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

Deliverable 17: Self Assessment Year 3

Preparation date:	March 14, 2005
Classification:	Public
Contract start date	1 January 2002
Duration:	3 years
Project co-ordinator:	Joachim Parrow
Partners:	Univ. Uppsala, Sweden Univ. Pisa, Italy INRIA, France Univ. FFCT, Portugal

PROFUNDIS Deliverable 17: Self Assessment Year 3

March 14, 2005

1 Executive Summary

The work in PROFUNDIS has been successful in year 3 (2004). An elaboration of what has been accomplished can be found in the Periodic Progress Report (PPR) for year 3. The present document contains a self assessment of our progress.

Overall we are very satisfied with the progress of PROFUNDIS. Scientific goals have been reached with minor exceptions in some details, and in some cases we have gone beyond what was originally planned. The quantitative goals of publications have been exceeded. Case studies and prototypes have progressed well. Several PhD theses are completed or under way. Unsurprisingly there are deviations from the original plan made three and a half years ago; in a basic research endeavour this is to be expected and shows that PROFUNDIS researchers adapt well to new circumstances and discoveries.

2 Overview of the Work Packages

PROFUNDIS consists of three technical Work Packages (WPs) outlined below. A fourth WP is devoted to project management and is given no special consideration in the SEP.

WP1

The objectives of the Work Package consist of the development of a HD-Automata model, suitable for finite-state verification, enhanced with additional capabilities like name fusions and substitutions. Also, versions of mobile calculi should be defined, e.g. for the symbolic analysis of security protocols. A verification environment should be designed and implemented, equipped with a general, open architecture and consisting of new tools realizing the models and the verification methods above. Several case studies should show the flexibility and effectiveness of our approach.

WP2

The objectives of the Work Package are to develop new logics to support the verification of structural (spatial) and behavioural properties of concurrent mobile systems, and to develop proof systems for these logics based on sequent calculi. A tool for the logical framework should be built, integrated in the verification environment developed together with other tasks. The usefulness of the approach should be illustrated by several case studies.

WP3

The objectives are to develop new type systems to control interferences among processes and the resources used by the processes [Task 3.1]; to integrate the type techniques with operational and logic techniques [Task 3.2]; to investigate the robustness of the type techniques and their algorithmic definitions [Task 3.3]; to assess the applicability of the techniques and ideas developed, and use them in implementations [Task 3.4].

3 Self Assessment of Work Package 1

The work on WP1 has progressed essentially according to what has been scheduled in the TA. The third year has been successful for all the tasks. In particular:

- The development of a general framework for the symbolic semantics of nominal calculi based on the notion of reactive systems and borrowed context.
- The development of abstract models for nominal calculi based on categorical notions (functorial semantics).
- The bialgebraic technique has been extended to provide a compositional approach to deal with the observational semantics of nominal calculi with fusions and distinctions.
- A new calculus general fusion and binding mechanisms, which is an extension of both open π-calculus and Fusion Calculus, has been defined.
- Symbolic techniques which facilitate certification of properties of security protocols have been further developed.
- The Profundis WEB has been designed and several verification toolkits have been made available as Web Services. Some case studies have illustrated the potential of the PWeb to address the issues of toolkit integration and modular verification.

The success of the activities in the third year can be measured in terms of the following facts:

- the work on the Profundis verification environment is a result of collaborations and visits within Profundis;
- the objectives indicated in the TA have been essentially obtained.
- some of the work has been published, and other has been submitted for publication;
- within the Italian Ministry of Research Project *Architetture Software ad Alta Qualità di Servizio per Global Computing su Cooperative Wide Area Networks*, the Pisa Profundis Group, together with the Telecom Italia Lab group, is exploiting some of the toolkits of the PWeb to verify security properties of the PARLAY-X infrastructure.

4 Self Assessment of Work Package 2

The work in WP2 has in the overall progressed according to what has been scheduled in the TA and SEP. According to the TA and SEP, the work to be performed during the third year was:

- Final versions of the spatial logic with high-level extensions and of the prototype of the proof tool.
- A collection of validated case studies.

These objectives have been successfully attained, with two exceptions due to a reevaluation of priorities:

- The work on high-level extensions required further foundational work on logics and some experience with case studies. This topic had to be put on hold for now.
- Instead of the theorem-proving tool it seemed more appropriate to develop first the model-checking tool for the reasons explained below. This tool is currently publicly available on the web.

Furthermore, new logics for different applications continued to be developed and expressiveness properties of several logics have been established.

