Assume-guarantee tools for component-based software verification

Hung P.N., Nguyen V.-H., Aoki T., Katayama T.
College of Technology, Vietnam National University, Hanoi, Viet Nam; School of Information Science, Japan Advanced Institute of Science and Technology, Japan

Abstract: This paper presents a minimized assumption generation method and its associated tools for L*-based assume-guarantee verification of component-based software by model checking. The method is not only fitted to component-based software but also has a potential to solve the state space explosion problem in model checking. In the proposed method, a verification target is decomposed into components so that we can model check each of them separately. The key idea of this method is finding the minimal assumptions in the search spaces of the candidate assumptions. The minimal assumptions generated by the proposed method can be used to recheck the whole system at much lower computational cost. Our experience so far indicates that the implemented tools are potential for verifying practical component-based software. © 2010 IEEE.
Index Keywords: Associated tool; Component based software; Computational costs; Generation method; Model check; Search spaces; State-space explosion; Whole systems; Systems engineering; Model checking

Year: 2010
Source title: Proceedings - 2nd International Conference on Knowledge and Systems Engineering, KSE 2010
Art. No.: 5632130
Page : 172-177
Link: Scorpus Link
Correspondence Address: Hung, P. N.; College of Technology, Vietnam National University, Hanoi, Viet Nam; email: hungpn@vnu.edu.vn
Conference name: 2nd International Conference on Knowledge and Systems Engineering, KSE 2010
Conference date: 7 October 2010 through 9 October 2010
Conference location: Hanoi
Conference code: 83923
ISBN: 9.78077E+12
DOI: 10.1109/KSE.2010.18
Language of Original Document: English
Abbreviated Source Title: Proceedings - 2nd International Conference on Knowledge and Systems Engineering, KSE 2010
Document Type: Conference Paper
Source: Scopus
Authors with affiliations:

- Hung, P.N., College of Technology, Vietnam National University, Hanoi, Viet Nam
- Nguyen, V.-H., College of Technology, Vietnam National University, Hanoi, Viet Nam
- Aoki, T., School of Information Science, Japan Advanced Institute of Science and Technology, Japan

• Katayama, T., School of Information Science, Japan Advanced Institute of Science and Technology, Japan

References:

• Angluin Dana, LEARNING REGULAR SETS FROM QUERIES AND COUNTEREXAMPLES. (1987) Information and Computation, 75 (2), pp. 87-106
• Clarke, E.M., Grumberg, O., Peled, D., (1999) Model Checking, , The MIT Press
• Cobleigh, J.M., Giannakopoulou, D., Pasareanu, C.S., Learning assumptions for compositional verification (2003) Proc. 9th International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS), pp. 331-346. , Poland, April
• Giannakopoulou, D., Pasareanu, C.S., Learning-based assume-guarantee verification (2005) Proc. 12th International SPIN Workshop on Model Checking Software, pp. 282-287. , San Francisco, USA, Aug
• Hung, P.N., Aoki, T., Katayama, T., Modular conformance testing and assume-guarantee verification for evolving component-based software (2009) IEICE Transactions on Fundamentals, E92-A (11), pp. 2772-2780. , Nov
• Hung, P.N., Aoki, T., Katayama, T., An effective framework for assume-guarantee verification of evolving component-based software (2009) Proc. of the IWPSE-EVOL Workshops, pp. 109-118. , ACM, New York, Aug
• Hung, P.N., Aoki, T., Katayama, T., A minimized assumption Generation method for component-based software verification (2009) Proc. 6th International Colloquium on Theoretical Aspects of Computing (ICTAC), 5684, pp. 277-291. , LNCS, Springer-Verlag Berlin Heidelberg, Aug
• Hung, P.N., Katayama, T., Modular conformance testing and assume-guarantee verification for evolving componentbased software (2008) Proc. 15th Asia-Pacific Software Engineering Conference (APSEC), pp. 479-486. , IEEE Computer Society, Washington, DC, Dec
• Jones, C.B., Tentative steps toward a development method for interfering programs (1983) ACM Transactions on Programming Languages and Systems (TOPLAS), 5 (4), pp. 596-619. , Oct
• Magee, J., Kramer, J., (1999) Concurrency: State Models & Java Programs, , John Wiley & Sons
• Nerode, A., Linear automaton transformations (1958) Proc. of the American Mathematical Society, (9), pp. 541-544
• French national institute for research in computer science and control (INRIA) (2004) Objective Caml, , http://caml.inria.fr/ocaml/index.en.html
• Pnueli, A., In transition from global to modular temporal reasoning about programs (1985) Logics and Models of Concurrent Systems, 13, pp. 123-144. , K. R.Apt, Ed. Nato Asi Series F: Computer And Systems Sciences, Springer-Verlag New York
• Stark, E.W., A proof technique for rely/guarantee properties (1985) Proc. 5th Conference on Foundations of Software Technology and Theoretical Computer Science, pp. 369-391
• Rivest, R.L., Schapire, R.E., Inference of finite automata using homing sequences (1993) Information and Computation, 103 (2), pp. 299-347. , April