Project React Plus, Progress report

Project directors: Camilo Rueda[1], Jesús Aranda[2], Frank Valencia[3], and Gérard Assayag[4]

[1] Pontificia Universidad Javeriana, Cali, Colombia
[2] Universidad del Valle
[3] Ecole Polytechnique, Paris
[4] IRCAM, Paris

1 Participants

Contributors in this stage of the project are the following:

1. Main researchers:
   - Camilo Rueda, project director at Universidad Javeriana-Cali
   - Jesús Aranda, project director at Universidad del Valle
   - Frank Valencia, project director at Ecole Polytechnique-Paris
   - Gérard Assayag, project director at IRCAM-Paris
   - Juan Francisco Díaz, researcher at Universidad del Valle
   - Carlos Olarte, researcher at Universidad Javeriana-Cali
   - Jean-Louis Giavitto, researcher at IRCAM-Paris
2. Research assistants
   - Andrés Aristizábal, PhD student at Ecole Polytechnique-Paris
   - Luis Pino, PhD student at Ecole Polytechnique-Paris
   - Mauricio Toro, PhD student at Université de Bordeaux I
   - Michell Guzmán, MSc student at Universidad del Valle
   - Jaime Arias, MSc student at Universidad Javeriana-Cali
   - Salim Perchy, MSc student at Universidad Javeriana-Cali
   - Diana Hermith, PhD student at Università degli Studi di Siena, Italy

2 introduction

This report describes advances in the project "React Plus: Robust theories for Emerging Applications in Concurrency Theory: Processes and Logic Used in Emergent Systems" (code 1251-521-28471 Contract 476-2011). The report relates each one of the project goals to progress and results supported by publications. Based on this we estimate our advance and report what remains to be done to completely achieve each goal.

The general goal of the project is to provide concurrent constraints calculi (ccp) with automatic verification and simulation techniques and user-friendly tools that can be used by practitioners in our intended applications areas: Security, Biology and Multimedia Semantic Interaction. As stated in the proposal, this constitutes a big challenge since, on the one hand, known verification strategies for ccp are far from being practical (due to the state explosion problem) and, on the other, existing ccp simulators are more intended as “proof of concept” tools than as full-fledged modeling environments.

For the verification aspect, since there is, at present, no particular methodology that most researchers find specially promissory, we decided to explore various different strategies simultaneously. For the simulation tools we considered two general strategies, one that builds stand-alone simulators based on developing efficient implementation of concurrent threads and one that constructs applications around existing tools.

In what follows we present the advance of our work in these areas for each specific goal of the project. *All referred papers and thesis are products resulting from the project.*

3 Techniques

We proposed to develop automaton-based, constraint-based symbolic methods as well as abstract-interpretation and type techniques for the automatic verification of system properties in ccp calculi.

3.1 Automata-based techniques

In a previous work it is shown that the strongest post-condition of a ntcc process (representing its possible outputs), whose guards do not depend on local variables, can be translated into a Büchi automaton. The disadvantage of using the Büchi translation to make a model checker based on the classic LTL model checking algorithm is that computing the complement of Büchi automata is intractable. In this project we have been exploring subsets of ccp languages that can be used in practical applications and at the same time are suitable for tractable automaton-based strategies. One possibility is to restrict ntcc process replication to finite instances. This allows to use the previously mentioned strategy with finite automata instead of Büchi and then to take advantage of existing finite automata tools to construct the verifier. In this project we developed a strategy along these lines, that is reported in [8].

3.2 Bisimilarity techniques

There is a different alternative to model checking for verification of ccp, namely the definition of *bisimilarity* relations. Intuitively, two systems are bisimilar if they match each others moves. Roughly, properties to be verified of some process P are represented by the behavior of some abstract specification process A, that is then checked to be bisimilar to P. Different types of bisimilarity relations (strong, weak, barbed, etc) serve different verification purposes. Bisimilarity relations have been widely used for verification of concurrent process calculi such as the π-calculus, but not for ccp calculi. In fact, there have been few attempts to define a notion of bisimilarity for ccp. Existing definitions were not satisfactory, either because they may tell apart processes with identical observable behaviour, or because their implementation is not feasible. In this project we have achieved the following:

1. We developed a bisimilarity (both strong and weak) notion for ccp ([1]) which allows to benefit of the feasible proof and verification techniques typically associated with bisimilarity. We also described the relationship between this equivalence and other existing semantic notions for ccp.

