Flow analysis for verifying properties of concurrent software systems

APPENDICES and SUPPLEMENTS


ABSTRACT

This article describes FLAVERS, a finite-state verification approach that analyzes whether concurrent systems satisfy user-defined, behavioral properties. FLAVERS automatically creates a compact, event-based model of the system that supports efficient dataflow analysis. FLAVERS achieves this efficiency at the cost of precision. Analysts, however, can improve the precision of analysis results by selectively and judiciously incorporating additional semantic information into an analysis. We report on an empirical study of the performance of the FLAVERS/Ada toolset applied to a collection of multitasking Ada systems. This study indicates that sufficient precision for proving system properties can usually be achieved and that the cost for such analysis typically grows as a low-order polynomial in the size of the system.

REFERENCES

Note: OCR errors may be found in this Reference List extracted from the full text article. ACM has opted to expose the complete List rather than only correct and linked references.


3  G. S. Avrunin, J. C. Corbett, M. B. Dwyer, C. S. Pasareanu, S. F. Siegel, Comparing Finite-State Verification Techniques for Concurrent Software, University of Massachusetts, Amherst, MA, 1999

4  Thomas Ball, Sriram K. Rajamani, Automatically validating temporal safety properties of interfaces, Proceedings of the 8th international SPIN workshop on Model checking of software, p.103-122, May 2001, Toronto, Ontario, Canada


6  Randal E. Bryant, Symbolic Boolean manipulation with ordered binary-decision diagrams, ACM Computing Surveys (CSUR), v.24 n.3, p.293-318, Sept. 1992


8  Shing-Chi Cheung, Jeff Kramer, Tractable Flow Analysis for Anomaly Detection in Distributed Programs, Proceedings of the 4th European Software Engineering Conference on Software Engineering, p.283-300, September 13-17, 1993

9  Shing Chi Cheung, Jeff Kramer, Context constraints for compositional reachability analysis, ACM Transactions on Software Engineering and Methodology (TOSEM), v.5 n.4, p.334-377, Oct. 1996

10 Edmund M. Clarke, Jr., Orna Grumberg, Doron A. Peled, Model checking, MIT Press, Cambridge, MA, 2000

11 Rance Cleaveland, Joachim Parrow, Bernhard Steffen, The concurrency workbench: a semantics-based tool for the verification of concurrent systems, ACM Transactions on Programming Languages and Systems (TOPLAS), v.15 n.1, p.36-72, Jan. 1993

12 Cliff Click, Keith D. Cooper, Combining analyses, combining optimizations, ACM Transactions on Programming Languages and Systems (TOPLAS), v.17 n.2, p.181-196, March 1995


19 Claudio DeMartini, Radu Iosif, Riccardo Sisto, A deadlock detection tool for concurrent Java programs, Software—Practice & Experience, v.29 n.7, p.577-603, June 1999


22 Matthew Barbour Dwyer, Lori A. Clarke, Data flow analysis for verifying correctness properties of concurrent programs, 1995


25 Matthew B. Dwyer, Lori A. Clarke, Data flow analysis for verifying properties of concurrent programs, Proceedings of the 2nd ACM SIGSOFT symposium on Foundations of software engineering, p.62-75, December 06-09, 1994, New Orleans, Louisiana, United States


information for concurrent Java programs, Proceedings of the 7th European software engineering conference held jointly with the 7th ACM SIGSOFT international symposium on Foundations of software engineering, p.338-354, September 06-10, 1999, Toulouse, France

53 Gleb Naumovich, George S. Avrunin, Lori A. Clarke, Leon J. Osterweil, Applying static analysis to software architectures, Proceedings of the 6th European conference held jointly with the 5th ACM SIGSOFT international symposium on Foundations of software engineering, p.77-93, September 22-25, 1997, Zurich, Switzerland

54 Gleb Naumovich, Lori A. Clarke, Classifying properties: an alternative to the safety-liveness classification, Proceedings of the 8th ACM SIGSOFT international symposium on Foundations of software engineering: twenty-first century applications, p.159-168, November 06-10, 2000, San Diego, California, United States


60 Kurt M. Olender, Leon J. Osterweil, Interprocedural static analysis of sequencing constraints, ACM Transactions on Software Engineering and Methodology (TOSEM), v.1 n.1, p.21-52, Jan. 1992


