PHD IN COMPUTER SCIENCE (XVII CICLO)

LOGICS FOR DISTRIBUTED RESOURCES
RESEARCH REPORT

DAMIANO MACEDONIO
DIPARTIMENTO DI INFORMATICA
UNIVERSITÀ CA' FOSCARI DI VENEZIA

Abstract. This report outlines the research carried out during the PhD course in Venice. The general aim is to define logical characterisations of distributed systems, to describe resources in heterogeneous environments. We identified two complementary approaches: *proof theoretical* and *model theoretical*. The former studies the Bunched Implications Logic and Intuitionistic Modal Logic. The latter leads to the definition of a spatial logic for bigraphs, named *BiLog*.

Introduction

In our daily life it is common to deal with distributed computing resources. Prime examples are programs which are sent or fetched from different sites, and may be run as a code to do simple calculation tasks or as interactive parallel programs using resources located almost everywhere in the world. Accordingly, the ability to reason about correctness of the behaviour of concurrent systems holding or using such resources, as well as the need of design and implementation tools, is raising to an increasing prominent role. This prefigures exciting future perspectives, but it poses enormous challenger to computer science. The lack of any kind of central control, the continuously mutating topology of the network, the lack of reliable information, the absence of any intrinsically trustable object imply the necessity of designing new formal models to describe and reason on properties of distributed resources. This necessity has been recognised by several authors (e.g., [4, 23, 26, 36]).

Following the traditional approaches, properties of concurrent systems and distributed resources can be expressed in terms of *semantics*, *logics*, or *types*. We propose to study logical characterisations of distributed systems which are suitable to describe resources in heterogeneous environments. Our principal aim is to specify logics to characterise concurrent systems. The logics we developed mainly describe the structures of a distributed system. Our focus is more on the structure and the distribution of resources, than their behaviour. A logical formalism should simplify the definition and the verification of properties for a distributed system. A formula defines a property which assumes meaning in a defined model. On the one hand, a formula characterises a class of processes: the processes that enjoys the expressed property [4]. On the other hand, a formula models directly the observed properties of resources in a distributed system [23, 32, 36].

Date: October 2005.

Moreover a logic helps in deriving new properties as well as connections between different characterisation of processes properties or resource distributions. Our purpose is to individuate a logical language which is able to describe the behaviour and spatial structure of concurrent systems. The aim of the thesis is to use the logic to describe process and resources behaviour. Its title is *'Logics for Distributed Resources.'*

Thesis

In order to develop a logic that exploits both the spatial characteristics and interconnections of objects in a distributed system, we identified two complementary strategies to follow.

(1) *Proof theoretical approach*: to specialise a pure logical calculus in order to express properties in a distributed system, and to introduce a pure logical framework suitable to characterise heterogeneous environments.
(2) *Model theoretical approach*: to define a logical calculus by considering a formalisation for distributed systems as a model, and to interpret the new logical constructs in such a model.

On the one hand, we identified a group of candidate languages suitable for developing the proof theoretical approach. They are

- *Spatial Logic* [4, 5], which provides a powerful language to formally describe the structure of concurrent processes.
- *Bunched Implication* [32] or *Separation Logic* [1, 36], which provide a powerful language to describe resources in distributed systems.
- *Modal Intuitionistic Logic* [23, 30, 31], in which the modalities are not interpreted *temporarily*, but *spatially*.

On the other hand, in the second approach, the range of process calculi to choose as a formalism for distributed system is wide. We focalised on *Bigraphs* [22, 26], which are establishing themselves a truly general (meta-)model of global systems, and appear to encompass several existing calculi and models, including CCS [29], π-calculus [22], ambients [20], and Petri-nets [28]. A logic founded on bigraphs aims at achieving the same generality as a description language: as bigraphs specialise to particular models, the focus of our research is to understand how to specialise BiLog to powerful logics on these, in this sense, some results have already been reached in [15, 16].

The thesis is basad on the following publications:

[2] A. Bossi, D. Macedonio, C. Piazza and S. Rossi. *Information Flow in Secure Contexts.* Journal of Computer Security, 2005.

[12] R. Chadha, D. Macedonio and V. Sassone. *A Distributed Kripke Semantics.* Computer Science Report 2004:04, University of Sussex, 2004.

[13] R. Chadha, D. Macedonio and V. Sassone. *A Hybrid Intuitionistic Logic: Semantics and Decidability.* Accepted for publication in the Journal of Logic and Computation, October 2005.

[14] G. Conforti, D. Macedonio and V. Sassone. *Bigraphical Logics for XML.* Proc. of the Thirteenth Italian Symposium on Advanced Database Systems (SEBD), 2005.

[15] G. Conforti,D. Macedonio and V. Sassone. *BiLog: spatial logics for bigraphs.* Computer Science Report 2005:02, University of Sussex, 2005.