2. We analyzed existing algorithms to check bisimilarity equivalence of two processes with the aim to adapt them to ccp. We showed that that the standard partition refinement algorithm does not work for ccp, and we introduced a modified partition refinement algorithm for saturated barbed bisimilarity of ccp ([1]).
3. When considering weak bisimilarity, the standard way is to first reduce it to strong bisimilarity and then use the partition refinement algorithm. We showed that the standard method for achieving this reduction does not work for ccp and we provide a way out of the impasse ([2])

3.3 Abstract Interpretation Techniques

In [5] we consider the denotational semantics for tcc, and we extend it to a "collecting" semantics for utcc based on closure operators over sequences of constraints. Relying on this semantics, we formalize a general framework for data flow analyses of tcc and utcc programs by abstract interpretation techniques. The concrete and abstract semantics we propose are compositional, thus allowing us to reduce the complexity of data flow analyses. We show that our method is sound and parametric w.r.t. the abstract domain. Thus, different analyses can be performed by instantiating the framework. We illustrate how it is possible to reuse abstract domains previously defined for logic programming, e.g., to perform a groundness analysis for tcc programs. We show the applicability of this analysis in the context of reactive systems. Furthermore, we make also use of the abstract semantics to exhibit a secrecy flaw in a security protocol. We also show how it is possible to make an analysis which may show that tcc programs are suspension free. This can be useful for several purposes, such as for optimizing compilation or for debugging.

4 Tools

We proposed producing a tool prototype along the lines of the Mobility Workbench, an automated tool for manipulating and analyzing mobile concurrent systems described in the pi-calculus. Such tool should allow describing, exploring, simulating and automatically verifying systems described in ccp calculi.

4.1 Verification

We have explored the construction of a Kripke-like structure for the model checking of tcc programs. This technique is based on the work of Falaschi and Alicia Villanueva (published in 2006) and relies on the symbolic representation of the execution of tcc programs. Up to now we have an algorithm for building the tcc structure and we are working on the construction of the model checking graph based on the temporal logic representing the property to be proved.

Currently we are exploring the use of abstract domains (see 3.3) in the model checking (MC) algorithm for the verification of tcc programs. The idea is to reduce the number of spaces generated in the construction of the MC structure by considering an over-approximartion of the behavior of the system.

4.2 Simulation

Simulators of ccp models are fundamental for the user. They allow to form an idea about the evolution of a system. For systems interacting with the environment it is crucial that such simulators be efficient. In previous works our research group developed “proof of concept” simulators of ntcc, that were successfully tested in various examples. We had developed two ntcc simulators, one written in the multi paradigm language Oz and another one written in c++. The first used the constraint system embedded in Oz to handle the calculus operations and the other built an interface with the constraints library Gecode. In this project we have refined both implementations. The Oz simulator was supplied with a user interface to bring process definitions closer to the end user (biologists) language. This is called *Bioways* and is available on http://avispa.puj.edu.co. The other one is described in some detail in [8].

We have also developed a simulator for the lcc language (a concurrent constraints calculus based on linear logic) and used it in a real application, the verification of program correctness. This simulator, called *Alcove*, is available on http://avispa.puj.edu.co.

We are working in a tool that allows to write ntcc programs in a natural way, i.e. using directly the ntcc syntax. Such ntcc program can be compiled into a virtual machine implemented over the oz programming language. The aim is to ease the construction of ntcc models to people in areas different from computer science such as biology, music, etc. We have chosen bison and flex in order to implement the lexical analyzer and parser and the oz programming language for implementing the ntcc virtual machine. We have at present completed the following activities:

- ntccPL (*ntcc Programming Language*) grammar definition.
- Implementation of the compiler front end (lexical analyzer and parser).
- Modification of the ntcc virtual machine adding the new process *abort, bounded replication, bounded star, whenever, next*^{n} .
- Semantic analysis implementation (in process, most part already implemented).
- Code generation (in process, most part already implemented).
- Inclusion of the local process into the virtual machine (in process, most part already implemented).

The remaining activities are:

- Integration between the ntccPL compiler and the ntccPL virtual machine.
- Test run.
- First version of the tool.

4.3 Integration with sound processing

One of the project application fields is Multimedia Interaction. For ccp simulators to be effective in this realm they must be real-time capable. For this project we have developed an interface that allows the ntcc simulator to interact in real-time with the FAUST sound processing software. This interaction has been tested in real multimedia applications, as reported in [8].

5 Applications

We proposed putting to test our tools and techniques by developing real-world applications in several areas. In what follows we describe what has been accomplished in this realm.

5.1 Program Correctness

A recent trend in object oriented programming languages is the use Access Permissions (AP) as abstraction to control concurrent executions. AP define a protocol specifying how different references can access the mutable state of objects. Although AP simplify the task of writing concurrent code, an unsystematic use of permissions in the program can lead to subtle problems. In [3] we present a Linear Concurrent Constraint (lcc) approach to verify AP annotated programs. We model AP as constraints (i.e., formulas in logic) in an underlying constraint system, and we use entailment of constraints to faithfully model the flow of AP in the program. We verify relevant properties about programs by taking advantage of the declarative interpretation of lcc agents as formulas in linear logic. Properties include deadlock detection, program correctness (whether programs adhere to their AP specifications or not), and the ability of methods to run concurrently. We show that those properties are decidable and we present a complexity analysis of finding such proofs. We implemented our verification and analysis approach as the Alcove tool, which is available at http://avispa.puj.edu.co.