63 G. Ramalingam, Context-sensitive synchronization-sensitive analysis is undecidable, ACM Transactions on Programming Languages and Systems (TOPLAS), v.22 n.2, p.416-430, March 2000

64 Thomas Reps, Susan Horwitz, Mooly Saqiv, Precise interprocedural dataflow analysis via graph reachability, Proceedings of the 22nd ACM SIGPLAN-SIGACT symposium on Principles of programming languages, p.49-61, January 23-25, 1995, San Francisco, California, United States


72 Jianbin Tan, George S. Avrunin, Lori A. Clarke, Shlomo Zilberstein, Stefan Leue, Heuristic-guided counterexample search in FLAVERS, Proceedings of the 12th ACM SIGSOFT twelfth international symposium on Foundations of software engineering, October 31-November 06, 2004, Newport Beach, CA, USA


76 Willem Visser, Klaus Havelund, Guillaume Brat, SeungJoon Park, Model Checking Programs, Proceedings of the The Fifteenth IEEE International Conference on Automated Software Engineering (ASE'00), p.3, September 11-15, 2000

77 Wei Jen Yeh, Michal Young, Compositional reachability analysis using process algebra, Proceedings of the symposium on Testing, analysis, and verification, p.49-59, October 08-10, 1991, Victoria, British Columbia, Canada


INDEX TERMS

Primary Classification:
  D. Software
  D.2 SOFTWARE ENGINEERING
  D.2.4 Software/Program Verification

Additional Classification:
  D. Software
  D.1 PROGRAMMING TECHNIQUES
  D.1.3 Concurrent Programming
  Subjects: Parallel programming
General Terms:
Verification

Keywords:
Dataflow analysis, finite-state verification, model checking

Collaborative Colleagues:

**Lori A. Clarke:**
- George S. Avrunin
- Daniel J. Barrett
- Frank C. Belz
- Matthew P. Billmers
- A. T. Chamillard
- Albert Timothy Chamillard
- Jamieson M. Cobleigh
- Matthew B. Dwyer
- Matthew Barbour Dwyer
- Michael Evangelist
- Joseph Fialli

**Lori A. Clark:**
- Lori A. Clarke
- Matthew B. Dwyer
- Dimitra Giannakopoulou
- Barbara Staudt Lerner
- Gleb Naumovich
- Leon J. Osterweil
- Corina S. Pasareanu
- Alexander Wise

**Matthew B. Dwyer:**
- George S. Avrunin
- Vicki Carr
- Adam Childs
- Lori A. Clarke
- Jamieson M. Cobleigh
- James C. Corbett
- Matthew J. Craig
- William Deng
- Xianghua Deng
- Xinghua Deng

**Gleb Naumovich:**
- Vikram Anantapadmanabhan
- George S. Avrunin
- Paolina Centonze

**Jeffrey Kramer:**
- Stefan Leue
- Douglas Long
- Douglas L. Long
- Eric K. McCall
- Eric Kenneth Mccall
- Gleb Naumovich
- Gleb N. Naumovich
- Kari A. Nies
- Leon Osterweil
- Leon J. Osterweil

**Andy Podgurski:**
- H. Andy Podgurski
- Debra J. Richardson
- Dieter Rombach
- Arnold L. Rosenberg
- Richard W. Selby
- Timothy J. Sliski
- Rachel L. Smith
- Jianbin Tan
- Peri Tarr
- Peri L. Tarr

**Peri Lynn Tarr:**
- Richard N. Taylor
- Margaret C. Thompson
- Jack C. Wileden
- Alexander E. Wise
- Alexander L. Wolf
- Michael Young
- Steven J. Zeil
- Shlomo Zilberstein

**Jamieson M. Cobleigh:**
- Lori A. Clarke
- Matthew B. Dwyer
- Dimitra Giannakopoulou
- Barbara Staudt Lerner
- Gleb Naumovich
- Leon J. Osterweil
- Corina S. Pasareanu
- Alexander Wise

**Gleb Naumovich:**
- Vikram Anantapadmanabhan
- George S. Avrunin
- Paolina Centonze

**Aleksey Solodovnik:**
- Mikhail Sosonkin

**John Hatcliff:**
- Robby Robby
- Robby Robby
- Roby Eric Runquist
- Gurdirp Singh
- Stefan Sokolowski
- Richard N. Taylor
- Oksana Tkachuk
- Willem Visser
- Hongjun Zheng