DELIVERABLE SUMMARY SHEET

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

Deliverable Number:	6
Due date:	Project month 36
Delivery date:	March 15, 2005

Short Description: Short Description: Extension of model checking for coping with recursive properties. Spatial observations. Spatial logic for quality-of-service properties. Applications to web services and wireless systems. Undecidability of dynamic spatial logics and of model checking with contextual operators. Separation logic and a classical fragment. Extensional spatial logics. Implementation of version 1.0 of the Spatial Logic Model Checker (SLMC). Case study.

Partners owning:	FFCT
Partners contributed:	FFCT, INRIA, PISA
Made available to:	

PROFUNDIS: Third Year Report
Workpackage 2: Specifications
Deliverable 6: High-level extensions, case studies and implementations

Contents

1 Summary

This deliverable describes the scientific contributions of the third year for WP2 and includes the contributed papers as appendices.

The objectives of WP2 for the third year were a final prototype of the proof tool and a collection of case studies. These objectives have been extended to allow for further refinements of the logics, their expressiveness properties and applications.

In summary, the scientific contributions are the following:

- Version 1.0 of the Spatial Logic Model-Checker (SLMC), available on the web, extended to cope with recursive properties; case studies.
- Extensional spatial bisimulation based on spatial observations.
- Spatial logic for quality-of-service properties of applications.
- Undecidability of dynamic spatial logics and of model checking with contextual operators.
- Expressiveness results on separation logic and on extensional spatial logics.
- Undecidability results on constraint problems with an open number of variables.

2 Contributions

We present the contributions per task of the workpackage.

Task 2.1: Logics for systems with spatial and temporal structure

A paper on a sequent calculus based proof system for spatial logic was published in a high-quality journal [CC04]. The investigation on decision procedures for model-checking pi-calculus processes against spatial logic properties was extended [Cai04]. In particular, extensions to the mechanisms for coping with recursive properties (both inductive and co-inductive) were devised and implemented. Another line of research, which will still fructify before the end of the project, is the proposal of decidable spatial type systems inspired by spatial logics.

A CCS-like calculus has been defined for which the observations have been enriched with spatial observations, giving rise to models of spatial logic [TV04].

A simple spatial logic that supports specification of quality of service (QoS) properties of applications has been introduced [FLL04]. The evaluation of a formula in the spatial logic is a value of a suitable algebraic structure, a c-semiring, representing the QoS level of the formula and not just a boolean value expressing whether or not the formula holds. Applications of this spatial logic with quantitative information to web services [Mon04] and wireless systems [Tuo04] have been considered.

Task 2.2: Expressiveness

We addressed the difficult problem of decidability of validity in dynamic spatial logics [CL04, CL]. The striking conclusion of this research is that the validity problem for the simplest dynamic spatial logics is undecidable, which entails the undecidability of model-checking of spatial logics with contextual operators (composition adjunct). This research contributed to raise the question of finding expressive and tractable forms of contextual reasoning inspired by the composition adjunct, extending those already provided by the decidable behavioral-spatial logics also investigated in the project.

The comparison between the spatial logics for concurrency and more standard logics has led to the definition of a spatial logic for the π-calculus that is *extensional*, in the sense that the induced logical equivalence coincides with behavioural equivalence on processes [Hir04]. This result shows which subset of spatial logics shares the same separative power as the Hennessy-Milner logic.

Separation logic and a classical fragment of it have been compared and shown to be equally expressive [Loz04b].

The quantifier-free, static fragment of ambient logic, with composition adjunct and iteration, which corresponds to a kind of regular expression language for semistructured data, was proved to be decidable [ZLM04].

A PhD thesis on the expressiveness of spatial logics was concluded [Loz04a].

A framework for specifying constraint problems with an open number of variables was proposed and the decidability of the satisfiability for various families of these problems has been studied [DV04].

Task 2.3: Tools and case studies

Version 1.0 of the Spatial Logic Model Checker (SLMC) was implemented and made available to the community through the web, together with illustrating examples. We also reported on an example of verification of correctness of a distributed protocol using spatial logics with a proof-theoretic approach [RCM04].

3 Publication list

References

[Cai04] L. Caires. Behavioral and spatial properties in a logic for the pi-calculus. In Igor Walukiwicz, editor, *Proc. of Foundations of Software Science and Computation Structures'2004*, Lecture Notes in Computer Science. Springer Verlag, 2004.

[CC04] L. Caires and L. Cardelli. A spatial logic for concurrency–II. *Theor. Comput. Sci.*, 322(3):517–565, 2004.

[CL] Luis Caires and Etienne Lozes. Elimination of quantifiers and undecidability in spatial logics for concurrency. *Theoretical Computer Science*. To appear.

[CL04] L. Caires and E. Lozes. Elimination of quantifiers and undecidability in spatial logics for concurrency. In *Proc. of CONCUR'04*, number 3170 in Lecture Notes in Computer Science, pages 240–257. Springer Verlag, 2004.

[DV04] S. Dantchev and F. Valencia. On infinite CSP's. In *In proceedings of the Third International Workshop on Modelling and Reformulating CSPs*, 2004.

[FLL04] Gianluigi Ferrari and Alberto Lluch-Lafuente. A Logic for Graphs with QoS. In *First International Workshop on Views On Designing Complex Architectures*, Electronic Notes in Computer Science, Bertinoro, Italy, September 2004. Elsevier. To appear.

[Hir04] D. Hirschkoff. An extensional spatial logic for mobile processes. In *Proc. of CONCUR'04*, volume 3170, pages 325–339. Springer Verlag, 2004.

[Loz04a] E. Lozes. *Expressivité des logiques d'espaces*. PhD thesis, École Doctorale MathInf, ENS Lyon, 2004.

[Loz04b] E. Lozes. Separation logic preserves the expressive power of classical logic. In *Proc. Workshop Space'04*, 2004. Electronic publication.

[Mon04] Ugo Montanari. Web services and models of computation. In *First International Workshop on Web Services and Formal Methods*, volume 105 of *Electronic Notes in Computer Science*. Elsevier, 2004.

[RCM04] A. Ribeiro, L. Caires, and L. Monteiro. Verifying the Arrow Protocol in a Spatial Logic. Technical Report TR-DI/FCT/UNL-04/2004, Departamento de Informatica, FCT/UNL, 2004.

[Tuo04] Emilio Tuosto. Tarzan: Communicating and Moving in Wireless Jungles. In A. Cerone and Alessandra Di Pierro, editors, *2nd Workshop on Quantitative Aspects of Programming Languages*, volume 112 of *Electronic Notes in Computer Science*, pages 77–94. Elsevier, 2004.

[TV04] Emilio Tuosto and Hugo T. Vieira. An Observational Model for Spatial Logics. In *First International Workshop on Views On Designing Complex Architectures*, ENTCS, Bertinoro, Italy, September 2004. Elsevier. To appear.

[ZLM04] S. Dal Zilio, D. Lugiez, and C. Meyssonnier. A logic you can count on. In *POPL 2004 – 31st Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*. ACM Press, 2004.