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

# Deliverable 16: Self Assessment Year 2

| | |
|---|---|
| Preparation date: | January 24, 2004 |
| Classification: | Public |
| Contract start date | 1 January 2002 |
| Duration: | 3 years |
| Project co-ordinator: | Joachim Parrow |
| Partners: | Univ. Uppsala, Sweden<br>Univ. Pisa, Italy<br>INRIA, France<br>Univ. FFCT, Portugal |

# PROFUNDIS Deliverable 16: Self Assessment Year 2

January 24, 2004

## 1 Executive Summary

The work in PROFUNDIS has been successful in year 2 (2003), with only minor deviations from the TA (Technical Annex) and from the criteria established in the Self Evaluation Plan (SEP). An elaboration of what has been accomplished can be found in the Periodic Progress Report (PPR) for year 2. The present document contains a self assessment of our progress in relation to the SEP.

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 by a great margin.

# 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 by means of case studies, and to implement some of the type algorithms and proof techniques.

# 3 Self Assessment of Work Package 1

The work in WP1 has in the overall progressed according to what has been scheduled in the TA and SEP. According to the TA, the work to be performed during the second year was:

- On task 1.1: Definition of an extended version of History Dependent (HD) automata for handling names and substitutions in their full generality.
- On task 1.2: Proof techniques (typically of security protocols) based on symbolic execution.
- On task 1.3: Extending the existing tools to handle the enriched versions of HD-automata.

According to the SEP, the work to be performed during the second year was as follows.

- A symbolic calculus with permutations.
- HD automata with fusions and a first version of a tool for them.
- Spatial logic and a first version of a tool for it.
- Optimized version of the minimization tool for HD automata with permutations.
- Second version of the verification environment architecture (distributed).
- First version of a symbolic interpreter with substitutions.
- Draft of a collection of case studies.

These objectives have been attained in good part, but not completely, as discussed below, due to a reevaluation of priorities. Our contributions are as follows.

- the structure of HD-automata and the minimization algorithm have been formally specified using a polymorphic $\lambda$-calculus with dependent types;
- the category of named sets and named functions, the category of permutation algebras and certain categories of presheaves have been shown essentially equivalent;
- the HD-automata approach has been extended to Parrow and Victor's Fusion Calculus, and the bialgebra approach to Fusion Calculus with explicit fusions. Fusion Calculus has also been also mapped to logic programming clauses;
- a new calculus with two binders, called DFusion, which is an extension of both open $\pi$-calculus and Fusion Calculus, has been defined;

- the symbolic technique of *history-dependent scheduling* has been implemented in the TRUST verifier;
- a "low level" protocol description language has been introduced, together with a notion of symbolic execution;
- a verification methodology based on the notion of symbolic state-space exploration has been developed and implemented in the verification environment called ASPASYA;
- the PROFUNDIS WEB has been designed and several toolkits have been made available on the web. Some services have been described which can be exploited in the verification of mobile systems.

The main difference with respect to plans is that we felt the need to further study the theoretical foundations and their relations with existing work: this accounts for the formal specification with dependent types and for the comparison with categories of presheaves. We also found new results in terms of language expressiveness, which suggested a new interpretation of the extensions, both in terms of fusions and of general substitutions. On the other side, the semantical understanding of models for spatial logics in terms of HD-automata with operations has not been fully developed, even if this year two notes have been produced on a closely related subject and a collaboration between Lisbon and Pisa has started. Moreover, a prototype implementation of a model checking environment for spatial logic has been developed, however it is not fully integrated inside the PWeb. Also the study of logic programming in this context (relevant for the theme of automata with substitutions) was limited to the case of *synchronized* logic programming, which is the natural counterpart of process calculi. As a consequence, we suggested not to consider task 1.1. completed within the second year - as planned in the TA and the SEP - but to extend it until the end of the project.

The number of publications has been close to planned: one on a prestigious journal (TOSEM), four on international conferences (MFCS, FMCO, VMCI, FCE) and one on a national conference (COMETA). In addition, several papers have been submitted for publication.

# 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 second year was:

- On task 2.1: Extensions to the logics with high-level extensions to handle resources, locations, and other non-functional features of processes.
- On task 2.2: Continuation of the investigation of meta-theoretical properties of the spatial logics (expressiveness and decidability).
- On task 2.3: Integration in tools of the logics and algorithms developed in other tasks and analysis of some case studies.

