DIET: Developing Implementation and Extending Theory
A Symbolic Approach to Reasoning about LOTOS
GR/M07779/01
Individual Grant Review Report

Executive Summary

The aims of the project were to support symbolic reasoning about LOTOS specifications by:

1. implementing a *symbolic* model checker for temporal logic and LOTOS.
2. adding E-LOTOS [ISO98] extensions to existing symbolic theory of LOTOS, adding modal μ-calculus extensions to existing symbolic logic theory, and implementing these extensions in the symbolic model checker,
3. carrying out case studies in the application of the temporal logic, LOTOS/E-LOTOS (as appropriate), and the model checker, to medium-sized real world problems,
4. carrying out a final evaluation of theory and implementation.

Despite staffing problems, these aims have all been achieved. In fact, we implemented three model checkers, exploiting different implementation paradigms, and also proved some crucial theoretical results (key advances 1 and 2) which were not part of the original plan. We investigated E-LOTOS extensions, but determined that further work in this area would not be beneficial.

The project ran for 40 months. A postdoctoral research fellow was employed for 12 months, and an undergraduate was given a summer studentship. Three prototype tools were produced. Members of the group attended national and international conferences and workshops. International collaborations were initiated. There were 5 publications in major refereed journals and conferences [CMS02, CMS01, CS01a, BS01, Mah01b], with 6 publications in other fora [BVS01a, BVS01b, RS01a, RS01b, CS00, CS01b], and 4 still in progress [BCM$^+$02, BMS02, Mah01a, Sha02], and expected to be submitted within the next 6 months.

Background to the Research

Computer failures can be spectacular, and occasionally fatal. It is essential that we find ways of making these systems more reliable. Formal methods can contribute to achieving this, but the chosen formalism must reflect the real world system accurately, otherwise any results proved about the mathematical model may not apply to the real system. Also, since only small studies can be analysed by hand, good tool support is required. Lastly, in order to assist and guide software engineers applying formal methods it is important to have a selection of case studies.

The work undertaken in this project is a part of an ongoing investigation to support software engineering by use of formal methods. Our research in the last six years has focussed on the development of a symbolic framework for reasoning about LOTOS specifications, separating the concerns of reasoning about data and reasoning about processes. The EPSRC DIET project allowed us to fill in some of that framework.

LOTOS (Language of Temporal Ordering Specification, ISO 8807 [ISO88]) has been widely used in a number of areas including ODP (Open Distributed Processing), Intelligent Networks, hardware design, and safety critical systems such as railway signalling systems, avionics, and radiation devices. In order to increase reliability, LOTOS is best used to describe the concrete properties of a system with a modal logic being used to describe the abstract properties of the system. A proof system or model checker can be used to validate these descriptions with respect to each other, and each language is used in its most appropriate way.

Model checking is a popular verification technique because of its high level of automation, but it is limited by the well known state explosion problem: only models of limited size can be checked, and the size of the model increases exponentially with the size of the target system. LOTOS is hit doubly by this, because the standard semantics yields infinite state transition systems.

Our approach is to use symbolic transitions systems, originally developed by Hennessy and Lin [HL95]. As well as giving a more elegant and tractable semantics for LOTOS, this can also be seen as an abstraction technique, tackling the state space explosion problem. This approach should not be seen as a competitor to abstraction techniques such as cone of influence reduction [CGP99], data abstraction [CGL94] and data independence [LN00]. Rather it is complementary, since it may be used in conjunction with other techniques to make greater savings in state space.

Key Advances

Our symbolic framework for LOTOS, see figure 1, is based around a symbolic semantics for Full LOTOS [ST97, CS01a] using Symbolic Transition Systems (STS) [HL95]. It also includes an HML-like logic (FULL) [CMS02] and symbolic bisimulation [CS01a, CS00, CS01b]. Although we focus on the use of LOTOS as a specification language, any similar process algebra can be represented in a symbolic framework.

