Ph. D. in Computer Science (XVII Ciclo) 3rd Year Report

Damiano Macedonio

Dipartimento di Informatica, Università Ca' Foscari di Venezia
via Torino 155, 30172 Venezia, Italy
mace@dsi.unive.it

1 Thesis's Objectives

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 and/or using such resources, as well as the need of design and implementation tools, will raise to an increasing prominent role. This prefigures exciting future perspectives, but it poses enormous challenger to computer science. Innovative paradigms for information processing and task coordination are required. In fact, traditional correctness properties and methodologies for sequential systems are no more applicable in presence of distributed and mobile systems. 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 recently recognizee by several authors (e.g., [11, 26, 28]).

Following the traditional approaches, properties of concurrent systems and distributed resources can be expressed in terms of *semantics* (e.g. *behavioural equivalences* [24]), *logics* [1, 10, 21, 31, 33], or *types* [25]. We propose to study semantic characterisations of distributed systems which are suitable to analyse processes in heterogeneous environments. Our purpose is to specify a logical/formal tool to characterise concurrent systems. A logical formalism should simplify the definition of properties for a distributed system. A logical formula defines a property which assumes meaning in a defined model. On the one hand a formula can detect a class of processes, the processes that enjoys that property [2]. On the other hand a formula can model directly the observed properties of resources in a distributed system [21, 31, 33].

Moreover the logical framework 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.

Our principal intention is to play on logic, to describe process and resources behaviour. A possibly title for our project could be: "A logical framework to deal with concurrency in heterogeneous systems".

2 Obtained Results

In order to develop a logical framework exploiting 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 introduce a pure logical framework suitable to characterise heterogeneous environments.
2. *Model theoretical approach*: define a logical calculus by considering a formalisation for distributed systems as a model, and interpret the new logical constructs in such model.

On the one hand, we identified a group of candidate languages suitable for developing the first point. They could be

- *Spatial Logic* [2, 3], which provides a powerful language to formally describe the structure of concurrent processes.
- *Bunched Implication* [31] or *Separation Logic* [1, 33], which provide a powerful language to describe the distribution of resources in distributed systems.
- *Modal Intutitionistic Logic* [21, 29, 30], in which the modalities are not interpreted *temporarily*, but *spatially*.

On the other hand, the range of process calculi to choose as a formalism for distributed system is wide. We focus on *Bigraphs* [26], which are establishing themselves a truly general (meta)model of global systems, and appear to encompass several existing calculi and models, like pi-calculus [20], ambients [18], and Petri-nets [27]. A logic found on bigraphs aims at achieving the same generality as a description language: as bigraphs specialize to particular models, we expect BiLog to specialize to powerful logics on these, e.g., spatial logic [3] for π-calculus and ambient logic [10] for ambients.

The following sections present a general overview of the work I did during the third year of my PhD, for more detailed explanations we refer to the quoted manuscripts [13–15].

2.1 Proof Theoretical Approach

The first logical formalism we considered is Separation Logic [32, 33], initially introduced to support compositional reasoning about sequential programs which manipulate pointers. Separation logic introduced the novel logical operation $\varphi * \psi$ (*separating conjunction*) that asserts that φ and ψ are formulae that hold for *disjoint* portions of the addressable storage. The prohibition of sharing is built into the operation.

The logic of Bunched Implications, **BI** [31], 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 modeled with a *commutative preordered monoid*, useful to obtain a Kripke-style semantics which freely combines multiplicative (intuitionistic linear) and additive (intuitionistic) connectives.

We studied the connection of **BI** with its principal constituents: Linear Logic (**LL**) [16] and Intuitionistic Logic (**IL**). They different 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.

We also compared **BI** with Basic Logic (**BL**) [34], that is the common core between **LL** and **IL**. 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* $\varphi \,\&\, \psi \vdash \mu$. By following the lines of [34], the *principle of reflection* in particular, we introduced a new calculus equivalent to **BI** and that does not use 'bunches' (i.e., two ways of composing formulae in contexts). I am currently working on a report that introduces **BI** in a natural way by using such calculus.

