cdot$ concatenation.

Lemma 7.3 *For all M, $[\![M]\!]$ is a regular language closed under sub-words.*

Corollary 7.4 *The $\bigcirc$-free fragment of Circuit-*PLL *is decidable.*

Proof: To determine whether a $\bigcirc$-free formula M is in Circuit-PLL, construct (an automaton accepting) $[\![M]\!]$. Now $[\![M]\!] = \Sigma^+$ is decidable. ∎

The regular languages (closed under subsequence) are still a much too coarse upper bound on expressiveness. In fact, one can get a sharper upper bound. We first need a definition:

Definition 7.5 *A language L over alphabet Σ is* locally reversible *if for all $u, v, w \in \Sigma^*$ and $a, b \in \Sigma$,*

$$uavbw \in L \Leftrightarrow uavbv^R avbw \in L,$$

where v^R denotes the reverse of v.

Lemma 7.6 *For every formula M, $[\![M]\!]$ is locally reversible.*

The results show that the languages expressible as $[\![M]\!]$ are a rather special type of regular languages. In terms of accepting automata closedness under sub-words intuitively amounts to saying that all states are both initial and terminal, and insensitivity to local reversal means that transitions are undirected. The question as to whether this class of regular languages is also a lower bound on expressibility remains open.

8 Higher-Order Transition Invariants

In this last section we are going to show that a class of formulas in the $\bigcirc$-free fragment of Circuit-PLL corresponds to generalized transition invariants, more precisely higher-order transition invariants. A higher-order transition invariant is a structure specifying a set of permitted higher-order transitions contained in a trace. The invariants introduced in section 7.1 are special cases of order 0 and 1: A state is a 0-order transition and a (dynamic) state invariant is a 0-order transition invariant defining a subset of permitted states; a transition in the sense of section 7.1 is a 1st-order transition defining an undirected transition between states; in general a transition of order $(n+1)$ is an undirected transition between two n-transitions, and an $(n+1)$-order transition invariant specifies a subset of such transitions. The precise definitions follow below.

Definition 8.1 *A (generalized)* transition *is an element of the set* $\mathbb{T} = \bigcup_{n\geq 0} \mathbb{T}^n$*, where*

$$\begin{array}{lcl} \mathbb{T}^0 & = & \Sigma \\ \mathbb{T}^1 & = & \{\, \{t_1, t_2\} \mid t_1, t_2 \in \mathbb{T}^0 \ \&\ t_1 \neq t_2 \,\} \\ \mathbb{T}^{n+2} & = & \{\, \{t_1, t_2\} \mid t_1, t_2 \in \mathbb{T}^{n+1} \ \&\ t_1 \neq t_2 \ \&\ t_1 \cap t_2 \neq \emptyset \,\}. \end{array}$$

The order *of a transition* $t \in \mathbb{T}$ *is the (unique)* $n \geq 0$ *with* $t \in \mathbb{T}^n$*. A transition of order* n *we call an* n-transition*.*

Thus, a 0-transition is simply a state $a \in \Sigma$, a 1st-order or 1-transition $t = \{a, b\}$ is uniquely determined by two distinct states a, b and a 2nd-order or 2-transition $t = \{\{a, b\}, \{b, c\}\}$ is given by three mutually distinct states a, b, c one of which is a distinguished 'pivot' state. Intuitively, a 0-transition is a degenerate case of a transition, the 'non-change' of a given state. A 1-transition $t = \{a, b\}$ represents an undirected change of state between a and b, and a 2-transition $t = \{\{a, b\}, \{b, c\}\}$ represents a change of a change of states, *viz.* a change from a change between a and b to a change between b and c with an intermediate pivot state b. We remark that for orders greater than 2 the description is no longer so simple, as *e.g.* a 3rd-order or 3-transition is of the form $t = \{\{\{a, b\}, \{b, c\}\}, \{\{b, c\}, x\}\}$ where the 1-transition x is one of $\{a, c\}$, $\{c, d\}$, $\{b, d\}$, where all states a, b, c, d are mutually different. Each one of the possibilities for x results in a different type of 3-transition. An example of a 3rd-order transition will be given below in figure 7.