5.2 Privacy in Distributed Systems

The notion of *space*, in the many different ways this notion can be conceived, is evermore fundamental in computation. The current trend towards the development of distributed applications makes this notion and, specially, the way users manage it, particularly fundamental. Agents posting and querying information in the presence of spatial hierarchies for sharing information and knowledge, e.g. friend circles and shared albums in social networks or shared folders in cloud storage, provide natural examples of managing information access. These domains raise important problems such as the design of models to predict and prevent privacy breaches, which are commonplace nowadays. The development of ccp techniques and tools to better address these problems is one of the goals of the project. We have thus generalized the underlying theory of constraint systems by adding space functions to their structure. These functions provide for the specification of spatial and epistemic information. We extended ccp with a spatial/epistemic operator. The spatial operator can specify a process, or a local store of information, that resides within the space of a given agent (e.g., an application in some users account, or some private data shared with a specific group). This operator can also be interpreted as an epistemic construction to specify that the information computed by a process will be known to a given agent. This work is reported in [7]

5.3 Multimedia Interaction

One of the goals of the project is to develop modeling tools for multimedia interaction that provide richer synchronization capabilities and at the same time allows the static specification of complex scenarios, such as those comprising sound and video performances. The existing *interactive score* formalism allows to specify a score composed of hierarchical objects representing controllers of sound, video or other multimedia material. These objects are disposed in time in a very flexible way, by means of constraints over their relative starting time or duration, or by decreeing their execution to be controlled by an external interaction. We developed in this project a formalization of interactive scores, comprising an event structures denotational semantics and its corresponding ntcc operational semantics, as described in [9].

Integration of ccp calculi with existing multimedia applications is also one of the goals of the project. We are currently developing a OSC interface for the ntcc calculus. OSC (Open Sound

Control) Is a content format intended for sharing music performance data (gestures, parameters and note sequences) between multimedia devices. Providing ntcc with OSC interaction will allow users to build models integrating communication with many different software/hardware multimedia devices.

In [9] examples of verifiable musical properties are given. These were proved by hand. What remains to be done is to use the verifiers tools developed in the project to do the proofs automatically.

5.4 Biology

In [4] we report on a technique for modelling biological systems based on the ntcc calculus. We show that the ability of ntcc to express partial information, concurrency, non-determinism and timed behaviour allows us to neatly model and simulate biochemical reactions networks. Based on this technique, we introduce BioWayS (BIOchemical pathWAY Simulator) (available at http://www.puj.edu.co), a software tool for the quantitative modelling and analysis of biological systems. We show the applicability of BioWayS in the context of two well studied biological systems: the glycogen breakdown pathway and the HIV life cycle. A detailed report of the latter is given in [6].

6 Products

The specific products at tis stage of the project are:

1. Papers (those included in the references):
   - International journals: 4
   - International conferences: 3
   - National conferences: 1
2. Software
   - BioWays, BIOchemical pathWAY Simulator, available at http://www.puj.edu.co
   - Alcove, A Linear Constraints Verifier for program correctness, available at http://www.puj.edu.co
3. PhD thesis: 1

References

1. A. Aristizábal, F. Bonchi, F. Valencia, and L. Pino. Partition refinement for bisimilarity in ccp. In *Proceedings of the 27th Annual ACM Symposium on Applied Computing (SAC'12)*, pages 88–93. ACM Press, 2012.
2. A. Aristizábal, F. Bonchi, F. Valencia, and L. Pino. Reducing weak to strong bisimilarity in ccp. In *Electronic proceedings of the 5th Interaction and Concurrency Experience (ICE'12)*. EPTCS, 2012.
3. Nestor Cataño, Carlos Olarte, Elaine Pimentel, and Camilo Rueda. A linear concurrent constraint approach for the automatic verification of access permissions. In *Proc. of PPDP'12*. ACM, 2012.
4. Davide Chiarugi, Moreno Falaschi, Michell Guzman, Diana Hermith, and Carlos Olarte. Simulating signalling pathways through bioways. In *Proc. of CS2BIO*, 2012.
5. Moreno Falaschi, Carlos Olarte, and Catuscia Palamidessi. Abstract interpretation of temporal concurrent constraint programs. *Theory and Practice of Logic Programming TPLP (submitted)*, 2012.
6. Michell Guzmán, Juan Francisco Díaz, and Jesús Aranda. Modeling the hiv life cycle using the ntcc calculus. In *7 Congreso Colombiano de Computación, 7CCC, Medellín, Colombia.* IEEE Explore, 2012.

7. S. Knight, C. Palamidessi, P. Panangaden, and F. Valencia. Spatial and epistemic modalities in constraint-based process calculi. In *Proceedings of the 23rd International Conference on Concurrency Theory (CONCUR'12)*, pages 317–332. Springer-Verlag, 2012.
8. Mauricio Toro. Structured interactive scores: From a structural description of a multimedia scenario to a real-time capable implementation with formal semantics. PhD thesis, Université de Bordeaux I, 2012.
9. Mauricio Toro, Myriam Desainte-Catherine, and Camilo Rueda. Formal semantics for interactive music scores: A framework to design, specify properties and execute interactive scenarios. *Journal of Mathematics and Music (to be published)*, 2012.