From a semantical point of view, we extended the work in [23] with a refined completeness theorem, which enables a semantical *cut elimination* proof. It is possible to extend the semantics of Basic Logic, i.e., relational monoids [23], in order to obtain a complete model for **BI**. It is sufficient to add two properties, that correspond to ask for two well defined implications: the one is linear and the other intuitionistic. We defined two properties to require for the relational monoids in order to obtain a completeness theorem for **IL** and **ILL**. We obtained the *semantical diamond* of Fig. 2.1: by starting from **BL**, we can obtain **ILL** by requiring a multiplicative implication ($\multimap$), **IL** by requiring an additive implication ($\rightarrow$), and finally **BI** by requiring both the implications.

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 only a 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 [10]. We preferred to focus on a weaker logic, by considering a modal intuitionistic logic [35] in which the modalities $\Box\varphi$ (always) e $\Diamond\varphi$ (in the future) are not interpreted *temporarily* any more, but *spatially*. We interpret them as *everywhere* and *somewhere*. Recently, many authors have moved in this direction [21, 29, 30]: intuitionistic modal logics are used as foundations of type systems by exploiting the *propositions-as-types, proofs-as-programs* paradigm [17]. An instance of this was introduced in [21], and we focused our study on the logic introduced there.

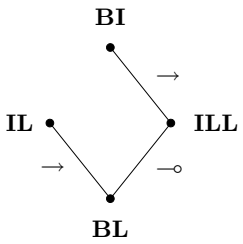

Fig. 1. Semantical diamond.

Formulae in such a logic 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 [21], whose judgements 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 [21], 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 [13] we bridged the gap by presenting a Kripke-style semantics [22] for the logic of [21]. We extended the Kripke semantics of the intuitionistic logic [22], 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 [22]. The enrichment of the model with places reveals the true meaning of the modalities in the logic. The modality $@p$ expresses a property in a named place, $\Box$ corresponds to a weak form of universal quantification and expresses a common property, and $\Diamond$ corresponds to a weak form of existential quantification and expresses a property valid somewhere in the system.

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. As in intuitionistic logic [22], we need not evaluate all the formulae of the language, since the interpretation follows inductively the structure of formulae.

We are considered several extensions of the logic. A major limitation of the logic presented in [21] 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 inaccessibility of places and we reached the well known intuitionistic modal setting [35].

By means of a counter example, we proved that the distributed Kripke model presented in [13] does not enjoy of the finite model property. We refined such model by introducing a *bi-relational model* [35] and we are confident that it is the right model to prove the finite model property. We are investigating in this sense.

The finite model property for the logic will imply the *decidability* of the logic, hance we could use such a logic to solve *query* in a distributed system, e.g., a P2P distributed database to address query such as "Is there such an information?", "Where are these data stored?" and so on...

2.2 Model Theoretical Approach

To describe and reason about structured, distributed, and dynamic resources is one of the main goal of global computing research. Recently, many *Spatial Logics*, in different contexts, have been studied to fulfill this goal. The term 'spatial', as opposed to 'temporal', refers to the use of modal operators inspecting the spatial structure of the model. Spatial logics are usually equipped with a separation/composition binary operator that *splits* the current model into two parts, in order to 'talk' about them separately. Looking closely, we observe that notion of *separation* is interpreted differently in different logics.

- In 'separation' logics [32, 33], the separation is used to reason about dynamic update of heap-like structures, and it is *strong* in that it forces names of resources and pointers in separated components to be disjoint. As a consequence of this constraint, model composition is usually partially defined.
- In static spatial logics (e.g. for trees [4], graphs [7] or trees with hidden names [8]), the separation/composition operator is *structural*, and it is used to describe properties of the underlying structure. In this case no constraint on the model is usually required, and *names* may be shared between separated parts.
- In dynamic spatial logics (e.g. for ambients [10] or π-calculus [2]), the separation is intended only for location in space, and names can be shared between separated resources.

Context tree logic, recently introduced in [5], integrates the first approach above with spatial logics for trees. The resulting logic is able to express properties of tree-shaped structures (and contexts) with pointers, and it is used as an assertion language for Hoare-style program specifications in a tree memory model.