Transitions are equipped with a natural ordering relation $\preceq$, the reflexive and transitive closure of inverse element-ship, *i.e.* $t \in \mathbb{T}$ is an immediate $\preceq$-successor of $s \in \mathbb{T}$ iff $t \in s$. Intuitively, $s \preceq t$ means that transition s contains t as a sub-transition. Clearly, $\preceq$ is antisymmetric, whence $(\mathbb{T}, \preceq)$ is a partial ordering. The 0-transitions $\mathbb{T}^0$ are the leaves in $(\mathbb{T}, \preceq)$ and every t of order $n > 0$ possesses exactly two distinct immediate $\preceq$-successors t_1, t_2 of order $n \perp 1$, and between 2 and n distinct successors of order 0. The ordering $\preceq$ is discrete within the same order, *i.e.* if $s, t \in \mathbb{T}^n$ then $s \preceq t$ implies $s = t$. Another important property of $\preceq$ to mention is that it is Noetherian, *i.e.* every nonempty set has a maximal element. It is also useful to note that $(\mathbb{T}, \preceq)$ is irredundant in the sense that an element is uniquely determined by the set of its proper successors.

To define the notion of a generalized transition invariant we need to make precise when a trace w satisfies a particular higher-order transition t. Clearly, we expect that w satisfies a 0-transition $a \in \Sigma$ just in case $a \sqsubseteq w$, a 1-transition $t = \{a, b\}$ iff $ab \sqsubseteq w$ or $ba \sqsubseteq w$, and a 2-transition $t = \{\{a, b\}, \{b, c\}\}$ iff $abc \sqsubseteq w$ or $cba \sqsubseteq w$. However, in order to deal with transitions of order greater than 2 we introduce a deterministic notion of satisfaction which we call 'firing':

Definition 8.2 *Given a trace $w \in \Sigma^+$ and a transition $t \in T$, we say that w* fires *t if $w \Vdash t$, where $\Vdash$ is the smallest relation closed under the following rules*

$$\frac{a \in \Sigma}{a \Vdash a}\ (F.0) \qquad \frac{au \Vdash t_1 \quad ub \Vdash t_2}{aub \Vdash \{t_1, t_2\}}\ (F.s)$$

$$\frac{au \Vdash t \quad ub \Vdash s}{aub \Vdash t}\ t \preceq s \quad (F.l) \qquad \frac{au \Vdash s \quad ub \Vdash t}{aub \Vdash t}\ t \preceq s \quad (F.r),$$

where $a, b \in \Sigma$ and $u \in \Sigma^*$, and it is understood that the right-hand side of $\Vdash$ in premisses and conclusion must be well-formed transitions.

Rule (F.0) completely defines firing for singleton traces. All traces that are not single states must be of the form aub where $a, b \in \Sigma$ and $u \in \Sigma^*$. These cases are dealt with by rules (F.s), (F.r), and (F.l), which reduce the firing of aub to the firing behaviour of its immediate sub-traces au and ub. According to the rules there are three possibilities for aub to fire a transition t: In (F.s), which is the typical case, $t = \{t_1, t_2\}$ is fired because one of the immediate sub-traces of aub fires t_1 and the other t_2 (there is an implicit symmetry in the application of this rule due to the fact that $\{t_1, t_2\} = \{t_2, t_1\}$). The other two possibilities for aub to fire t are the situations where t is fired by one of its immediate sub-traces already while the other fires a sub-transition of t.
Though on first glance the firing rules may appear hopelessly partial and nondeterministic the relation $\Vdash$ is actually a total function. The following proposition justifies interpreting $w \Vdash t$ as 't is *the* complete firing behaviour of w'. We will denote the unique t such that $w \Vdash t$ by $\tau(w)$.

