DELIVERABLE SUMMARY SHEET

Project Number:	IST-2001-33100
Project Acronym:	PROFUNDIS
Title :	Proofs of Functionality for Mobile Distributed Systems

Deliverable N. :	4
Due Date :	
Delivery Date :	

Partners Owning:	Fundação Fac. Ciências e Tecnologia, UNL, Portugal
Partners contributed :	FFCT, INRIA, Pisa
Made available to:	

1 Summary

The objectives of Workpackage 2 are to develop new logics to support the specification and verification of structural and behavioural properties of concurrent mobile systems, and to develop proof systems for those logics. This deliverable describes the scientific contributions of the first year for WP2 and includes the contributed papers as appendices. In summary, the scientific contributions are the following:

- Spatial logics for pi-calculi, that can describe not only behavioural properties, but also other key features of modern distributed systems (*e.g.,* resource control, distribution, and secrecy).
- Study of fundamental meta-theoretic properties of spatial logics for ambient and pi-calculi (*e.g.,* expressiveness, separation).
- Logics for semi-structured data and related decision procedures.
- Logical formalization of the secure composition of web services.

2 Contributions

We present the contributions per task of the workpackage.

Task 2.1: Logics for systems with spatial and temporal structure

This task concerns the development of logics to specify and verify, in an integrated way, both behavioural and structural properties of concurrent systems based on mobile process calculi.

Base logics In collaboration with Cardelli at Microsoft Research Cambridge, Lisbon introduced a spatial logic to describe and verify properties of concurrent systems specified in the pi-calculus [CC02a] (see Appendix 2.1.1). This logic allows the specification of spatial and behavioural properties by induction and co-induction (for instance, properties related to resource usage), and includes freshness and hidden name quantifiers (important to define secrecy and non-interference properties). A related logic and model-checker for the pi-calculus with recursion, based on a small set of structural behavioural and spatial observations, is currently under development in Lisbon [Cai02] (see Appendix 2.1.2).

The introduction of spatial logics as a foundation for query and programming languages for semistructured data (XML-like) has also been advocated recently; Inria (through the subsite LIF, Marseille), introduced new logics TL and SL to describe and query semi-structured data represented by multitrees [LZ02a, LZ02b] (see Appendices 2.1.3 and 2.1.4), and can embed XML Schema as a plain subset.

Pisa has applied a logic that combines modalities with a notion of type to formalize the secure composition of web services [BBFT02] (see Appendix 2.1.5). By its use of types, this work is also part of the WP3 deliverable.

Proof systems In collaboration with Cardelli at Microsoft Research Cambridge, Lisbon defined a sequent calculus based proof-system [CC02b] (see Appendices 2.1.6 and 2.1.7) for the spatial logic of [CC02a]. This proof system combines good proof-theoretic properties (*e.g.*, cut-elimination) and direct applicability to concurrency, it was proposed for the asynchronous pi-calculus, but the general techniques adopted are easily generalizable to the case of other nominal calculi.

Inria (through the subsite LIF, Marseille), introduced decision procedures for satisfaction and model-checking the query languages logics TL and SL againts formal representations of semi-structured documents [LZ02a, LZ02b], that also studies the complexity of the associated problems. This work builds upon new notions of tree- and sheaves-automata, which are tailored versions of automata for unranked trees with both associative and associative-commutative symbols.

Verification framework This topic was not expected to be substantially addressed during Year 1. Lisbon developed some preliminary work on the development of techniques of equational reasoning on pi-algebras, having in mind the development of specific techniques for (partially) mechanizing theorem proving in spatial logics.

Task 2.2: Expressiveness

This task focus on accessing the expressiveness of the base logics and in the identification of suitable high-level extensions. Although scheduled to start on the second year, some results have already been obtained in the first year.

Inria (through the subsite ENS, Lyon), have developed a work started by Sangiorgi on the expressive power of the Ambient Logic [HLS02] (see Appendix 2.2.1). They established several expressiveness and separation results in the case where we also consider in the underlying calculus the presence of the replication operator, that leads to possibly infinite behaviours and spatial decompositions.