[16] G. Conforti, D. Macedonio and V. Sassone. *Spatial Logics for Bigraphs.* Proc. of Int. Colloquium on Automata, Languages and Programming (ICALP), 2005.
[25] D. Macedonio and G.Sambin. *Relational Semantics for Basic Logic.* To appear in the Journal of Symbolic Logic.

Proof Theoretical Approach.

Separation Logic. The first logical formalism we considered is Separation Logic [33, 36], initially introduced to support compositional reasoning about sequential programs which manipulate pointers. Separation Logic introduced the novel logical operation $\varphi * \psi$ (the *separating conjunction*) that asserts that φ and ψ are formulae holding for *disjoint* portions of the addressable storage. The prohibition of sharing is built into the operation.

The logic of Bunched Implications, **BI** [32, 35], generalises the idea of separation by dealing not only with pointers, but also with distributed resources in general. It models directly the observed properties of resources. The very first model of the logic is very simple: a *set* of resources, which can be *combined* and *compared*. Mathematically, this set-up is modelled with a *partial monoid* that is *commutative* and *partially ordered*. Such a model is useful to obtain a Kripke-style semantics which freely combines multiplicative (intuitionistic linear) and additive (intuitionistic) conjunctions.

The main feature of **BI** are the *bunches* instead of the contexts (i.e., lists of formulae) in a sequent. Intuitively, bunches are trees of formulae. They are built by using two ways of combining formulae at the meta level: multiplicative (only commutative) and additive (with weakening and contraction). Thanks to the particular structure of bunches the calculus presents two conjunctions and two adjoint operators: the multiplicative $*$, the additive $\wedge$, and the corresponding implications $-\!\!*$ and $\rightarrow$. We studied the connection of **BI** with its principal constituents: Linear Logic (**LL**) [18] and Intuitionistic Logic (**IL**). They differ principally in the implications. In **LL** an **IL** there is only a native implication: multiplicative for **LL** and additive for **IL**. In **BI** there are two native and independent implications. From a proof theoretical point of view (natural deduction and sequent calculus), we found that **BI** is the Intuitionistic Linear Logic (**ILL**) with a new connective ($\rightarrow$) defined to be adjoint to the additive conjunction between formulae ($\&$). In other words, in order to obtain **BI** from **ILL** it is sufficient to enrich the language with the symbol $\rightarrow$ and require the axiom "$\varphi \vdash \psi \rightarrow \mu$ *if and only if* $\varphi \,\&\, \psi \vdash \mu$." We also compared **BI** with Basic Logic [37, 25], that is the common core between **LL** and **IL**. This work has been concluded, but not written yet.

Basic Logic. The sequent calculus **B**, named Basic Logic, has been introduced in [37] with the aim of finding a structure in the space of the logics. Classical, intuitionistic, quantum and non-modal linear logics, are all obtained as extensions in a uniform way. The calculus is defined by introducing the *principle of reflection*. A logical constant obeys the principle of reflection if it is characterised semantically by an equation binding it with a metalinguistic link between assertions, and if its syntactic inference rules are obtained by solving that equation. All the connectives of Basic Logic satisfy reflection. As an example, consider the additive conjunction $\&$. The common explanation of the truth of a compound proposition like $\varphi \,\&\, \psi$ is that $\varphi \,\&\, \psi$ is true if and only if φ is true *and* ψ is true. In this case the connective

& reflects at the level of object language the link *and* at the metalanguage. The semantical equivalence that we obtain in term of sequents is "$\Gamma \vdash \varphi \,\&\, \psi$ *if and only if* $\Gamma \vdash \varphi$ *and* $\Gamma \vdash \psi$" which we call *definitional equation* for &. By *solving* such an equation, we obtain the inference rules for &, and we say that & is introduced according to the principle of reflection.

We found that also the sequent calculus for **BI** [35] can be introduced according to the principle of reflection. In particular the connectives $*$ and $\wedge$ reflect the two way of combining formulae with bunches. Moreover, inspired by the principle of reflection, we introduced a new sequent calculus equivalent to **BI** that does not use bunches. Such a calculus is useful to introduce **BI** in a natural and intuitive way, but, unfortunately, it does not enjoy the *cut elimination* property. Such a calculus is the combination of two kind of sequents: the linear (multiplicative) $\Gamma \vdash \varphi$, and the intuitionistic (additive) $\Gamma \Vdash \varphi$. The only communication between the two way of reasoning can happen only when the left context is a single formula, i.e., we allow for two communication rules:

$$\frac{\varphi \vdash \psi}{\varphi \Vdash \psi}\ \text{Mult to Add} \qquad\qquad \frac{\varphi \Vdash \psi}{\varphi \vdash \psi}\ \text{Add to Mult}$$

Unfortunately, these two rules are not appropriate for the elimination of cut rules.