Proposition 8.3 *For all $w \in \Sigma^+$ there exists a unique $t \in \mathbb{T}$ such that $w \Vdash t$.*

As an illustration of the firing relation figure 7 displays a 3-transition t and a trace w firing t. The example is chosen for $\Sigma = \{0, 1\}^2$ where, for simplicity, we identify Σ with the set of natural numbers $\{0, 1, 2, 3\}$ under binary coding. The trace w is the state sequence 012113, *i.e.*

$$\tau(012113) \quad = \quad \{\{\{0, 1\}, \{1, 2\}\}, \{\{1, 2\}, \{1, 3\}\}\}.$$

A transition invariant describes the set of transitions that may be fired by a trace. One can show that $w' \sqsubseteq w$ implies $\tau(w) \preceq \tau(w')$ so that the firing behaviour of a trace includes the behaviour of all its sub-traces. Vice versa, if we permit a transition t to be fired we must also permit all of its sub-transitions $t \preceq s$ to be fired as well, since $\tau(w) \preceq s$ implies there exits a sub-trace $w' \sqsubseteq w$ with $\tau(w') = s$. This motivates the following definition:

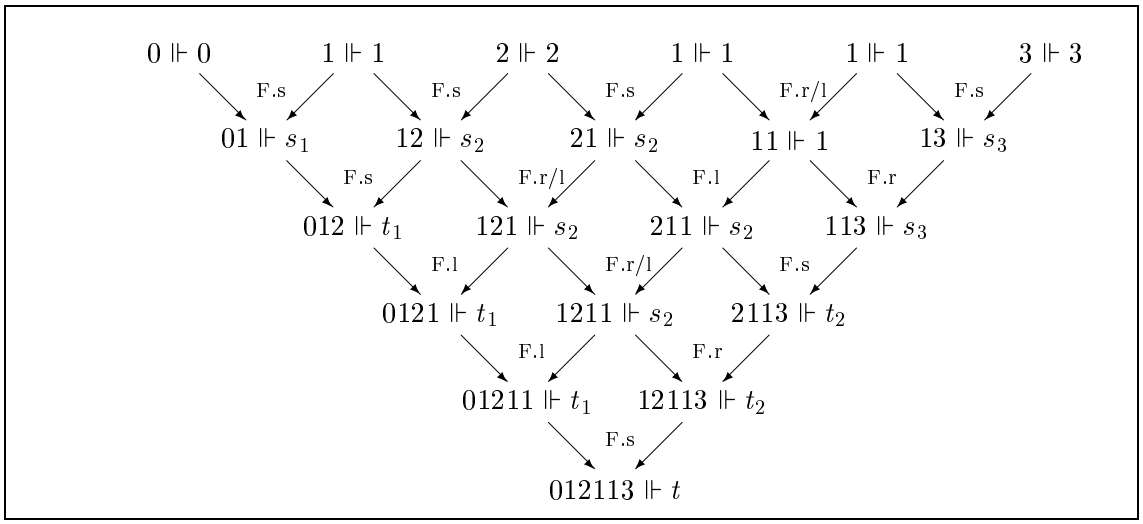

Figure 7: Example: The 3rd-order firing behaviour of trace 012113.

Definition 8.4 *A (generalized)* transition invariant *is an upper closed subset T of $\mathbb{T}$, i.e. whenever $\{t_1, t_2\} \in T$ then both $t_1, t_2 \in T$, too. A trace $w \in \Sigma^+$ is said to* satisfy *T if $\tau(w) \in T$.*

