A Distributed Kripke Semantics

ROHIT CHADHA, DAMIANO MACEDONIO and VLADIMIRO SASSONE
COMPUTER SCIENCE TECHNICAL REPORT 04/2004
DEPARTMENT OF INFORMATICS
UNIVERSITY OF SUSSEX, BRIGHTON BN1 9QH, UK.
DECEMBER 2004

ABSTRACT. An intuitionistic, hybrid modal logic suitable for reasoning about distribution of resources was introduced in [10]. We extend the Kripke semantics of intuitionistic logic, enriching each possible Kripke state with a set of places, and show that this semantics is both sound and complete for the logic. In the semantics, resources of a distributed system are interpreted as atoms, and placement of atoms in a possible state corresponds to the distribution of the resources. The modalities of the logic allow us to validate properties in a *particular place*, in *some* place and in *all* places. We extend the logic with disjunctive connectives, and refine our semantics to obtain soundness and completeness for extended logic. The extended logic can be seen as an instance of *Hybrid IS5* [2, 18].

1 Introduction

In current computing paradigm, distributed resources spread over and shared amongst different nodes of a computer system is very common. For example, printers may be shared in local area networks, or distributed data may store documents in parts at different locations. The traditional reasoning methodologies are not easily scalable to these systems as they may lack implicitly trustable objects such as a central control.

This has resulted in the innovation of several reasoning techniques. A popular approach in the literature has been the use of algebraic systems such as process algebra [13, 8, 5]. These algebras have rich theories in terms of semantics [13], logics [7, 15, 4, 3], or types [8]. Another approach is logically-oriented [9, 10, 19, 14]: intuitionistic modal logics are used as foundations of type systems by exploiting the *propositions-as-types, proofs-as-programs* paradigm [6]. An instance of this was introduced in [9, 10] and the logic introduced there is the focus of our study.

The formulae in this logic include names, called *places*. Assertions in the logic are associated with places, and are validated in places. In addition to considering *whether* a formula is true, we are also interested in *where* a formula is true. The three modalities of the logic allow us to infer whether a property is

Research partially supported by '**MIKADO**: Mobile Calculi based on Domains', EU FET-GC IST-2001-32222, and '**[illegible]1168.48 ceecuri**

validated in a specific place of the system ($@p$), or in an unspecified place of the system ($\Diamond$), or in any part of the system($\Box$). The modality $@p$ internalises the model in the logic and hence can be classified as a hybrid logic [1, 16, 2]. An intuitionistic natural deduction for the logic is given in [9, 10], and judgements in the logic mention the places under consideration. The natural deduction rules for $\Diamond$ and $\Box$ resemble those for existential and universal quantification of first-order intuitionistic logic.

As noted in [9, 10], the logic can also be used to reason about distribution of resources in addition to serving as the foundation of a type system. The papers [9, 10], however, lack a model to match the usage of the logic as a tool to reason about distributed resources. In this report, we bridge the gap by presenting a Kripke-style semantics [12] for the logic of [9, 10]. In Kripke-style semantics, formulae are considered valid if they remain $\forall^{\text{ifit}}$

completeness. In the refined semantics, the set of places in Kripke states are not fixed. Different possible Kripke states may have *different* set of places. However, the set of places vary in a conservative way: larger Kripke states contain larger set of places.

We show that the refined semantics is both sound and complete for the extended logic. The proof of soundness once again depends on duplication of places. The proof of completeness follows closely the standard proofs of completeness of intuitionistic modal logics. The extended logic can be seen as hybridization of the well-known intuitionistic modal system *IS5* [2, 18].

The rest of the paper is organised as follows. In Section 2, we present the logic in [9, 10]. In Section 3 we present the distributed Kripke model used to interpret the logic, and prove soundness and completeness of the semantics. We present the extension of logic with logical connectives in Section4. The refined semantics is given in Section 5, where we also show soundness and completeness of the refined logic. We discuss related work in Section 6, and we summarise our results in Section 7.