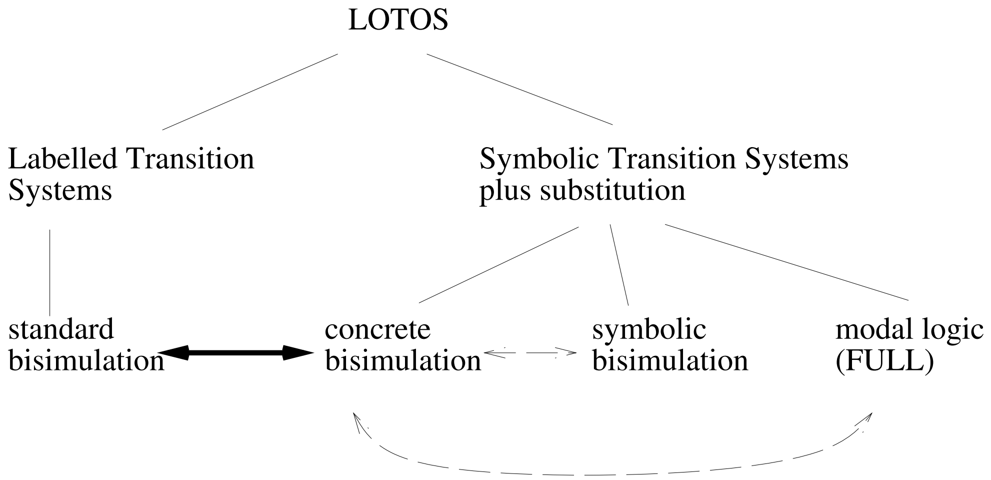

Figure 1: Symbolic Framework for LOTOS

In this project our key advances are:

1. **Proof of the relation between symbolic and standard bisimulation**

   LOTOS is a standardised language, therefore it is important that the meaning of the semantics is retained while gaining the benefit of a more convenient compact notation using symbolic transition systems. This result means that if two closed processes are bisimilar under the standard bisimulation relation, then they are bisimilar under symbolic bisimulation [BCM$^+$02]. This relation is shown by the heavy arrow in figure 1.

2. **Proof of adequacy of FULL with respect to symbolic bisimulation**

   This result shows that if two processes are bisimilar then they satisfy the same logical properties [CMS02, CMS01]. Conversely, if the processes are not bisimilar then there is a logical property which captures the difference between them. This is an important result because it shows that our symbolic framework is self-consistent in this sense. The logic differentiates exactly the same sets of processes as the bisimulation relation. This result is represented by the dashed arrows in figure 1.

3. **Three prototype model checking tools for the logic**

The three tools are built on top of existing tools, and all exploit different paradigms. The first [BS01] is built on top of CADP, and is useful because although the semantics in this case is not really symbolic, our tool can be part of an established suite of tools for reasoning about LOTOS specifications. The second [RS01a] is built on top of the theorem prover Ergo. This implements a truly symbolic semantics, and gives access to theorem proving tactics for reasoning about the data part of specifications. The third [BVS01a] is built in a term rewriting system Maude. This also implements a symbolic semantics, and gives access to term rewriting techniques for dealing with data.

4. **Extended version of FULL**

   The FULL logic has some nice theoretical properties, described above; however, for practical specification purposes a more expressive logic is required. A particular flaw in FULL is the inability to describe properties with loops. FULL* [BMS02] is an extended version of FULL which can describe such properties. Prototype implementation has been carried out in CADP.

5. **Case studies**

   To demonstrate the functionality of our symbolic framework it is important to carry out case studies. Some small case studies exist, but these are not yet fully written up and published [BHS02, HS00, Sha02].

Collaborations have arisen through the tool development work with Alberto Verdejo (UCM, Spain) and Peter Robinson (SVRC, Australia). These are ongoing: Mr Verdejo is implementing other parts of the symbolic framework in Maude [Ver02b] as part of his thesis, and an extended version of the Ergo paper [RS01a] is in preparation. New collaborations also arose in the theoretical work: Savi Maharaj (Stirling) contributed as much as a co-investigator [CMS02, CMS01, Mah01a, Mah01b], and Lionel Morel (IMAG, France) continues to work with us on a paper describing FULL* [BMS02].