In [25] a monoidal semantics for Basic Logic has been introduced. The models we introduced are close to **BI**'s models. They are just monoids $(M, \cdot, 1)$ equipped with any binary relation R, that we name *relational monoids*. Note that in this case the operation $\cdot$ is *total*. The idea we follow to define the semantics is thinking of M as the set of resources in a distributed system. We admit a representative or *null* resource (the neutral element "1") and a way of *combining* resources (the monoidal operation "$\cdot$"). We can read the relation R as an *accessibility* relation, by saying xRy if *the resource x can access the resource y* in the system. Such a relation induces two operator on resources:

$$\begin{array}{lll} x^{\rightarrow} \stackrel{def}{=} & \{y \in M \,:\, xRy\} & \text{the resources that } x \text{ can access;} \\ y^{\leftarrow} \stackrel{def}{=} & \{x \in M \,:\, xRy\} & \text{the resources that access to } y. \end{array}$$

The operators are extended on subsets and are used to define an evaluation of formulae. We proved a theorem of soundness and a theorem of *refined* completeness that enables a semantical proof of cut elimination as corollary. We extended in a modular way the relational semantics to intuitionistic and classical linear logic, intuitionistic logic, and classical logic. All the extensions allow for a refined completeness theorem, leading to a semantical cut elimination proof.

It is possible to extend such a result also to **BI**. In this case the model is a set with a binary relation and two monoidal operations. Such a monoid is the combination of the monoids that gives a semantic to **ILL** and **LL**. The extended semantics gives a refined completeness theorem, that provides a constructive semantical proof of cut elimination for the sequent calculus **LBI** introduced in [35]. Intuitively the two properties we add to relational monoids correspond to ask for two well defined implications: the one is linear and the other intuitionistic. Hence we have a *semantical diamond*: by starting from **B**, we obtain **ILL** by requiring a multiplicative implication ($\multimap$), **IL** by requiring an additive implication ($\rightarrow$), and finally **BI** by requiring both the implications (and two monoidal operations).

If we relax the requirement of a refined completeness theorem, it is possible to simplify the models for **BI** by considering partial ordered monoids $(M, \cdot, \leq)$, where

the order $\leq$ is partial and the monoidal operation $\cdot$ is total. In fact, the extension of the monoidal semantics for **LL** has recently been simplified in [17] to a partial ordered set of resources $(M, \leq)$. The semantics for **BI** is obtained by combining the relational semantics for **ILL** and the semantics for **IL** given in [17]. We prove a soundness and completeness theorem for **BI** on partially ordered monoids (with a total operation), whose proof is entirely constructive. A paper is in preparation on that.

Intuitionistic Modal Logic. A first attempt to deal explicitly with distributivity and **BI** is presented in [1], where the original monoidal model for **BI** is enriched with locations, in an ambients-like formalism. The work in [1] presents a simple Kripke model were resources are explicitly distributed in locations and extends the language of **BI** by introducing locations. Roughly speaking, this work can be seen as an intuitionistic version of ambient logic [11]. We preferred to focus on a more general logic, by considering a modal intuitionistic logic [38] in which the modalities $\Box\varphi$ (always) e $\Diamond\varphi$ (in the future) are not interpreted *temporarily*, but *spatially*. We interpret them as *everywhere* and *somewhere* in the system. Recently, many authors have moved in this direction [23, 30, 31]: intuitionistic modal logics are used as foundations of type systems by exploiting the *propositions-as-types, proofs-as-programs* paradigm [19]. An instance of this was introduced in [23], and we focused our study on the logic introduced there.

Formulae in such a logic [23] include names, called *places*. Assertions in the logic are associated with places, and are validated in places. The three modalities of the logic allow us to infer whether a property is validated in a specific place of the system ($@p$), or in an unspecified place of the system ($\Diamond$), or in any part ($\Box$). The modality $@p$ internalises the model in the logic and hence it can be classified as a hybrid logic. Although hybrid logics are usually studied in a classical setting, an intuitionistic natural deduction for such a logic is given in [23], whose judgements mention the places under consideration.

As noted in [23], the logic can also be used to reason about distribution of resources in addition to serving as the foundation of a type system. That paper, however, lacks a model to match the usage of the logic as a tool to reason about distributed resources. In [12] we bridged the gap by presenting a Kripke-style semantics [24] for the logic of [23]. We extended the Kripke semantics of the intuitionistic logic [24], enriching possible worlds with fixed sets of places. In each possible world, different places satisfy different formulae. For the intuitionistic connectives, the satisfaction of formulae at a place in a possible world follows the standard definition [24]. The enrichment of the model with places reveals the true meaning of the modalities in the logic. In the model, we interpret atomic formulae as the resources of a distributed system, and placement of atoms in a possible world corresponds to the distribution of resources.