2 Logic

We now introduce, through examples, the logic presented in [9, 10]. The logic is used to reason about heterogeneous distributed systems. To gain some intuition, consider a *distributed peer to peer database* where the information is partitioned over multiple communicating nodes (peers).

Informally, the database has a set of nodes, or *places*, and a set of resources

three modalities to accommodate reasoning about the properties valid at different locations.

In order to internalise resources at a single location, the modality $@p$, one for every place in the system, is used. The modality @ casts the meta-linguistic "***at***" on the language level, and in fact the two constructs will have the same interpretation in the semantics. The modal formula $\varphi@p$ means that the property φ is valid at p, and not necessarily an

Each judgement in this logic is of the form

$$\Gamma; \Delta \vdash^{P} \varphi \textbf{ at } p.$$

where

- the *global context* Γ is a (possibly empty) finite set of pure formulae, and represents the properties assumed to hold at every place of the system;
- the *local context* Δ is a (possibly empty) finite set of sentences; since a sentence is a pure formula associated to a place, Δ represents what we assume to be valid in any particular place.
- the sentence φ ***at*** p says that φ is derived to be valid in the place p by assuming $\Gamma; \Delta$.

In the judgement, it is assumed that the places mentioned in Γ and Δ are drawn from the set P. In order to be more formal, we define the function $\mathsf{PL}(X)$, which denotes the set of places that appear in X, for any syntactic object X. It is defined as follow

DEFINITION 1 (PLACES IN A FORMULA). *We define inductively the operator* $\mathsf{PL}(\,)$ *on any syntactic object of the logic as:*

$$\mathsf{PL}(A) \quad \stackrel{\text{def}}{=}$$

L

$$\frac{}{\Gamma;\Delta,\varphi\ \mathbf{at}\ p \vdash^P \varphi\ \mathbf{at}\ p}$$

G

$$\frac{}{\Gamma,\varphi;\Delta \vdash^P \varphi\ \mathbf{at}\ p}$$

$\top I$

$$\frac{}{\Gamma;\Delta \vdash^P \top\ \mathbf{at}\ p}$$

$\wedge I$

$$\frac{\Gamma;\Delta \vdash^P \varphi_1\ \mathbf{at}\ p \quad \Gamma;\Delta \vdash^P \varphi_2\ \mathbf{at}\ p}{\Gamma;\Delta \vdash^P \varphi_1 \wedge \varphi_2\ \mathbf{at}\ p}$$

$\wedge E_i$ (i=1,2)

$$\frac{\Gamma;\Delta \vdash^P \varphi_1 \wedge \varphi_2\ \mathbf{at}\ p}{\Gamma;\Delta \vdash^P \varphi_i\ \mathbf{at}\ p}$$

$\rightarrow I$

$$\frac{\Gamma;\Delta,\varphi\ \mathbf{at}\ p \vdash^P \psi\ \mathbf{at}\ p}{\Gamma;\Delta \vdash^P \varphi \rightarrow \psi\ \mathbf{at}\ p}$$

$@I$

$$\frac{\Gamma;\Delta \vdash^P \varphi\ \mathbf{at}\ p}{\Gamma;\Delta \vdash^P \varphi@p\ \mathbf{at}\ p'}$$

$@E$

$$\frac{\Gamma;\Delta \vdash^P \varphi@p\ \mathbf{at}\ p'}{\Gamma;\Delta \vdash^P \varphi\ \mathbf{at}\ p}$$

$\rightarrow E$

$$\frac{\Gamma;\Delta \vdash^P \varphi \rightarrow \psi\ \mathbf{at}\ p \quad \Gamma;\Delta \vdash^P \varphi\ \mathbf{at}\ p}{\Gamma;\Delta \vdash \psi\ \mathbf{at}\ p}$$

$\Diamond I$

$$\frac{\Gamma;\Delta \vdash^P \varphi\ \mathbf{at}\ p}{\Gamma;\Delta \vdash^P \Diamond\varphi\ \mathbf{at}\ p'}$$