Related work, extending tool support for the framework in figure 1 by developing and implementing an algorithm for symbolic bisimulation [RC02] is being carried out by Brian Ross (Glasgow), who is a student of Prof. Calder.

Project Plan Review

The original proposal was for a project student who would carry out the bulk of the work over three years, producing the main deliverables. In 1998 it was extremely difficult to attract PhD students therefore the plan was substantially revised (in consultation with EPSRC) to employ a postdoctoral research fellow for one year. Dr Bryans already had substantial experience in exactly the right area, therefore could come up to speed on the project very quickly. The disadvantage was that there was a full time employee for only one third of the original proposed time. Dr Bryans also had some serious health problems during that year, losing even more time. In light of this we had to rationalise the deliverables somewhat; however, we have achieved a major part of what was originally proposed, together with some additional goals.

There were 4 main tasks in the original workplan, corresponding to the project aims described on page 1 of this report. Key advances 1 and 2 were not part of the original workplan, but are crucial to the solid foundation of the symbolic framework. The introduction of Dr Maharaj to the project made key advance 2 possible.

Key advance 3 corresponds to the original task 1: implementation of a symbolic model checker for LOTOS and logic of [ST97]. This has been completed threefold, allowing us to explore the boundaries between model checking and proof theoretic techniques. This hybrid verification technique blurs the lines between model checking and theorem proving and is an active area of research. This has been the basis of further project proposals.

Key advance 4 partially addresses the original task 2: to extend the theory of FULL with operators from the μ-calculus, and to extend the symbolic semantics of LOTOS to include features of E-LOTOS. FULL* has been developed. While this has not the full expressive power of the modal μ-calculus, it does have loop operators, which are sufficient for many purposes and easier to understand for users. At the time of the original proposal E-LOTOS was an exciting new extension to the LOTOS language which would potentially solve all the problems of LOTOS. We did spend some time investigating E-LOTOS, and the use of symbolic transitions in its semantics, but our conclusion was that E-LOTOS is too complex and that the community was not taking it up to any great extent. Therefore we did not expend any further effort in this direction.

Key advance 5 corresponds exactly to the original task 3: case studies. An undergraduate summer intern helped progress the case study work. The case studies have been written up informally, with the intention of incorporating them into some of the other implementation and theory papers.

Finally, task 4: final evaluation of theory and implementation, remains to be completed. We are currently working on a paper with that theme [BCM$^+$02].

Research Impact and Benefits to Society

Model checking is a verification technique at the focus of much international research. Symbolic transitions systems provide a compact semantics for LOTOS, making specifications more amenable to automated analysis. This can be used in conjunction with other abstraction techniques to make greater savings in state space. This can only increase the total number of systems which are amenable to analysis, therefore the development of this abstraction technique should be of great interest to the model checking community.

On a broader level, our work provides another formal approach to specification and verification, aimed at improving the reliability of software engineering and the correctness of critical systems. The Technology Foresight programme identified Software Engineering as a key research topic.

Further research arising from our symbolic semantics work is being carried out by Alberto Verdejo and Brian Ross, both PhD students. Mr Verdejo is expressing other parts of the symbolic semantics in Maude, and has published several papers [Ver02a, Ver02c, Ver02b]. Mr Ross is working on a different branch of the framework, looking at bisimulation, and has submitted a paper [RC02].

Explanation of Expenditure

The main variation from the original expenditure plan was the use of monies allocated for the studentship and student fees to employ the postdoctoral research fellow and the summer intern. Some monies from the travel budget were also used for this purpose. The travel budget was used for two international (European) conferences (FM 99 and FME 2001), two UK workshops (BCTCS 2001 and AVOCS 2001), to visit Mr Verdejo in Madrid, and for regular project meetings with the co-investigator in Glasgow.