Bigraphs [20, 26] are an emerging model for structures in global computing, which can be instantiated to model several well-known examples, including the

π-calculus [19, 20], the ambient calculus [18] and Petri nets [27]. Specifying a set of reaction rules between bigraphs (of a certain signature) we can define a Bigraphical Reactive Systems (BRS). BRS can model several calculi, included pi-calculus and ambient calculus. Based on categorical construction BRS induce a labelled transition system with ground bigraphs as states and contextual bigraphs as labels.

Bigraphs consist essentially of two graphs sharing the same nodes, which have a *control* for specifying their nature or behavior. 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 hypergraph 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 make clear the difference between 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 the 'strong' version of separation for general bigraphs.

In [15], we build on such bi-structural nature to introduce a '*contextual 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 name the formalism *Bilogic*.

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. By using link expressions in the logic, we can also force name-sharing between resources with formulae like:

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

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. Contextual resources have many important applications. In

particular, the contextuality of bigraphs is useful to specify reaction rules, 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. [20, 18, 27]). *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 result of [15] is the encoding in BiLog of the spatial logics of [4] and [5]. In this sense, the contribution of [15] is to propose BiLog as a unifying language for the description of global resources. We will explore this path in future work, fortified by the positive preliminary results obtained for semistructured data [14].

XML data are essentially tree-shaped resources, and have been modelled with unordered labelled tree in [6] where an important connection between semistructured data and mobile ambients was uncovered. Starting from [6]., several works on spatial logic for semistructured data and XML have been proposed (e.g. [7, 8]). Among these, a query language on semistructured data based on Ambient Logic was studied in [9]. The work in [14] enriches over such model of tree-shaped data by adding links on resource names, so as to obtain a more general model for semistructured data and XML. A similar step was taken in [12], which we improved upon by making use of the well-studied categorical structure of bigraph, which internalise the notion of link and makes the difference between strong and structural separation explicit. 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 [14] we focus on the applications of bigraphical logics to XML data. 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 Bilogic and show how they can be applied to describe and reason about XML. The contribution of the paper is therefore to identify (fragments of) Bilogic as a suitable formalism for semistructured data, and illustrate its expressiveness by means of selected examples.

3 Future Work Organization

In order to complete the work we described previously, an extension to my PhD is needed. The first (proof theoretical) approach is almost accomplished, the second one (bigraphs) needs further investigations. The work program for the next future can be divided in two tasks.

Task 1. Complete the proof of the finite model property for the modal intuitionistic logic of [21], and conclude the decidability. This task is almost completed. I am currently working on a Technical Report of the University of Sussex that I plain to conclude by next December.

Task 2. In [15] we moved a first step towards describing global resources by focusing on static bigraphs. We aim at a decidable logic hence we are working on extending the result of [4], and we are isolating decidable fragments of BiLog. Moreover, in order to compare BiLog with other spatial logics thoroughly (e.g., [3]), we are developing a sequent calculus.

Several important questions remain: 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 [10] and spatial logics for π-calculus [2].

Publications

Journal Papers

- A. Bossi, D. Macedonio, C. Piazza and S. Rossi. *Information Flow in Secure Contexts*. To appear in Journal of Computer Security. IOS Press.
- D. Macedonio and G.Sambin. *Relational Semantics for Basic Logic*. To appear in The Journal of Symbolic Logic.

Conference Proceedings

- A. Bossi, R. Focardi, D. Macedonio, C. Piazza, and S. Rossi. *Unwinding in Information Flow Security*. I n Proc. of Workshop MEFISTO, ENTCS, Elsevier Sciences, 2004. To appear.
- 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.
- 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. *Information Flow Security and Recursive Systems*. In Proc. of the Italian Conference on Theoretical Computer Science (ICTCS '03). October 2003.

Technical Reports

- 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. Extended version of the paper that has appeared in Proc. WITS'03.
- 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. Extended version of the paper that has appeared in Proc. ICTCS'03
- 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.