We have considered several extensions of the logic. A major limitation of the logic presented in [23] is that if a formula ψ is validated at some named place, say p, then the formula $\psi@p$ can be inferred at every other place. Similarly if $\Diamond\psi$ or $\Box\psi$ can be inferred at one place, then they can be inferred at any other place. In a large distributed system, we may want to restrict the rights of accessing information in a place. We investigated an extension of the logic to formalise accessibility of places and we reached the well known intuitionistic modal setting [3, 38].

By means of a counter example, adapted from [34], we proved that the semantics in [12] does not enjoy the finite model property. In [13] we refined such model by introducing a *bi-relational models* [38], the semantics given on such models is sound and complete for the logic.The reason for introducing bi-relational models is that they satisfies the finite model property, and so they allow us to prove decidability. As in Kripke models, birelational models have a partially ordered set. In addition, birelational models also have an equivalence relation amongst elements. Unlike the Kripke semantics, we do not enriched each world with a set of places. Instead, we defined a partial function, *the evaluation function*, which attaches a name to a world in its domain. The partiality of the function is crucial to the proof of decidability. The canonical model used to prove completeness is carefully defined in order to deduce the finite model property for the birelational semantics: if a judgement is not provable in the logic, then we can construct a finite birelational model which invalidates the judgement. The proof is adapted from the case of intuitionistic modal logic [38]. Then we conclude the decidability of the logic. Hence we could use such a logic to solve *queries* in a distributed system, e.g., a P2P distributed database to address query such as "Is there such information?", "Where are these data stored?"

Model Theoretical Approach.

Bigraphs. Bigraphs [22, 26] are an emerging model for structures in global computing, which can be instantiated to model several well-known examples, including CCS [29], the π-calculus [21, 22], the ambient calculus [20] and Petri nets [28]. Bigraphs consist essentially of two graphs sharing the same nodes, which have a *control* for specifying their nature or behaviour. The first graph, the *place graph*, is tree structured and expresses a hierarchical relationship on nodes (viz. locality in space and nesting of locations). The second graph, the *link graph*, is an hyper-graph and expresses a generic n-to-n relationships among nodes (e.g. data link, sharing of a channel). The two structures are orthogonal, so links between nodes can cross locality boundaries. Thus, bigraphs express two kinds of separation: *structural* separation (i.e. separation in the place graph) and *name* separation (i.e. separation on the link graph). By combining these two notion we obtain a 'strong' version of separation for general bigraphs.

At the top level of the tree structure sit the *regions*. Inside nodes there may be 'context' *holes* which are uniquely identified by ordinals. Place graphs can be seen as arrows over a symmetric monoidal category whose objects are ordinals. We write $P : m \to n$ to indicate a place graph P with m holes and n regions. Given place graphs P_1, P_2, their composition $P_1 \circ P_2$ is defined only if the holes of P_1 are as many as the regions of P_2, and amounts to *filling* holes with regions, according to the number each carries. The tensor product $P_1 \otimes P_2$ corresponds to put close the two structures, it is symmetric, but not commutative, as it 'renumbers' regions and holes 'from left to right'.

Link graphs are arrows of a partial monoidal category whose objects are (finite) sets of names, X, Y. Given an link graph $W : X \to Y$, the set X represents the *inner* names and Y represents the set of *outer* names. The composition of link graphs $W_1 \circ W_2$ corresponds to *linking* the inner names of W_1 with the corresponding outer names of W_2 and forgetting about their identities. The tensor product $\otimes$ of link graphs is defined in the obvious way only if their inner/outer names are disjoint.

Combining ordinals m with names X we obtain *interfaces*, that are couples $\langle m, X\rangle$. Combining the notion of place graph and link graphs on the same nodes we obtain the notion of bigraphs, i.e., arrows $G : \langle m, X\rangle \to \langle n, Y\rangle$. Given two bigraphs G_1 and G_2, intuitively the composition $G_1 \circ G_2$ *first* places every region of G_2 in the proper hole of G_1 (place composition) and *then* joins equal inner names of G and outer names of F (link composition). The operation is partially defined, since it requires the inner names and the number of holes of G to match the number of regions and the outer names of F, respectively. Shared names create the new links between the two structures. On the other hand the tensor product $G_1 \otimes G_2$, consists of placing close the two bigraphs, only in the case that the tensor product between their link graphs is defined.

BiLog: a logic for bigraphs. In [16], we exploited the bi-structural nature of the bigraphical model to introduce a '*contextual nominal/spatial logic*' for bigraphs built on two orthogonal sublogics:

- a *place graph logic* (for tree contexts), to express properties of resource locations;
- a *link graph logic* (for name linkings), to express connections between resources (or, more precisely, resource names).

For this reason, we named the formalism *BiLog*.