$\Diamond E$

$$\frac{\Gamma;\Delta \vdash^P \Diamond\varphi\ \mathbf{at}\ p' \quad \Gamma;\Delta,\varphi\ \mathbf{at}\ q \vdash^{P+q} \psi\ \mathbf{at}\ p''}{\Gamma;\Delta \vdash^P \psi\ \mathbf{at}\ p''}$$

$\Box I$

$$\frac{\Gamma;\Delta \vdash^{P+q} \varphi\ \mathbf{at}\ q}{\Gamma;\Delta \vdash^P \Box\varphi\ \mathbf{at}\ p}$$

$\Box E$

$$\frac{\Gamma;\Delta \vdash^P \Box\varphi\ \mathbf{at}\ p \quad \Gamma,\varphi;\Delta \vdash^P \psi\ \mathbf{at}\ p'}{\Gamma;\Delta \vdash^P \psi\ \mathbf{at}\ p'}$$

FIGURE 1. Natural deduction.

that the formula is validated there. If any assertion that does not mention the new place is validated thus, then it is also validated using the old local context. The rule $\Box$

3 Kripke Semantics

There are a number of semantics for intuitionistic logic and intuitionistic modal logics that allow for a completeness theorem [2, 11, 18]. In this section we concentrate on the semantics introduced by Kripke [12, 20], as it is convenient for applications and fairly simple. This would provide a formalisation of the intuitive concepts introduced in Section 2.

In Kripke semantics for intuitionistic propositional logic, logical assertions are interpreted over Kripke models. The validity of an assertion depends on its

it is valid in a given state, then it remains valid at the same places in all larger states. For example, the formula $\varphi \wedge \psi$ is valid in a state k at place p, if both φ and ψ are true at place p in all states $l \geq k$.

The introduction of places in the model allows the interpretation of the spatial modalities of the logic. Formula $\varphi@p$ is satisfied at a place in a state k, if it is true at p in all states $l \geq k$; $\Diamond\varphi$ and $\Box\varphi$ are satisfied at a place in state k, if φ is true respectively at some or at every place in all states $l \geq k$.

We extend now the interpretation of atoms to interpretation of formulae, we use induction on the structure of the formulae.

DEFINITION 3 (KRIPKE SEMANTICS). *For* $\mathcal{K} = (K$

the same properties that we inferred in Section 2 by using a distributed Kripke model. Fix a Kripke state k. The assumption that the two parts, $\mathsf{doc}_1, \mathsf{doc}_2$, can be combined in p in a state k to give the document doc can be expressed as $(k, p) \models (\mathsf{doc}_1 \wedge \mathsf{doc}_2) \rightarrow \mathsf{doc}$. If the resources doc_1 and doc_2 are assigned to the place p, i.e., $(k, p) \models \mathsf{doc}_1$ and $(k, p) \models \mathsf{doc}_2$, then, since $(k, p) \models \mathsf{doc}_1 \wedge \mathsf{doc}_2$, it follows that $(k, p) \models \mathsf{doc}$.

Let us consider a slightly more complex situation. Suppose that $k \models \Diamond(\mathsf{doc}_2 \wedge (\mathsf{doc}_2 \rightarrow \Box\mathsf{doc}_2))$ ***at*** p'. According to the semantics of $\Diamond$, there is some place r such that $(k, r) \models \mathsf{doc}_2 \wedge (\mathsf{doc}_2$

LEMMA 2 (

$(k, q) \models {}_{q(p)}\varphi_1$. We conclude $(k, t) \models {}_{q(p)}\varphi_1$ for every $t \in Pls_{q(p)}$, which implies $(k, r) \models {}_{q(p)}\Box\varphi_1$. ■

Another property of distributed Kripke models is the possibility to rename the places in the model. The property says that if we rename a place in the model, then we do not modify the set of valid properties not involving the renamed place. First we prove that the renamed model is still a distributed Kripke model, then we formalize the property in Lemma 3.

PROPOSITION 2 (p-RENAMING

two most significant cases and prove property *1*. The other cases can be dealt with easily.

