Scientific Annals of Computer Science vol. 22 (1), 2012, pp. 1–4
DOI: 10.7561/SACS.2012.1.1

Towards Interaction Reliability in Concurrent Applications

Simon BLIUDZE[1], Roberto BRUNI[2], Marco CARBONE[3]
Alexandra SILVA[4]

Abstract

Developing trustworthy concurrent applications is a seemingly never ending quest, which is necessary but difficult. It is necessary because mainstream systems and applications are inherently concurrent and they are pervasive to our daily life activities. It is difficult because such systems are inherently interactive and heterogeneous, so that boundaries can hardly be established for studying subsystems in isolation. Formal methods are a key instrument in resolving ambiguities and design reliable applications in a rigorous way. The authors overview major problems in the application of formal methods and outline how they are tackled by the papers collected in this volume.

Keywords: interactive systems, coordination, game semantics, reactive contexts, contracts, multi-party choreographies

Recent evolution of hardware and communication infrastructure has resulted in the shift of mainstream systems and applications to highly concurrent and distributed execution architectures ranging from multi-core processors to world wide available web services. As both industry and society grow increasingly dependent on these applications, reliability and, more generally, trustworthiness of complex systems and services becomes a crucial issue. State space explosion, inherent to the concurrency in these

[1]EPFL, Rigorous System Design Laboratory, Lausanne, Switzerland.
Email: `simon.bliudze@epfl.ch`

[2]Computer Science Department, University of Pisa, Italy. Email: `bruni@di.unipi.it`

[3]IT University of Copenhagen, Denmark. Email: `carbonem@itu.dk`

[4]Radboud University Nijmegen, The Netherlands. Also affiliated to CWI (Amsterdam, The Netherlands) and HasLab / INESC TEC, Universidade do Minho (Braga, Portugal).
Email: `alexandra@cs.ru.nl`

systems and exacerbated by their growing complexity, renders the application of existing techniques such as testing and model checking difficult to scale up and impractical. In this context, understanding interaction and composition assumes a prominent role: How to circumscribe system boundaries of the right dimension so that it can be conveniently studied in isolation? Which realistic hypotheses can we impose on the environment to guarantee that the system will behave in a reliable manner? Moreover, each system has its own requirements and goals and its reliability depends on the degree in which they are met: How can we guarantee that the composition of systems reliable on their own are then reliable w.r.t. the overall requirements? We argue that reliability can be achieved through a rigorous design flow taking into account both functional and architectural constraints of the system and producing the system implementation through a series of transformations with well-defined and non-ambiguous semantics, which are complemented by sound and compositional principles which allow for a correct implementation of the compound system.

Several problems have to be addressed when defining such a rigorous design flow.

1. First and foremost, as mentioned above, all the involved models and transformations must have a well-defined and non-ambiguous semantics. As it stands, however, development frameworks are either designed with the primary concern put on syntactical aspects, rendering the semantics incomplete, or have their semantics evolving to incorporate recent research. Many semantics have been defined to tackle different issues (e.g. functional and non-functional aspects) in which case it is then important to relate them and possibly identify their synergic use. Moreover, interactive systems rely on the behaviour of the environment in which they are enacted, and, in this context, their semantics must expose some (minimal) hypotheses under which the system will behave correctly.

   The paper by Jongmans and Arbab gives a comprehensive survey of all different semantic formalisms that have been used to define the semantics of Reo, a prominent coordination language for component-based systems, discussing the main features, analogies and differences between each proposal and showing how the theoretical results can have practical consequences in improving the performance of available analysis tools.

   The paper by Hirschowitz and Pous presents a categorical game se-

mantics for CCS, where the so-called innocent strategies are modeled as presheaves and shown to form a terminal coalgebra. Moreover, fair and must testing equivalences are revisited in the new setting.

The paper by Dorman, Heindel and König investigates an SOS style axiomatization of the standard labelled transition semantics for graph transformation systems which is based on the idea of minimal reaction contexts as labels and improves the so-called *borrowed context* technique.

2. Another important issue are the various kinds of heterogeneity encountered in concurrent application development, among which we will particularly mention the heterogeneity of modelling formalisms. Over the years, numerous programming languages and design formalisms have been proposed to deal with the constraints imposed by various application domains. In general, these languages and formalisms do not have a common semantics, whereas operational semantics of some are incompatible. Proper interactions are possible only if suitable (behavioural) contracts are negotiated and subscribed that can drive sound computations and assign responsibilities when some processes do not respect the obligations they are bound to by the contract.

   The paper by Bartoletti, Tuosto and Zunino presents a parametric calculus for contract-based computing in distributed systems that generalises both the contracts-as-processes and contracts-as-formulae paradigms. Contracts bind processes in terms of promises and facts, and the primitives of the calculus are centered on the advertising, matching and enactment of contracts over freshly created sessions. The work in this paper has the merit of being independent of the contract specification language, thereby alleviating the problem of formalism heterogeneity.

3. Last, but not least, one should account for the fact that specifications are bound to be incomplete and, in some cases, contradictory. On one hand, affirming specification completeness requires a model of the system and its environment. Such model becomes then also a specification, whereof one has to demonstrate the completeness, *et cetera ad infinitum.* In practice, one settles for incomplete specifications, which are later refined with additional knowledge of the system environment and expected behaviour gained during the later stages of the design and/or maintenance process. On the other hand, several

developers are commonly involved in the specification and design of a single application, each being responsible for some component or subsystem. Often such arrangement leads to constraints being imposed on the system from the standpoint of a given component that come into conflict with similar constraints imposed from the standpoint of other components.

The paper by Bocchi, Lange and Tuosto defines a sound methodology for dealing with two classes of flaws in multi-party choreographies, viz. so-called history sensitivity and temporal satisfiability. The approach is illustrated by a well-selected set of examples that address the improvement of some frequent patterns.

The papers assembled in this volume are full extended version of selected papers presented at ICE'11, satellite event of the DisCoTec'11 federated conference that took place in June 2011 in Reykjavik, Iceland. The Proceedings of ICE'11 have been published in the volume 59 of the open access, on-line series *Electronic Proceedings in Theoretical Computer Science*.

We want to thank all the authors who contributed to this volume. We would like to thank all the members of the Program Committee and reviewers of ICE, who helped us in the selection of the papers and who helped the authors to improve their contributions in several ways. Additional referees were involved in the review of the papers invited for this special issue and we thank their timely contributions. We also want to warmly thank Gabriel Ciobanu, the Editor-in-Chief of this journal, for giving us the opportunity to prepare this special issue and for his constant guidance and support in reducing the publication timing.