Formal Methods for Parallel Programming:
Theory and Applications

Formal methods allow specifications of parallel and distributed programs to be precisely stated and the conformance of an implementation to be verified using mathematical techniques. These methods are especially important in parallel and distributed programming where the inherent non-determinism makes testing ineffective.

Formal methods can be used in the development of individual programs and effective tools are becoming available that help to automate the verification task. Foundations for frameworks can be developed that, while requiring no proofs by the programmer, are guaranteed to result in programs with certain properties. These approaches provide significant leverage to a formal analysis.

This year FMPPTA will be held in association with IPDPS for the 6th time and attracts participants from both academia and industry, who use and/or develop formal methods for parallel or distributed programming. The association with IPDPS allows participants to take part in a workshop focussed on formal methods as well as interact with researchers in the broader parallel and distributed processing community.

Our program this year includes papers on an interesting variety of topics. Several of the papers contribute to the foundational work necessary to reason about various types of parallel and distributed systems. For example, Ene and Muntean give a process calculus and operational semantics for reconfigurable systems with broadcast as the basic communications primitive. Prensa-Nieto extend the earlier classical work of Owicki and Gries to allow parameterized parallel programs and show that their proof theory for this extension is sound and relatively complete.

Crazzolara and Winskel demonstrate the use of Petri-nets to verify properties such as secrecy and authentication for security protocols. Java is becoming an increasingly significant implementation language for multi-threaded server applications, and many researchers are investigating optimizations that would make its use in high-performance parallel applications practical. Chaumette’s and Ugarte’s work is a contribution to the effort to develop methods to formally verify these important, often mission critical, multithreaded Java programs.

Other papers discuss efforts to mechanize formal approaches. Mechanization has the potential to eliminate some of the difficulty of applying formal methods and can significantly increase the reliability of a formal analysis. The CafeOBJ specification language, described by Ogata and Futatsugi extends UNITY with facilities to model real time systems while the CafeOBJ system provides automation to support verification activities. The authors illustrate their approach with a case study verifying a railway crossing systems. Cachera and colleagues present verification methods to prove properties of parallel systems described by multi-dimensional affine recurrence equations using a novel combination of polyhedral transformation techniques and theorem proving (using the PVS theorem prover). Royer presents a system that combines graphical elements, model-checking, and theorem proving for verifying mixed systems, where different aspects of the system are specified using different formalisms. Zulkernine and Seviora describe a way to monitor systems as they execute to ensure that assumptions made by component designers about the environment in which a component executes are met.

We are looking forward to a stimulating and enjoyable workshop and would like to thank all authors who submitted papers, the program committee, and the reviewers. Reviewers include Mauno Rönnkö, Pave Emelianov, Christophe Silbertin-Blanc, Linas Laibinis, Marina Walden, Jürgen Dingel, Philippe Queinnéc, G. Juannole, David Monniaux, and the members of the program committee.

Michel Charpentier and Beverly Sanders
Accepted papers

Proving Properties of Multidimensional Recurrences with Application to Regular Parallel Algorithms
D. Cachera, P. Quinton, S. Rajopadhye and T. Risset

A formal model of the java multi-threading system and its validation on a known problem
Serge Chaumette and Asier Ugarte

Petri nets in cryptographic protocols
Federico Crazzolara, Glynn Winskel

A Broadcast-based Calculus for Communicating Systems
Cristian Ene, Traian Muntean

Specifying and verifying a railroad crossing with CafeOBJ
Kazuhiro Ogata and Kokichi Futatsugi

Completeness of the Owicki-Gries System for Parameterized Parallel Programs
Leonor Prensa-Nieto

Formal Specification and Proof Techniques for Mixed Systems
Jean-Claude Royer

Assume-Guarantee Supervisor for Concurrent Systems
Mohammad Zulkernine and Rudolph E. Seviora

Program Committee

Mani Chandy Caltech, USA
Michel Charpentier University of New Hampshire, USA (co-chair)
Radhia Cousot CNRS, France
Mamoun Filali CNRS, France
Klaus Havelund NASA, USA
Jason Hickey Caltech, USA
Dominique Mery Universite Henri Poincare, France
Michael Mislove Tulane University, USA
Lawrence Paulson Cambridge University, UK
Joy Reed Oxford Brookes University, UK (co-chair)
Beverly Sanders University of Florida, USA
Kaisa Sere Abo Akademi University, Finland
David Skillicorn Queens University, Canada