Manuscripts

- `http://www.dsi.unive.it/~mace/dll.pdf`
  R. Chadha and D. Macedonio and V. Sassone. *A Distributed Kripke Semantics*. To appear as Technical Report of the University of Sussex, UK.
- `http://www.di.unipi.it/~confor/publications.html`
  G. Conforti, D. Macedonio, and V. Sassone. *Bigraphical Logics for XML*. Submitted to PlanX 2005.
- `http://www.di.unipi.it/~confor/publications.html`
  G. Conforti and D. Macedonio and V. Sassone. *BiLogics: Spatial-Nominal Logics for Bigraphs (Extended Abstract)*. Submitted to ESOP 2005.

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. 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.
3. 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.
4. 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.
5. 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.
6. L. Cardelli. Describing semistructured data. *SIGMOD Record, Database Principles Column*, 30(4), 2001.
7. 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.
8. L. Cardelli, P. Gardner, and G. Ghelli. Manipulating trees with hidden labels. In *Proc. of FOSSACS '03*, volume 2620 of *LNCS*, pages 216–232. Springer-Verlag, 2003.
9. L. Cardelli and G. Ghelli. TQL: a query language for semistructured data based on the ambient logic. *Mathematical Structures in Computer Science*, 14:285–327, 2004.
10. L. Cardelli and A.D. Gordon. Ambient logic. To appear in Mathematical Structures in Computer Science.
11. L. Cardelli and A.D. Gordon. Mobile Ambients. *Theoretical Computer Science, Special Issue on Coordination*, 240(1):177–213, 2000.
12. L. Cardelli, P.Gardner, and G. Ghelli. Querying trees with pointers. Manuscript.
13. R. Chadha, D. Macedonio, and V. Sassone. A distributed kripke semantics. Manuscript, June 2004.
14. G. Conforti, D. Macedonio, and V. Sassone. Bigraphical logics for XML. Manuscript, October 2004.

15. G. Conforti, D. Macedonio, and V. Sassone. Bilogics: Spatial-nominal logics for bigraphs (extended abstract). Manuscript, October 2004.
16. J.Y. Girard. Linear Logic. *Theoretical Computer Science*, 50(1):1–120, 1987.
17. J.Y. Girard. *Proofs and Types*. Cambridge University Press, 1989.
18. O.H. Jensen. Forthcoming PhD Thesis. Aalborg University, 2004.
19. 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.
20. O.H. Jensen and R. Milner. Bigraphs and mobile processes (revised). Technical Report UCAM-CL-TR-580. University of Cambridge, February 2004.
21. 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.
22. S.A. Kripke. Semantical analysis of intuitionistic logic, I. In *Proc. of Logic Colloquium, Oxford, 1963*, pages 92–130. North-Holland Publishing Company, 1965.
23. D. Macedonio and G.Sambin. Relational Semantics for Basic Logic. *The Journal of Symbolic Logic*. To appear.
24. R. Milner. *Communication and Concurrency*. Prentice-Hall, 1989.
25. R. Milner. Sorts in the π-calculus (Extended Abstract). In E. Best and G. Rozenberg, editors, *Proc. of the 3rd Workshop on Concurrency and Compositionality*, volume 191 of *GMD-Studien*. GMD, Bonn, 1991. Also avaible as Report 6/91 from University of Hildesheim.
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. Bigraphs for petri-nets. In *Lectures on Concurrency and Petri Nets: Advances in Petri Nets*, pages 686–701. Springer, 2004.
28. R. Milner, J. Parrow, and D. Walker. Calculus of Mobile Processes, parts I and II. *Information and Computation*, 100(1):1–77, 1992.
29. J. Moody. Modal logic as a basis for distributed computation. Technical Report CMU-CS-03-194, Carnegie Mellon University, 2003.
30. 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.
31. P.W. O'Hearn and D.J. Pym. The Logic of Bunched Implications. *Bulletin of Symbolic Logic*, 5(2):215–244, 1999.
32. 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.
33. 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.
34. G. Sambin, G. Battilotti, and C. Faggian. Basic Logic: Reflection, Symmetry, Visibility. *Journal of Symbolic Logic*, 65:979–1013, 2000.
35. A. Simpson. *The Proof Theory and Semantics of Intuitionistic Modal Logic*. PhD thesis, University of Edinburgh, 1994.