We consider the axiomatisation given in [27], where the bigraphical terms are introduced. Every bigraph is formalised as the composition of fixed constructor terms by using the bigraphical operations $\circ$ and $\otimes$. BiLog internalises the bigraphical term constructors in the style of the ambient logic [11]. Constructors are represented in the logic as constant formulae, while tensor product and composition are expressed by connectives. We thus have two binary spatial operators. This contrasts with other spatial logics, which have only one: ambient-like logics, with parallel composition $A \mid B$, Separation Logic [36], with separating conjunction $A * B$, and Context Tree Logic [8], with application $K(P)$. Our logic is parameterised on a transparency predicate, that establish when a term can be directly observed in the logic: some are opaque and do not allow inspection of their contents. In [16] we showed that when all terms are observable, logical equivalence corresponds to congruence. Otherwise, it can be less discriminating.

The logic features a logical constant for each *transparent* construct. The satisfaction of logical constants is simply defined as the congruence to the corresponding constructor. The *horizontal decomposition* formula $A \otimes B$ is satisfied by a term that can be decomposed as the tensor product of terms satisfying A and B respectively. The *vertical decomposition* formula $A \circ B$ is satisfied by terms that can be seen as the composition of terms satisfying A and B. Moreover we define the *left* and *right adjuncts* for composition and tensor to express extensional properties.

The main point is that a resource has a spatial structure as well as a link structure associated to it. Suppose for instance to be describing a tree-shaped distribution of resources in locations. We may use atomic formulae like $\mathsf{PC}(A)$ and $\mathsf{PC}_x(A)$ to describe a resource in an unnamed location, respectively location x, of 'type' PC (e.g. a computer) whose contents satisfy A. We can then write $\mathsf{PC}(\top) \otimes \mathsf{PC}(\top)$ to characterise models with two unnamed PC resources whose contents satisfy the tautological formula (i.e., with anything inside). Using named locations, as e.g. in $\mathsf{PC}_a(\top) \otimes \mathsf{PC}_b(\top)$, we are able to express name separation, i.e., that names a

and b are different. The logic is also so expressive to force name-sharing between resources with formulae like:

$$\mathsf{PC}_a(\mathsf{In}_c(\mathbf{1}) \otimes \top) \overset{c}{\otimes} \mathsf{PC}_b(\mathsf{Out}_c(\mathbf{1}) \otimes \top)$$

This describes two PC with different names, a and b, sharing a link on a distinct name c, which models, e.g., a communication channel. Name c is used as input for the first PC and as an output for the second PC.

A bigraphical structure is, in general, a context with several holes and open links that can be filled by composition. This means that the logic can describe contexts for resources at no addition cost. We can then express formulae like $\mathsf{PC}_a(\top \otimes \mathsf{HD}(id_1 \wedge A))$ that describes a modular PC, where id_1 represents a 'pluggable' hole (e.g. some disk space in PC's hard disk). Contextual resources have many important applications. In particular, the contextual nature of bigraphs is useful to specify reaction rules to deal with dynamics, but it can also be used as a general mechanism to describe contexts of bigraphical (bigraph-shaped) data structures (cf. [14]).

Bigraphs are establishing themselves a truly general (meta)model of global systems, and appear to encompass several existing calculi and models (cf. [22, 20, 28]). *BiLog*, our bigraph logic, aims at achieving the same generality as a description language: as bigraphs specialise to particular models, we expect BiLog to specialise to powerful logics on these. The main technical results of [16] are the encoding in BiLog fragments of the static spatial logics of [7], [10] and [8]. In this sense, the contribution of [16] is to propose BiLog as a unifying language for the description of global resources. We are currently exploring this path, fortified by the positive preliminary results obtained for semistructured data [14].

Dynamics. The main aim of [15] and [16] is to show the expressive power of BiLog in describing static structures. In some cases, BiLog is however able to deal with the dynamic behaviour of the model also [15]. Essentially, this happens thanks to the contextual nature of the logic that can be used to characterise structural parametric reaction rules.

In process algebras the dynamics is often presented by *reaction* (or rewriting) rules of the form $r \rightarrow r'$, meaning that r (the *redex*) is replaced by to r' (the *reactum*) in *suitable* contexts, named *active*. A *bigraphical reactive system* [26] is a system provided with a set of parametric reaction rules, i.e., a set S of couples (R, R'), where the bigraphs R and R' are the redex and the reactum of a parametric reaction. Intuitively, we say that a bigraph g reacts to g' (and we write $g \rightarrow g'$) if there is a couple $(R, R') \in S$, and a bigraphical structure $G(\,)$ such that $g = G(R)$ and $g' = G(R')$.

When the model is enriched with a dynamical framework, it is natural to enrich the logic in order to catch the temporal evolution of its model. The usual way is to introduce a modality $\Diamond$ (the *next step modality*), and extend the forcing relation by defining "$g \models \Diamond A$ *iff* $g \rightarrow g'$ *and* $g' \models A$." In several cases, notably the bigraphical system describing CCS [29], we know that such operator can be expressed directly by using the static fragment of BiLog [15]. This happens because BiLog is *intensional*: in some cases it can fully describe the structure of bigraphs. Even more interesting is the relation between activeness of controls and their transparency as it seems related to the intensionality/extensionality of the logic. We are currently investigating a full treatment of dynamics in BiLog, and in particular the encoding of existing logic for concurrency.