It will be convenient to characterize a transition invariant in terms of those transitions that are not permitted by it. Given a transition invariant T, a transition $t \in \mathbb{T}$ is called a *T-glitch* if t is a $\preceq$-maximal transition outside of T, *i.e.* $t \notin T$ and if $t = \{t_1, t_2\}$ then both $t_1, t_2 \in T$. We call T an *n-transition invariant*, or n-ti for short, if all T-glitches have orders less than or equal to n. Let $\delta^n T$ be the set of T-glitches of order n, and $\delta T = \bigcup_{n \geq 0} \delta^n T$ the set of all T-glitches. Every transition invariant is uniquely determined by δT, *viz.*

$$T \quad = \quad \{\, t \in \mathbb{T} \mid \forall s \in \delta T.\ t \not\preceq s \,\}.$$

In other words: a transition invariant T is the set of all transitions that do not contain any T-glitch. One further shows that a trace w satisfies T iff there does not exist any $s \in \delta T$ and $w' \sqsubseteq w$ such that $w' \Vdash s$.

We now proceed to determine a characteristic formula χ_T^n that approximates a transition invariant T as a specification for eliminating glitches up to and including order n. More precisely, if T is a ti then denote by $[T]_n$ the set

$$[T]_n \quad = \quad \{t \in \mathbb{T} \mid \forall m \leq n.\ \forall s \in \delta^m T.\ t \not\preceq s\}.$$

One checks that this defines an approximating sequence of well-defined transition invariants

$$T = \bigcap_{n \geq 0} [T]_n \quad \subseteq \quad \cdots \quad [T]_{n+1} \ \subseteq \ [T]_n \ \subseteq \ \cdots \ \subseteq \ [T]_1 \ \subseteq \ [T]_0.$$

Intuitively, $[T]_n$ removes a glitch of T only up to and including order n, otherwise preserves it. If T is an n-ti, *i.e.* does not have any glitches above order n, then $[T]_n = T$.

The characteristic formula χ_T^n capturing $[T]_n$ is constructed simultaneously for all T by induction on n as follows:

$$\begin{aligned} \chi_T^0 &= \neg\neg \bigvee_{b \in T \cap \Sigma} (\bigwedge_{b_i=1} p_i \wedge \bigwedge_{b_i=0} \neg p_i) \\ \chi_T^{n+1} &= \chi_T^n \wedge \bigwedge_{\{t_1,t_2\} \in \delta^{n+1} T} \chi_{\{t_1,t_2\}}^n \supset \chi_{\{t_1\}}^n \vee \chi_{\{t_2\}}^n, \end{aligned}$$

where we identify subset $S \subseteq \mathbb{T}$ with the induced ti $\{\, t \in \mathbb{T} \mid \exists s \in S.\ s \preceq t \,\}$. Note that since Σ is finite both $T \cap \Sigma$ and $\delta^{n+1} T$ are finite sets.

Theorem 8.5 *Let T be an n-transition invariant and $w \in \Sigma^+$. Then $w \models \chi_T^n$ iff w satisfies $[T]_n$.*

With an nth-order transition invariant we can specify a dynamic process with internal memory of length n, *i.e.* whose behaviour depends on a history of length n. A 0-ti (state invariant) specifies a process whose behaviour does not depend on anything: the neighbour states can be chosen arbitrarily from a global set of permitted states independent from the previous history or the present state. A 1-ti specifies memory of length 1, *i.e.* the set of possible neighbour states depends on the present state, and in an n-ti ($n > 1$), in general, the set of permitted neighbour states depends not only on the present state but also on the previous $n \perp 1$ states.