Case $\varphi = \Diamond\varphi_1$. Let $r \in P$ and suppose $(k, r) \models_{q/p} \Diamond\varphi_1$. Then, by definition there exists $s \in Pls_{q/p} = P \cup \{q\}$ such that $(k, s) \models_{q/p} \varphi_1$. If $s \in P$, we use inductive

THEOREM 1 (SOUNDNESS). *If* $\Gamma; \Delta \vdash^{P} \mu$ **at** *p is derivable in the logic, then it is valid.*

Proof: The proof proceeds by induction on the number *n* of inference rules applied in the derivation of the judgement Γ

inductive hypothesis says that $(k, q) \models \varphi@p$, and therefore $(k, p) \models \varphi$.

Case $\Box I$. Then μ is of the form $\Box\varphi$. Moreover $\Gamma; \Delta \vdash^{P+q} \varphi$ ***at*** p_1 for some $p_1 \notin P$ by using $n - 1$ instances of the inference rules. By inductive hypothesis we know that $\Gamma; \Delta \models^{P+p_1} \varphi$ ***at*** q. Please note that since $\Gamma; \Delta \vdash^{P} \mu atp$, we also have $\mathsf{PL}(\Gamma; \Delta) \cup \mathsf{PL}(\varphi) \subseteq P$. Let *Pls* be $P + p_1$.

First, consider the case when $p_1 \notin Pls$. We need to show that $k \models \Box\varphi$ ***at*** p. According to semantics of $\Box$, it suffices to show that $k \models \varphi$ ***at*** r, for all $r \in Pls$. Fix one $r \in Pls$, and consider the r-duplicated extension

sentences by saying that $\Gamma; \Sigma \vdash^P \varphi$ ***at*** q, if and only if, there exists a finite set $\Delta \subseteq \Sigma$ such that $\Gamma; \Delta \vdash^P \varphi$ ***at*** q.

As in standard proofs of completeness of intuitionistic logics[20, 18, 2], the proof of completeness is based on the construction of a particular distributed Kripke model: the *canonical model*. We will prove that a sequent is valid in the canonical model if and only if it is derivable in the logic. In the construction of the canonical model, we consider particular kinds of sets of formulae.

DEFINITION 6 (PRIME SET). *Given a set of places Pls and a finite set* Γ *of pure formulae in Frm*(*Pls*)*, a (possibly non-finite) set* Σ *of sentences with* $\mathsf{PL}(\Sigma)$

2. *Given* $\varphi \in Frm(P_n$ *and*

2. *for all* $\varphi \in Frm(Pls)$, $\Sigma \in M$ *and* $q \in Pls$: $(\Sigma, q) \models \varphi$ *if and only if* $\Gamma; \Sigma \vdash^{Pls} \varphi$ **at** q.

Proof: Clearly the inclusion

case that for every k

fined distributed Kripke model with set of places, Pls. Given $k \in K$, $p \in P_k$, *a pure formula* φ *with* $\mathsf{PL}(\varphi) \subseteq Pls$, *we define* (*k*

Moreover we say that $\Gamma; \Delta \vdash^P \mu$ ***at*** p is ref-valid *(and we write* $\Gamma; \Delta \models \mu$ **at** p*) if it is valid in every refined distributed Kripke model.*

5.1 Soundness

In this section we shall prove the soundness of the extended logic in refined distributed Kripke models. The proof of soundness will follow the proof of the soundness in section 3.2. We start by defining the p-duplicated extension of a refined distributed Kripke model.

PROPOSITION 4 (p-DUPLICATED EXTENSION

- $I'_k : Atoms \rightarrow P$

treatment of logical connectives is standard. The modalities @ and ◊ are teated as in Theorem 1. If the last inference rule used is □*E*, then the result follows from a simplethe

Property).

As in [18, 2] we first show that every set of sentences can be extended to a prime set, that respects the non-prov

- $\psi_1 \vee \psi_2$ ***at*** $q \notin \mathit{treated}^{\vee}_n$.