These objectives have been successfully attained, with an exception discussed below due to a reevaluation of priorities, witnessed by the following contributions:

- (T2.1, T2.2) A spatial logic for systems specified in the synchronous Pi-calculus with recursion, based on a small set of behavioral and spatial observations. Expressiveness results for this logic were studied. It is also shown that model-checking in this logic is decidable for a useful class of processes that includes the finite-control fragment of the Pi-calculus.
- (T2.2) Expressiveness and minimality results have been obtained for spatial logics, showing that they can be expressed within a core, calculus-independent, spatial logic. In particular, it has been established that these spatial logics can express potentiality of interaction as they appear in the Hennessy-Milner logic. Minimality has also been addressed for the static Ambient Logic with operator of name revelation and fresh name quantification, in this context it was proved that the spatial adjunct operator can be eliminated in behalf of the remaining connectives without losing expressive power.
- (T2.2) Tree automata were applied to obtain several complexity results related to XML schema, in a tree logic that can be seen as a form of spatial logic. This approach was also applied to derive the decidability of 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.
- A prototype version of a tool for model-checking distributed systems modelled in the pi-calculus against a version of a spatial logic was implemented, and will be made available on the web, and integrated with the PROFUNDIS Verification Environment. Some case studies have been already tested and implemented using this tool. A sound and complete sequent calculus-based proof system for a core spatial logic was developed, and the corresponding decision procedure for validity of formulas has led to a

prototype implementation, to be further developed in the project. Some case studies of concurrent systems related to global computing (e.g., peer-to-peer algorithms) were already used to test the usefulness of the logics developed in PROFUNDIS.

The research conducted in WP2 have lead to a number of publications that fairly exceeded what was initially expected in the SEP: (3 articles in first rate journals, 4 publications in first rate conferences, and two reports).

Given this collection of results, published or accepted for publication in high-quality conferences and journal, we think that the success of the activities in the second year can be justified by comparing with the objectives indicated in the TA and SEP, with one exception. The work planned on high-level extensions to the logics, did not produce significant results yet, due to the identified need of pursuing further foundational work on the logics, and some difficulty of Lisbon on hiring a post doc for the second year of the project (a candidate is already hired for the third year). This delay is not a serious problem, and is in the process of being recovered.

# 5 Self Assessment of Work Package 3

As planned in the TA and SEP, the work in Tasks 3.3 and 3.4 has gained more attention during year 2 than in year 1 (where they were actually not planned to start), while results from Tasks 3.1 and 3.2 have been consolidated and further developed. This shows that, as announced, year 2 is a transition step between some prospective studies (corresponding essentially to Tasks 3.1 and 3.2) and work on the application and scalability of type systems (Tasks 3.3 and 3.4).

In terms of publications, the objectives indicated in TA and SEP have been obtained (most of the results obtained in year 1, as well as some from year 2, are now published). Like in year 1, some results have been obtained through collaborations between PROFUNDIS members or with other projects belonging the GC initiative, on the subject of Work Package 3 (type systems).

An important novelty in year 2 is the beginning of interaction between packages *within* PROFUNDIS (as was planned in the TA and SEP). This interaction was mainly concerned with the addition of types (WP3) to (some of) our tools (WP1), in order to improve performances.

We comment on some points that we did not address the way it was announced in the TA and SEP.

An aspect of type systems that has not been treated yet is the notion of intensional type systems, in relation to the subject of Work Package 2, logics. Contrary to what was planned, there has been no result yet corresponding to the entry *'Space in types'* of Task 3.2, and collaboration between WP2 and WP3 has been less active than expected. Possible explanations for this are:

- The novelty of spatial logics, that makes them difficult to integrate with a type system. Recent results in the field (including those obtained in WP2) give us a better view on properties related to expressive power and decidability, which should help in understanding how ideas or constructs borrowed from spatial logics can be associated to a more traditional type system.

- The priority for WP2, as far as interactions are concerned, is the development of automated support for spatial logics, in order to assess their practicability.

We still believe, however, that the entry *'space in types'* is interesting and deserves a research effort. We plan to address this issue in year 3.

Concerning the study of termination of mobile processes, the PhD student who has been hired in year 2 to work on this subject has been facing some difficulties. While we were hoping to improve on last year results (that is, to be able to prove termination for a much larger class of processes), we have not really succeeded in that: we have only some – rather incremental — new results. As a consequence, we have started examining other techniques for proving termination, departing from the approach based on logical relations. Some promising initial results have been obtained; a paper is in preparation.

Another difficulty we have been facing is that the postdoc that was hired for the project quit after one year (in August 2003), which resulted in a weaker effort than expected in the work on advanced programming constructs (Task 3.3). We hope to be able to exploit the remaining manmonths soon in year 3.

Finally, type inference algorithms have not been studied as expected. One of the main novel type systems that we put forward during year 1 was Teller's, and he had planned to look into the type inference problem. He has not done this yet, because of other problems that Teller has got involved with.

Despite these discrepancies w.r.t. the plans in the TA and SEP, we believe that we have done most of what was due for year 2, in some cases going beyond expectations on some subjects that were due to be treated mostly in year 3. All in all, the outcome of year 2 goes beyond our plans, which is why we consider it to be satisfactory.