Logics and calculi for cyberphysical components

PhD Proposal
MAP-i 2013-14

January, 2014

1 Aims

For the last 15 years, the emergence of massive concurrent, heterogeneous systems and the growing complexity of interaction protocols has brought coordination of software components to a central place in software development. This contributed to broadening its scope of application taken here to the level of physical devices but contrasts to the fact that, despite remarkable progress in the representation of software architecture, its specification remain, at present, largely informal. On the other hand, most of the mathematical models for hybrid systems and stochastic components in the literature are formally heavy and not easily amenable to calculation.

Actually, existing models for software coordination still lack widely accepted and proved effective means for reasoning about non functional, QoS related properties of interacting parts. Such inadequacy is explained by systems complexity (which entails the need for flexible compositional approaches), inappropriate simplifications (e.g., the assumption that QoS parameters are independent of each other) and the inability to deal with partial data and stochastic behaviour.

This is even more challenging when non discrete behavioural properties are involved, arising from computational engines deeply embedded in physical systems. Examples include cooperating medical devices, micro scale cyberphysical materials, devices in vehicular networks, or controllers for electricity generation and distribution, among many others.

This PhD project proposes to study the compositional specification and formal analysis of systems exhibiting non functional and non discrete behavioural properties. In particular, it aims at addressing the following research questions:

- How to logically model and reason about continuous, stochastic and mixed properties of software components, their composition and interoperability in the context of complex, heterogeneous software systems?
- How to specify, design, analyse and transform evolving networks of (dynamically reconfigurable) heterogeneous software including components directly involving (or embedded in) physical systems?

2 Starting points

This PhD project is framed in previous work developed at the research units to which the proponents are affiliated (CIDM, U. Aveiro and HASLab INESC TEC, U. Minho), part of it in the context of joint FCT-funded research projects on the formal foundations of software architecture. These include the following two research directions.

- An approach to the specification of *reconfigurable* software based on *hybridised* logics (i.e., logics resulting from the systematic development of hybrid features on top of a base specification logic) carried on on an institutional setting [3, 5, 4]. To express, analyse and verify behavioural properties entails the need for hybrid logics enriched with quantitative annotations and inference. Specification frameworks for quantitative reasoning, dealing for example

with weighted or probabilistic transition systems, emerged recently as a main challenge for software engineers. This witnesses a shift from classical models of computation, such as labeled transition systems, to similar structures where quantities can be handled. Examples include weighted, hybrid or probabilistic automata, as well as their coalgebraic rendering. A step worth to explore consists of taking up this *quantitative* challenge within the context of the hybridisation process itself. The simplest move in such a direction proceeds by instantiation. In this case quantitative reasoning is just reflected and expressed at the local level of concrete, specific configurations. A complementary path may focus on generalising the underlying semantic structures, replacing the relational component in models by coalgebras over suitable categories of probability distributions, metric, or topological spaces.

- The development of a component calculus in a coalgebraic framework, parametrized by a notion of behaviour model formalised as a strong monad (to capture, eg, partiality or non determinism) [1, 6, 2]. As it stands the calculus targets classical (i.e. discrete, non deterministic) components. Lifting this work to meet the aims of the the present proposal will require a semantical shift towards monads, or related structures (e.g. Lawvere theories), capturing more complex behaviours (stochastic and/or continuous) and the development of calculi to reason about them. The definition of suitable specification logics to reason about probabilistic and/or cyber-physical components buds a bridge to the first research direction mentioned above.

  For stochastic components there is solid work on coalgebraic reasoning within probabilistic settings, resorting to the distribution monad (or the Giry monad for the continuous case), stimulated by the need to provide quantitative information about system's behaviour. Metrics replace the classical two valued behavioural equivalences as a tool to analysis and design. Things are less clear for the continuous case. Nearly from the beginning (cf, Henzinger's 1996 paper) such systems have been modelled as hybrid automata, which equip states and edges with variables and differential equations to reflect the behaviour of the environment in each node. Recent research in the area favours the development of analysis techniques combining (quantitative) model-checking (see e.g. the work of C. Baier) with automated theorem proving. The work of A. Platzer [7] is particularly challenging from a logic point of view.

3 Context

Research Units. HASLab INESC TEC and CIDMA.

Supervisors.

- Luis S. Barbosa, HASLab INESC TEC and Dep. Informatics of Universidade do Minho
- Manuel Antóbio Martins, CIDMA and Dep. Mathematics of Universidade de Aveiro

External member of the Monitoring Committee: Marcello Bonsangue (CWI and Leiden University, Holland)

References

[1] L. S. Barbosa. Towards a Calculus of State-based Software Components. *Journal of Universal Computer Science*, 9(8):891–909, August 2003.

[2] L. S. Barbosa and J. N. Oliveira. Transposing partial components: an exercise on coalgebraic refinement. *Theor. Comp. Sci.*, 365(1-2):2–22, 2006.

[3] A. Madeira. *Foundations and techniques for software reconfigurability.* PhD thesis, Universidades do Minho, Aveiro and Porto (Joint MAP-i Doctoral Programme), July 2013.

[4] A. Madeira, J. M. Faria, M. A. Martins, and L. S. Barbosa. Hybrid specification of reactive systems: An institutional approach. In G. Barthe, A. Pardo, and G. Schneider, editors, *Software Engineering and Formal Methods (SEFM 2011, Montevideo, Uruguay, November 14-18, 2011)*, volume 7041 of *Lecture Notes in Computer Science*, pages 269–285. Springer, 2011.

[5] M. A. Martins, A. Madeira, R. Diaconescu, and L. S. Barbosa. Hybridization of institutions. In A. Corradini, B. Klin, and C. Cîrstea, editors, *Algebra and Coalgebra in Computer Science (CALCO 2011, Winchester, UK, August 30 - September 2, 2011)*, volume 6859 of *Lecture Notes in Computer Science*, pages 283–297. Springer, 2011.

[6] S. Meng and L. S. Barbosa. Components as coalgebras: The refinement dimension. *Theor. Comp. Sci.*, 351:276–294, 2005.

[7] A. Platzer. *Logical Analysis of Hybrid Systems: Proving Theorems for Complex Dynamics.* Springer, 2010.