New contributions to the project came from unforeseen collaborations. These contributions were all in terms of academic staff time:

- Dr Savi Maharaj, University of Stirling, joined the project and contributed substantially to the theoretical work (key advance 2).
- Mr Alberto Verdejo, Universidad Complutense de Madrid, contributed as an expert on E-LOTOS and on the third prototype tool, implemented using Maude (key advance 3).
- Dr Peter Robinson, University of Queensland, contributed to the second prototype tool, implemented in Ergo (key advance 3).
- Mr Lionel Morel, IMAG, contributed to the theoretical development of the logic FULL* and its implementation in CADP (key advance 4).

Further Research and Dissemination Activities

The results of the project have been disseminated in three main ways:

- presentation at national and international conferences and workshops. We attended FME 2001, FORTE 2001, BCTCS 2001, AVOCS 2001, AVIS 2001 and presented our work.
- We have published in a journal [CMS02], proceedings of internationally respected conferences [CMS01, CS01a, BS01, Mah01b], national and international workshops [BVS01a, RS01a, BVS01b, RS01b], and departmental reports [CS00, CS01b]. Our collaborator Alberto Verdejo has also published work based on the symbolic transition systems for Full LOTOS described in [CS01a] in an international conference [Ver02b] and in technical reports [Ver02a, Ver02c].
- a web site, to disseminate information electronically `http://www.cs.stir.ac.uk/diet/`.

At every opportunity we talk to colleagues about the symbolic framework, the logic, and the tools developed. We have had some discussions with colleagues at the Motorola Australian Software Centre and at QinetiQ, but in the main we have disseminated our work to academics, through departmental seminars. Seminars have been given at the University of Kent at Canterbury, University of York, the Robert Gordon University, the University of Adelaide, the Software Verification Research Centre at the University of Queensland, the Universidad Politecnica de Madrid, at the Scottish Model Checkers and Scottish Theorem Provers seminars, and at the BCTCS workshops.

At the end of the grant period, some loose ends remain. Papers to be finished in the next six months include: a paper describing and evaluating the whole symbolic framework [BCM+02] (to be submitted to a journal), a paper detailing the extended version of the logic [BMS02] (to be submitted to a conference), and an extended version of the Ergo implementation paper [RS01a] (to be submitted to a journal). Also, the case study material remains to be written up formally [BHS02, HS00, Sha02], but these are more likely to be incorporated as illustrative examples in the above papers.

References

[BCM+02] J. Bryans, M. Calder, S. Maharaj, B. Ross, and C. Shankland. Report on Developing a Symbolic Framework for Reasoning about Full LOTOS. In preparation, 2002.

[BHS02] J. Bryans, R. Hardy, and C. Shankland. A Symbolic Approach to the RPC case study. In preparation, 2002.

[BMS02] J. Bryans, L. Morel, and C. Shankland. Extending FULL with * operations. In preparation, 2002.

[BS01] J. Bryans and C. Shankland. Implementing a modal logic over data and processes using XTL. In M. Kim, B. Chin, S. Kang, and D. Lee, editors, *Proceedings of FORTE 2001, 21st International Conference on Formal Techniques for Networked and Distributed Systems*, pages 201–218. Kluwer Academic Publishers, 2001.

[BVS01a] J. Bryans, A. Verdejo, and C. Shankland. Using Rewriting Logic to implement the modal logic FULL. In R. Bharadwaj, editor, *AVIS'01: First International Workshop on Automated Verification of Infinite-State Systems*. Naval Research Laboratory Technical Memorandum, 2001.

[BVS01b] J. Bryans, A. Verdejo, and C. Shankland. Using Rewriting Logic to implement the modal logic FULL. In D. Nowak, editor, *AVoCS'01: Workshop on Automated Verification of Critical Systems*, 2001. Oxford University Computing Laboratory technical report PRG-RR-01-07.

[CGL94] Edmund M. Clarke, Orna Grumberg, and David E. Long. Model checking and abstraction. *ACM Transactions on Programming Languages and Systems*, 16(5):1512–1542, September 1994.

[CGP99] E. M. Clarke, O. Grumberg, and D. A. Peled. *Model Checking*. The MIT Press, 1999.

[CMS01] M. Calder, S. Maharaj, and C. Shankland. An Adequate Logic for Full LOTOS. In J. Oliveira and P. Zave, editors, *Formal Methods Europe'01*, LNCS 2021, pages 384–395. Springer-Verlag, 2001.