An application: Semistructured data. In [14] we focus on the applications of BiLog to semistructured data, XML in particular. XML data are essentially tree-shaped resources, and have been modelled with unordered labelled tree (cf. [9]). The work in [14] enriches over such model of tree-shaped data by adding links on resource names, to obtain a more general model for semistructured data and XML. In addition, bigraphs naturally model XML contexts: we thus obtained, with no additional effort, a logic to describe XML contexts which can be interpreted as web services or XML transformations. In particular, we first show how XML data (and, more generally, contexts or positive web services) can be interpreted as a bigraph. Equipped with such 'bigraphical' representation of XML data and contexts, we then give a gentle introduction to different fragments of BiLog and show how they can be applied to describe and reason about XML. The contribution of the paper is therefore to identify (fragments of) BiLog as a suitable formalism for semistructured data, and illustrate its expressiveness by means of selected examples.

Some Investigations left open by the thesis

In [16] we moved a first step towards describing global resources by focusing on static bigraphs. An important question remains: as bigraphs have an interesting dynamics, specified using reactions rules, we plan to extend BiLog to such a framework. Building on the encodings of the ambient and the π calculi into bigraphical reactive systems, we expect a dynamic BiLog to be able to express both ambient logic [11] and spatial logics for π-calculus [4]. We obtained a first result in this direction for a fragment of CCS [15]. By using the bigraphical encoding for CCS in [29] we encoded into BiLog a simple dynamical spatial logic [6] suitable to analyse CCS processes.

Moreover the encoding of CCS into bigraphs, and the instantiation of BiLog as a logic for CCS as well, opens the possibility to apply the logic to a non-interference problem studied during the first years of the PhD course. In [2] we consider information flow security in a multilevel system, which aims at guaranteeing that no high level information is revealed to low level users, even in the presence of any possible malicious process. The process calculus we consider is straight derived from CCS. We introduce the notion of *secure contexts for a class of processes.* A context is a process with a variable subprocess (a hole) that can be replaced by any process, in order to characterise the environments in which processes are evolving. The notion of secure context is parametric with respect to both the observation equivalence and the operation used to characterise the low level behaviour of a process. We believe that a "secure" context is a context which cannot change in unpredictable ways, but follows some predetermined rules. These behavioural constraints are reflected in the structure of the context itself. We analysed the secure contexts for some class of processes. Now, our aim is tho exploit the contextuallity of BiLog, and the encoding of CCS, in order to characterise such contexts.

Another possible application for BiLog can be in the software engineering field. In fact the main characteristics of bigraphs are: locality (places), connectivity (links), dynamics (reaction system), and open-endedness. These are the main characteristics of a software architecture. We expect to use BiLog as a powerful language to describe and open-ended software.

References

[1] N. Biri and D. Galmiche. A Separation Logic for Resource Distribution (Extended Abstract). In *Proc. of the 23rd Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS'03)*, LNCS. Springer-Verlag, 2003.

[2] A. Bossi, D. Macedonio, C. Piazza, and S. Rossi. Information flow in secure contexts. *Journal of Computer Security*, 2005. To appear.

[3] T. Braüner and V. de Paiva. Towards constructive hybrid logic (extended abstract). In *Elec. Proc. of Methods for Modalities 3*, 2003.

[4] L. Caires and L. Cardelli. A Spatial Logic for Concurrency (Part I). In N. Kobayashi and B.C. Pierce, editors, *Proc. of 4th International Symposium on Theoretical Aspects of Computer Software (TACS'01)*, volume 2215 of *LNCS*, pages 1–37. Springer-Verlag, Berlin, 2001.

[5] L. Caires and L. Cardelli. A Spatial Logic for Concurrency (Part II). In L. Brim, P. Jancar, M. Kretinsky, and A. Kucera, editors, *Proc. of the 13th International Conference on Concurrency Theory (CONCUR'02)*, volume 2421 of *LNCS*, pages 209–225. Springer-Verlag, Berlin, 2002.

[6] L. Caires and É. Lozes. Elimination of quantifiers and undecidability in spatial logics for concurrency. In P. Gardner and N. Yoshida, editors, *Proceedings of CONCUR*, volume 3170 of *LNCS*, pages 240 – 257. Springer-Verlag, 2004.

[7] C. Calcagno, L. Cardelli, and A. Gordon. Deciding Validity in a Spatial Logic for Trees. In *ACM Sigplan Workshop on Types in Language Design and Implementation (TLDI'03)*. ACM Press, 2003.