Example *For a concrete example of a 2nd-order transition invariant we consider the following variant of the 3-bit up/down counter. Let us suppose that in any sequence of contiguous counting steps in the same direction (up or down) the counter alternates between counting with distance 1 and counting with distance 2; Equivalently: in any three successive states $s_1 s_2 s_3$ the absolute difference between s_1 and s_3 must not be 2 or 4. For instance, 3464675 is a valid counting sequence but 345467 is not. This behaviour cannot be specified by any 1-ti (in terms of the output signals p_0, p_1, p_2) because we need an extra internal state to keep track of the counting difference. One of the transitions we need to eliminate, for instance, is the transition between 0 and 2 via the intermediate state 1, i.e. the sequences 012 and 210. If we focus on this single constraint then we could capture it by the ti*

$$T(012) \quad = \quad \{\, t \in \mathbb{T} \mid t \not\preceq \{\{0,1\},\{1,2\}\} \,\},$$

where $0, 1, 2$ are identified with the corresponding states in $\Sigma = \mathbb{B}^3$. $T(012)$ is a 2-ti with the 2nd-order transition $g = \{\{0,1\},\{1,2\}\}$ as its single glitch. The characteristic formula can be computed as

$$\begin{aligned} \chi_{T(012)}^2 \quad = \quad & \neg\neg(0 \vee 1 \vee \ldots \vee 7) \wedge \\ & (\neg\neg(0 \vee 1 \vee 2) \wedge (\neg\neg(0 \vee 2) \supset \neg\neg 0 \vee \neg\neg 2)) \ \supset \ (\neg\neg(0 \vee 1) \ \vee \ \neg\neg(1 \vee 2)), \end{aligned}$$

where the states $0, 1, 2$ now are identified with the formulas $M(0), M(1), M(2)$, i.e. $0 = M(0) = \neg p_0 \wedge \neg p_1 \wedge \neg p_3$, and so on. From theorem 8.5 we can conclude that a state

sequence w satisfies $\chi^2_{T(012)}$ iff it does not contain the subsequence 012 *or* 210*. The reader is invited to check this directly by unfolding the semantics of the formula $\chi^2_{T(012)}$.*
It should now be clear how the counter can be specified completely by a conjunction $\chi^1_{T_1} \wedge \bigwedge \chi^2_{T(xyz)}$, where T_1 is a suitable 1*-ti and xyz runs through all unwanted* 3*-state sequences, such as* 012 *above.* ∎

9 Conclusion

The paper presented a novel intuitionistic modal logic, PLL, a conservative extension of the standard intuitionistic propositional calculus by a new modal operator $\bigcirc$ 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.
medskip
The modality algebraically resembles a strong closure operator or — from a type-theoretic perspective — a strong monad. The main result is that PLL has a natural class of two-frame Kripke models for which it is sound and complete. This provides a satisfactory model-theoretic account of the modality $\bigcirc$ in an intuitionistic setting. 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, and the disjunction property.

We have given a number of concrete models for PLL, one of them motivated from hardware verification. We interpret PLL over timing diagrams such that $\bigcirc$ expresses truth up to stabilization. In the resulting theory, Circuit-PLL, one derives safe stabilization information even in the presence of glitches, where the standard classical reasoning is sound only under implicit stabilization assumptions. Some results have been presented demonstrating that this logic is able to express nontrivial stability behaviour and a wide class of transition invariants.

The full characterization of expressibility in Circuit-PLL and the existence of finite or complete axiomatizations remain open. A finite axiomatization would establish decidability of and ideally give rise to a cut-free sequent calculus for full Circuit-PLL. As regards expressiveness we conjecture that the upper bound given to the $\bigcirc$-free fragment of Circuit-PLL in section 7.2 is in fact also a lower bound: if this should turn out to be true, we have the perhaps surprising result that every reversible finite-state automaton, whose states are all initial as well as terminal, can be expressed in this intermediate logic.

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 introductory section 1.

10 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, and to Pierangelo Miglioli for pointing out the connection with Maksimova's intermediate logic.
Michael Mendler is supported by a Human Capital and Mobility fellowship in the *Euro-Form* network.

References

[Benton et al., 1993] Benton, N., Bierman, G., and de Paiva, V. (1993). Computational types from a logical perspective I. Draft 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.

[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.

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

[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.

[Moggi, 1989] Moggi, E. (1989). Computational lambda-calculus and monads. In *Proceedings LICS'89*, pages 14–23.

[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.

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

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