Ongoing work also by the Lyon team currently studies the spatial logic for the pi-calculus developed in [CC02a], trying to establish meta-theoretical properties about the expressive power of the spatial adjuncts, that, as the work of [HLS02] on the Ambient Logic testifies, turns out to be quite powerful.

Task 2.3: Tools and case studies

This task concerns the implementation of verification tools for the logics, no significant results can be reported here at the present moment.

References

[BBFT02] A. Bracciali, A. Brogi, G. Ferrari, and E. Tuosto. Security and dynamic composition of open systems. In *Proc. Int. Conference on Parallel and Distributed Techniques and applications*, USA, 2002. CSREA Press.

[Cai02] L. Caires. Model-checking of spatial properties in the pi-calculus. Research report 3, DI/FCT/UNL, December 2002.

[CC02a] L. Caires and L. Cardelli. A spatial logic for concurrency (part i). *Information and Computation*, 2002. Accepted for publication.

[CC02b] L. Caires and L. Cardelli. A spatial logic for concurrency (part ii). In *CONCUR 2002: Concurrency Theory (13th International Conference)*, Berlin, 2002. Lecture Notes in Computer Science. Springer-Verlag. Also as Technical Report 3/2002/DI/PLM/FCTUNL.

[HLS02] D. Hirschkoff, E. Lozes, and D. Sangiorgi. Separability, Expressiveness and Decidability in the Ambient Logic. In *Proc. of LICS'02*, 2002.

[LZ02a] Denis Lugiez and Silvano Dal Zilio. Multitrees Automata, Presburger's Constraints and Tree Logics. Research report 08-2002, LIF, Marseille, France, June 2002. http://www.lim.univ-mrs.fr/Rapports/08-2002-Lugiez-DalZilio.html.

[LZ02b] Denis Lugiez and Silvano Dal Zilio. XML Schema, Tree Logic and Sheaves Automata. Research report 4631, INRIA, November 2002. http://www.inria.fr/rrrt/rr-4631.html.

WP2 Scientific Contributions

APPENDIX

Appendix 2.1.1
L. Caires and L. Cardelli. A Spatial Logic for Concurrency (Part I). Accepted for publication in *Information and Computation*, 2002.

Appendix 2.1.2
Luis Caires. Model-Checking of Spatial Properties in the pi-calculus. Research report 3, DI/FCT/UNL, December 2002.

Appendix 2.1.3
Denis Lugiez and Silvano Dal Zilio. Multitrees Automata, Presburger's Constraints and Tree Logics. Research report 08-2002, LIF, Marseille, France, June 2002.

Appendix 2.1.4
Denis Lugiez and Silvano Dal Zilio. XML Schema, Tree Logic and Sheaves Automata. Research report 4631, INRIA, November 2002 (submitted).

Appendix 2.1.5
A. Bracciali, A. Brogi, G. Ferrari and E. Tuosto. Security and dynamic compositions of open services. In *Proc. Int. Conference on Parallel and Distributed Processing Techniques and Applications (PDTA'02).* CSREA Press, USA, 2002.

Appendix 2.1.6
L. Caires and L. Cardelli. A Spatial Logic for Concurrency (Part II). In *CONCUR 2002: Concurrency Theory (13th International Conference)*, Lecture Notes in Computer Science. Springer-Verlag, 2002.

Appendix 2.1.7
L. Caires and L. Cardelli. A Spatial Logic for Concurrency (Part II). Technical Report 3/2002/DI/PLM/FCTUNL, DI/PLM FCT Universidade Nova de Lisboa, 2002.

Appendix 2.2.1
D. Hirschkoff, E. Lozes, and D. Sangiorgi. Separability, Expressiveness and Decidability in the Ambient Logic. In *Third Annual Symposium on Logic in Computer Science*, Copenhagen, Denmark, 2002. IEEE Computer Society.