[8] C. Calcagno, P. Gardner, and U. Zarfaty. A context logic for tree update. In Proc. of LRPP 2004, revised version to appear in POPL 2005.

[9] L. Cardelli. Describing semistructured data. *SIGMOD Record, Database Principles Column*, 30(4), 2001.

[10] L. Cardelli, P. Gardner, and G. Ghelli. A spatial logic for querying graphs. In *Proc. of ICALP*, volume 2380 of *LNCS*, page 597. Springer-Verlag, 2002.

[11] L. Cardelli and A.D. Gordon. Ambient logic. To appear in Mathematical Structures in Computer Science.

[12] R. Chadha, D. Macedonio, and V. Sassone. A distributed kripke semantics. Computer Science Report 2004:04, University of Sussex, 2004.

[13] R. Chadha, D. Macedonio, and V. Sassone. A hybrid intuitionistic logic: Semantics and decidability. Accepted for publication in the Journal of Logic and Computation, October 2005.

[14] G. Conforti, D. Macedonio, and V. Sassone. Bigraphical logics for XML. In *Proc. of the Thirteenth Italian Symposium on Advanced Database Systems (SEBD)*, 2005.

[15] G. Conforti, D. Macedonio, and V. Sassone. BiLog: spatial logics for bigraphs. Computer Science Report 2005:02, University of Sussex, 2005.

[16] G. Conforti, D. Macedonio, and V. Sassone. Spatial logics for bigraphs. In *Proc. of Int. Colloquium on Automata, Languages and Programming (ICALP)*, 2005.

[17] M. Donolato. Forthcoming Master Thesis. Università di Padova. Supervisor: Prof. G. Sambin. Supporting Supervisor: D. Macedonio, March 2005.

[18] J.Y. Girard. Linear Logic. *Theoretical Computer Science*, 50(1):1–120, 1987.

[19] J.Y. Girard. *Proofs and Types*. Cambridge University Press, 1989.

[20] O.H. Jensen. Forthcoming PhD Thesis. Aalborg University, 2004.

[21] O.H. Jensen and R. Milner. Bigraphs and transitions. In *Proc. of the 30th ACM SIGPLAN-SIGACT symposium on Principles of programming languages*, pages 38–49. ACM Press, 2003.

[22] O.H. Jensen and R. Milner. Bigraphs and mobile processes (revised). Technical Report UCAM-CL-TR-580. University of Cambridge, February 2004.

[23] L. Jia and D. Walker. Modal proofs as distributed programs (extended abstract). In D. Schmidt, editor, *Proc. of the European Symposium on Programming (ESOP04)*, number 2986 in LNCS, pages 219–233. Springer-Verlag, 2004.

[24] S.A. Kripke. Semantical analysis of intuitionistic logic, I. In *Proc. of Logic Colloquium, Oxford, 1963*, pages 92–130. North-Holland Publishing Company, 1965.

[25] D. Macedonio and G.Sambin. Relational Semantics for Basic Logic. *The Journal of Symbolic Logic*. To appear.

[26] R. Milner. Bigraphical reactive systems. In *Proc. of the 12th International Conference on Concurrency Theory*, volume 2154 of *LNCS*, pages 16–35. Springer, 2001.
[27] R. Milner. Axioms for bigraphical structure. Technical Report UCAM-CL-TR-581. University of Cambridge, February 2004.
[28] R. Milner. Bigraphs for petri-nets. In *Lectures on Concurrency and Petri Nets: Advances in Petri Nets*, pages 686–701. Springer, 2004.
[29] R. Milner. Pure bigraphs. Technical Report UCAM-CL-TR-614. University of Cambridge, January 2005.
[30] J. Moody. Modal logic as a basis for distributed computation. Technical Report CMU-CS-03-194, Carnegie Mellon University, 2003.
[31] T. Murphy, K. Crary, R. Harper, and F. Pfenning. A symmetric modal lambda calculus for distributed computing. In *Proc. of the 19th Symposium on Logic in Computer Science (LICS'04)*, 2004. To appear.
[32] P.W. O'Hearn and D.J. Pym. The Logic of Bunched Implications. *Bulletin of Symbolic Logic*, 5(2):215–244, 1999.
[33] P.W. O'Hearn, J. Reynolds, and H. Yang. Local Reasoning about Programs that Alter Data Structures. In *Proc. of the 15th Int. Workshop on Computer Science Logic (CSL'01)*, volume 2142 of *LNCS*, pages 1–19. Springer-Verlag, 2001.
[34] H. Ono and N.-Y. Suzuki. Relations between intuitionistic modal logics and intermediate predicate logics. *Reports on Mathematical Logic*, 22:65–87, 1988.
[35] D.J. Pym. *The Semantics and Proof Theory of the Logic of Bunched Implications.*, volume 26 of *Applied Logic Series*. Kluwer Academic Publishers, 2002.
[36] J. Reynolds. Separation Logic: a Logic for Shared Mutable Data Structures. In *Proc. of the 17th Annual IEEE Symposium on Logic in Computer Science (LICS'02)*, pages 55–74. IEEE Computer Society Press, 2002.
[37] G. Sambin, G. Battilotti, and C. Faggian. Basic Logic: Reflection, Symmetry, Visibility. *Journal of Symbolic Logic*, 65:979–1013, 2000.
[38] A. Simpson. *The Proof Theory and Semantics of Intuitionistic Modal Logic*. PhD thesis, University of Edinburgh, 1994.