[CMS02] M. Calder, S. Maharaj, and C. Shankland. A Modal Logic for Full LOTOS based on Symbolic Transition Systems. *The Computer Journal*, 45(1):55–61, 2002.

[CS00] M. Calder and C. Shankland. A Symbolic Semantics and Bisimulation for Full LOTOS. Technical Report CSM-159, University of Stirling, 2000.

[CS01a] M. Calder and C. Shankland. A Symbolic Semantics and Bisimulation for Full LOTOS. In M. Kim, B. Chin, S. Kang, and D. Lee, editors, *Proceedings of FORTE 2001, 21st International Conference on Formal Techniques for Networked and Distributed Systems*, pages 184–200. Kluwer Academic Publishers, 2001.

[CS01b] M. Calder and C. Shankland. A Symbolic Semantics and Bisimulation for Full LOTOS. Technical Report TR-2001-77, University of Glasgow, 2001. Extended version of FORTE 2001 paper.

[HL95] M. Hennessy and H. Lin. Symbolic Bisimulations. *Theoretical Computer Science*, 138:353–389, 1995.

[HS00] R. Hardy and C. Shankland. Battleships: A Case Study using Symbolic Transition Systems. Draft manuscript, 2000.

[ISO88] International Organisation for Standardisation. *Information Processing Systems — Open Systems Interconnection — LOTOS — A Formal Description Technique Based on the Temporal Ordering of Observational Behaviour*, 1988.

[ISO98] International Organisation for Standardisation. *ISO/IEC JTC1/SC21 WG7: Enhancements to LOTOS*, May 1998. Final committee draft.

[LN00] Ranko Lazić and David Nowak. A Unifying Approach to Data-independence. Technical Report PRG-TR-4-00, Oxford University Computing Laboratory, June 2000.

[Mah01a] S. Maharaj. A PVS-Assisted Proof of Adequacy for a Logic for Full LOTOS. In preparation, 2001.

[Mah01b] S. Maharaj. A PVS Theory of Symbolic Transition Systems. In Richard J Boulton and Paul B Jackson, editors, *Supplemental Proceedings of Theorem Proving in Higher Order Logics 2001, September 2001*, pages 255–266, 2001. Published Informatics Research Report, Division of Informatics, University of Edinburgh.

[RC02] B. Ross and M. Calder. Computing Symbolic Bisimulations for Full LOTOS. Submitted to FACS, 2002.

[RS01a] P. Robinson and C. Shankland. Implementing the modal logic FULL using Ergo. In R. Bharadwaj, editor, *AVIS'01: First International Workshop on Automated Verification of Infinite-State Systems*. Naval Research Laboratory Technical Memorandum, 2001.

[RS01b] P. Robinson and C. Shankland. Implementing the modal logic FULL using Ergo. In D. Nowak, editor, *AVoCS'01: Workshop on Automated Verification of Critical Systems*, 2001. Oxford University Computing Laboratory technical report PRG-RR-01-07.

[Sha02] C. Shankland. Classic Case Studies using Symbolic Transition Systems. In preparation, 2002.

[ST97] C. Shankland and M. Thomas. Symbolic Bisimulation for Full LOTOS. In M. Johnson, editor, *Algebraic Methodology and Software Technology, Proceedings of AMAST 97*, LNCS 1349, pages 479–493. Springer-Verlag, 1997.

[Ver02a] A. Verdejo. A tool for Full LOTOS in Maude. Technical Report 123-02, Dpto. Sistemas Informaticos y Programacion, Universidad Complutense de Madrid, April 2002.

[Ver02b] A. Verdejo. Building tools for LOTOS Symbolic Semantics in Maude. In *Proceedings of FORTE 2002, 22nd International Conference on Formal Techniques for Networked and Distributed Systems*, 2002. To appear.

[Ver02c] A. Verdejo. LOTOS Symbolic Semantics in Maude. Technical Report 122-02, Dpto. Sistemas Informaticos y Programacion, Universidad Complutense de Madrid, January 2002.