Please note that if both $\Gamma; \Sigma_n, \psi_1$ ***at*** $q \vdash^{P_n} \varphi$ ***at*** p and $\Gamma; \Sigma_n, \psi_2$ ***at*** $q \vdash^{P_n} \varphi$ ***at*** p, then we can deduce $\Gamma; \Sigma_n \vdash^{P_n} \varphi$ ***at*** p. However, we have that Σ_n, P_n satisfy Property 2. Hence, it must be the case that either $\Gamma; \Sigma_n, \psi_1$ ***at*** $q \nvdash^{P_n} \varphi$ ***at*** p, or $\Gamma; \Sigma_n, \psi_2$ ***at*** $q \nvdash^{P_n} \varphi$ ***at*** p.

We define $\Sigma_{n+1} = \Sigma_n \cup \{\psi_1$ ***at*** $q\}$ if $\Gamma; \Sigma_n, \psi_1$ ***at*** $q \nvdash^{P_n} \varphi$ ***at*** p, and $\Sigma_{n+1} = \Sigma_n \cup \{\psi_2$ ***at*** $q\}$ otherwise. We define $P_{n+1} = P_n$. We get by construction that P_{n+1}, Σ_{n+1} satisfy Property 2. Finally, we let $\mathit{treated}^{\vee}_{n+1} = \mathit{treated}^{\vee}_n \cup \{\psi_1 \vee \psi_2$ ***at*** $q\}$ and $\mathit{treated}^{\Diamond}_{n+1} = \mathit{treated}^{\Diamond}_n$.

If $n + 1$ is even, pick the first formula $\Diamond\psi$ in the enumeration such that

- $\Diamond\psi$ is in $\mathit{Frm}(P_n)$, i.e., all the places in $\Diamond\psi$ are taken from P_n;
- $\Gamma; \Sigma_n \vdash^{P_n} \Diamond\psi$ ***at*** q, for some $q \in P_n$;
- $\Diamond\psi \notin \mathit{treated}^{\Diamond}_n$.

Let $P_{n+1} = P_n + q_{(n+}$

Now, we define the refined canonical model. In the refined canonical model, Kripke states are prime sets of sentences.

DEFINITION

canonical model, Σ' is (Γ, Q)-prime set. Therefore, we obtain φ_1 ***at*** $q \in \Sigma'$ for every $q \in Q$. Hence by inductive hypothesis, $(\Sigma', Q) \models \varphi_1$ ***at*** q for every $q \in Q$. Since $P \subseteq Q$, we get $(\Sigma', Q) \models \Box\varphi_1$ ***at*** p. ■

We are now ready to prove completeness.

THEOREM 4 (REFINED COMPLETENESS).

The work in [2] introduces the first intuitionistic version of hybrid logics. It investigates how to add names in constructive logics resulting in hybrid versions. A modal logic is hybridised by adding a new kind of propositional symbols: *nominals*. The

Oxford, 1963, pages 92–130. North-Holland Publishing Company, 1965.

[13] R. Milner, J. Parrow, and D. Walker. A calculus of mobile processes, parts I and II. *Information and Computation*, 100(1):1–77, 1992.

[14] J. Moody. Modal logic as a basis for distributed computation. Technical Report CMU-CS-03-194, Carnegie Mellon University, 2003.

[15] P.W. O'Hearn and D. Pym. The logic of bunched implications. *Bulletin of Symbolic Logic*, 5(2):215–244, 1999.

[16] A. Prior. *Past, Present and Future*. Oxford University Press, 1967.

[17] J. Reynolds. Separation logic: a logic for shared mutable data structures. In *LICS'02*, pages 55–74. IEEE Computer Society Press, 2002.

[18] A.K. Simpson. *The Proof Theory and Semantics of Intuitionistic Modal Logic*. PhD thesis, University of Edinburgh, 1994.

[19] K. Crary T. Murphy, R. Harper, and F. Pfenning. A symmetric modal lambda calculus for distributed computing. In *LICS'04*, 2004. To appear.

[20] D. van Dalen. *Logic and Structure*. Springer Verlag, 4th extended edition, 2004.