Structure of the dissertation

Title: '*Logics for Distributed Resources.*'

(1) *Introduction to Logic.* (cf. [17, 25])
   (a) Basic Logic and its extensions.
   (b) Relational semantics [25] for Basic Logic and its extensions: soundness, refined completeness and semantical cut elimination.
   (c) Simplified semantics for Intuitionistic Logic [17]

(2) **BI**, *a logic for compoundable resources.*
   (a) Introduction of **BI** by following the principle of reflection.
   (b) Relational semantics for **BI** and semantical cut elimination.
   (c) Preordered monoids as models for **BI**: completeness constructive proof.

(3) *Intuitionistic Modal Logic, for distributed resources.* (cf. [12, 13])
   (a) Introduction of places in the logic.
   (b) Distributed Kripke models: soundness and completeness [12].
   (c) Birelational models: finite model property and decidability [13].

(4) *BiLog, a logic for structured and dynamic resources.* (cf. [14, 15, 16])
   (a) Introduction of Bigraphs as a (meta-)model of global systems.
   (b) Introduction of BiLog and its semantics [16].
   (c) Encoding of fragments of spatial logics into BiLog [15, 16].
   (d) Dynamics in BiLog, a result with CCS calculus (cf. [15])
   (e) Application of BiLog (XML [14]):

Publications during the PhD course

Journal Papers.

- R. Chadha, D. Macedonio and V. Sassone. *A Hybrid Intuitionistic Logic: Semantics and Decidability.* Accepted for publication in the Journal of Logic and Computation, October 2005.
- A. Bossi, D. Macedonio, C. Piazza and S. Rossi. *Information Flow in Secure Contexts.* Journal of Computer Security. IOS Press.
- D. Macedonio and G.Sambin. *Relational Semantics for Basic Logic.* Under publication in the Journal of Symbolic Logic.

Conference Proceedings.

- G. Conforti, D. Macedonio and V. Sassone. *Spatial Logics for Bigraphs.* Proc. of Int. Colloquium on Automata, Languages and Programming (ICALP), 2005.
- G. Conforti, D. Macedonio and V. Sassone. *Bigraphical Logics for XML.* Proc. of the Thirteenth Italian Symposium on Advanced Database Systems (SEBD), 2005.
- A. Bossi, R. Focardi, D. Macedonio, C. Piazza, and S. Rossi. *Unwinding in Information Flow Security.* In Proc. of Workshop MEFISTO, ENTCS, Elsevier Sciences, 2004.
- A. Bossi, D. Macedonio, C. Piazza, and S. Rossi. *Information Flow Security and Recursive Systems.* In Proc. of the Italian Conference on Theoretical Computer Science (ICTCS '03). October 2003.
- A. Bossi, D. Macedonio, C. Piazza, S. Rossi. *Secure Contexts for Confidential Data.* In Proc. of the 16th IEEE Computer Security Foundations Workshop (CSFW '03), September 2003.

- A. Bossi, D. Macedonio, C. Piazza, and S. Rossi. *Secure Contexts (Extended Abstract).* In Electronic Proceedings of the Workshop on Issue in the Theory of Security (WITS'03), April 2003.

Technical Reports.

- G. Conforti,D. Macedonio and V. Sassone. *BiLog: spatial logics for bigraphs.* Computer Science Report 2005:02, University of Sussex, 2005.
- R. Chadha, D. Macedonio and V. Sassone. *A Distributed Kripke Semantics.* Computer Science Report 2004:04, University of Sussex, 2004.
- A. Bossi, D. Macedonio, C. Piazza, and S. Rossi. *Compositional Action Refinement and Information Flow Security.* Technical Report CS-2003-13, Dipartimento di Informatica, Università Ca' Foscari di Venezia, August 2003.
- A. Bossi, D. Macedonio, C. Piazza, and S. Rossi. *P_BNDC and Replication.* Technical Report CS-2003-6, Dipartimento di Informatica, Università Ca' Foscari di Venezia, April 2003.
- A. Bossi, D. Macedonio, C. Piazza, and S. Rossi. *Secure Contexts for Information Flow Security.* Technical Report CS-2002-18, Dipartimento di Informatica, Università Ca' Foscari di Venezia, December 2002.