Our contributions are as follows:

- The investigation on decision procedures for model-checking pi-calculus processes against spatial logic properties was extended. In particular, extensions to the mechanisms for coping with recursive properties (both inductive and co-inductive) were devised and implemented.
- A CCS-like calculus has been defined for which the observations have been enriched with spatial observations, giving rise to models of spatial logic.
- A spatial logic that supports specification of quality-of-service (QoS) properties has been introduced, where formulas have values in c-semirings that represent the QoS level of the formula. Applications to web services and wireless systems have been considered.
- A simple dynamic spatial logic with void, composition, its adjunct and the next step modality was studied from the point of view of its expressiveness. A number of results have been obtained including the undecidability of the model-checking and the satisfiability problems.
- The equivalence of separation logic with a classical fragment of it has been proved.
- A spatial logic for the π-calculus that is extensional in the sense that the induced logical equivalence of processes coincides with the behavioural equivalence, has been defined. This result shows which subset of spatial logics shares the same separative power as Hennessy-Milner logic.

- Version 1.0 of the Spatial Logic Model-Checker is available on the web. Some case studies have been tested and implemented using this tool. Case studies of concurrent systems related to global computing (e.g., peer-to-peer algorithms) were used to test the theorem-proving framework developed for the logic, but no implementation of the framework exists.

An important result of the research conducted in WP2 in Y3 is a proof of the essential undecidability of the purely spatial logics for concurrency. In these logics, contextual properties must be expressed by spatial adjunct operators, which combined with the simplest temporal modalities induce undecidability. This result strengthens the need of investigating fragments (or extensions) of spatial logics where contextual properties might be expressed while preserving computability of model-checking. An example of such a logic is the behavioral-spatial logic incorporated in the Spatial Logic Model Checker. This is a very expressive logic, allowing the specification and (finite state) verification of many interesting spatial and behavioral properties of distributed systems expressed in the π-calculus. On the other hand, purely spatial logics including adjunct operators seem to be more adequate for supporting verification techniques based on proof-theoretic reasoning. The development of such techniques are also among the project goals, but with a lower priority degree, in light of the above remarks.

Given this collection of results, published or accepted for publication in high-quality conferences and journals, and giving rise to a PhD thesis, we think that the success of the activities in the third year is justified by comparing with the objectives indicated in the TA and SEP.

5 Self Assessment of Work Package 3

The plan of work for this year, as written in last year's PPR, was to strengthen the work on applicability of the type systems we have developed, by giving more weight to the corresponding Tasks in the TA (3.3 and 3.4). We were also promising to continue some of the work on Tasks 3.1 and 3.2, although in the TA these tasks were supposed to stop at the end of year 2, because we had found this work more fruitful than expected. We had also promised to maintain a strong publication effort, with 3 papers accepted for publication in good journals by the end of year 3.

Overall, the plan above has been respected. We discuss below the main differences. The effort on the subtask "advanced programming constructs" (Task 3.3) has been bigger than expected. The reason for this is that we have found a number of challenging cases and programming constructs that we thought worth investigating.

We have fewer results than expected when we wrote the TA on the subtasks "Case studies" (Task 3.4), "expressiveness" and "space in types" (Task 3.2), "type inference" (Task 3.3) We did put effort on these topics. We have however encountered unexpected technical difficulties. For instance, on "space in types", Ferrari (Pisa) visited Lisbon, and Hugo Viera (Lisbon) is currently visiting Pisa; both visits has this topic as their main goal. The progress has been slow, and the work remains in its early stage. We were planning to carry our main case studies using the tools, after having enhanced them with type information. Magnus Johansson (UU) has visited Bologna and Pisa, with the objective to work on this topic. Here as well progress has been slow. People in Pisa did some experiments but we have not written any paper on it (basically we have a front-end for MIHDA which exploits a form of type annotation in the generation of the HD automaton). Finally, concerning type inference, some papers on type considers it, but without it as the main objective; we are currently working on problems of type inference and type checking for session types.

We do not regard the above discrepancies as failures because the quality and quantity of our results in the other subtasks are satisfying, sometimes going beyond what was expected.

Concerning publications during year 3, we have had 10 conferences, 3 workshops, and 2 journals. Further, a few have been submitted to journals and conferences. To all this we should add Teller's PhD thesis, that has been discussed during year 3 and whose content belongs entirely to Profundis WP3. Another PhD thesis, namely Deng's, has well advanced; in the light of the technical progresses made this year, Deng has enough results to start the writing of the thesis. A first draft is expected by the end of the project. We should remind that Deng's thesis is funded by Profundis and that Deng started his thesis 8 months after the beginning of the project; hence overall his thesis should be completed within the 3 years, as initially expected.