A minimized assumption generation method for component-based software verification

Pham N.H., Nguyen V.H., Aoki T., Katayama T.

College of Technology, Vietnam National University, Hanoi (VNU), 144 Xuan Thuy, Cau Giay, Hanoi, Viet Nam; School of Information Science, Japan Advanced Institute of Science and Technology (JAIST), Nomi-shi, 923-1292, Japan

Abstract: An assume-guarantee verification method has been recognized as a promising approach to verify component-based software by model checking. This method is not only fitted to component-based software but also has a potential to solve the state space explosion problem in model checking. The method allows us to decompose a verification target into components so that we can model check each of them separately. In this method, assumptions are seen as the environments needed for the components to satisfy a property and for the rest of the system to be satisfied. The number of states of the assumptions should be minimized because the computational cost of model checking is influenced by that number. Thus, we propose a method for generating minimal assumptions for the assumeguarantee verification of component-based software. 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. We have implemented a tool for generating the minimal assumptions. Experimental results are also presented and discussed. Copyright ?? 2010 The Institute of Electronics, Information and Communication Engineers.

Author Keywords: Assume-guarantee reasoning; Learning algorithm; Minimal assumption; Model checking; Modular verification

Index Keywords: Assume-guarantee reasoning; Component based software; Computational costs; Generation method; Minimal assumption; Model check; Modular verification; Number of state; Search spaces; State-space explosion; Verification method; Whole systems; Computer software selection and evaluation; Learning algorithms; Model checking

Year: 2010
Source title: IEICE Transactions on Information and Systems
Volume: E93-D
Issue: 8
Page : 2172-2181
Link: Scorpus Link
Correspondence Address: Pham, N. H.; College of Technology, Vietnam National University, Hanoi (VNU), 144 Xuan Thuy, Cau Giay, Hanoi, Viet Nam; email: hungpn@vnu.edu.vn
ISSN: 9168532
CODEN: ITISE
DOI: 10.1587/transinf.E93.D.2172
Language of Original Document: English

Abbreviated Source Title: IEICE Transactions on Information and Systems

Document Type: Conference Paper

Source: Scopus

Authors with affiliations:

1. Pham, N.H., College of Technology, Vietnam National University, Hanoi (VNU), 144 Xuan Thuy, Cau Giay, Hanoi, Viet Nam
2. Nguyen, V.H., College of Technology, Vietnam National University, Hanoi (VNU), 144 Xuan Thuy, Cau Giay, Hanoi, Viet Nam
3. Aoki, T., School of Information Science, Japan Advanced Institute of Science and Technology (JAIST), Nomi-shi, 923-1292, Japan
4. Katayama, T., School of Information Science, Japan Advanced Institute of Science and Technology (JAIST), Nomi-shi, 923-1292, Japan

References:

1. (2009) A Minimized Assumption Generation Tool for Modular Verification of Component-Based Software, , http://www.jaist.ac.jp/s0620204/MAGTool/
2. Angluin, D., Learning regular sets from queries and counterexamples (1987) Inf. Comput., 75 (2), pp. 87-106. , Nov
3. Blundell, C., Giannakopoulou, D., Pasareanu, C., Assumeguarantee testing (2005) Proc. 4th Microsoft Research -Specification and Verification of Component-Based Systems Workshop (SAVCBS), pp. 7-14. , Portugal, Sept
4. Chaki, S., Sharygina, N., Sinha, N., Verification of evolving software (2004) Proc. 3rd Microsoft Research -Specification and Verification of Component-Based Systems Workshop, pp. 55-61. , California, USA, Nov
5. Chaki, S., Strichman, O., Three optimizations for assumeguarantee reasoning with L* (2008) Formal Methods in System Design, 32 (3), pp. 267-284. , June
6. Clarke, E.M., Grumberg, O., Peled, D., (1999) Model Checking, , The MIT Press
7. Cobleigh, J.M., Giannakopoulou, D., Pasareanu, C., Learning assumptions for compositional verification (2003) Proc. 9th TACAS, pp. 331-346. , Poland, April
8. Giannakopoulou, D., Pasareanu, C., Barringer, H., Assumption generation for software component verification (2002) Proc. 17th IEEE Int. Conf. on Automated Softw. Eng., pp. 3-12. , Edinburgh, UK, Sept
9. Hung, P.N., Aoki, T., Katayama, T., Modular conformance testing and assume-guarantee verification for evolving componentbased software (2009) IEICE Trans. Fundamentals, E92-A (11), pp. 2772-2780. , Nov
10. 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), LNCS 5684, pp. 277-291. , Springer-Verlag Berlin Heidelberg, Aug
11. Hung, P.N., Katayama, T., Modular conformance testing and assume-guarantee verification for evolving component-based software (2008) Proc. 15th Asia-Pacific Softw. Eng. Conf. (APSEC), IEEE Computer Society, pp. 479-486. , Washington, DC, Dec
12. Jones, C.B., Tentative steps toward a development method for interfering programs (1983) ACM Trans. Programming Languages and Systems (TOPLAS), 5 (4), pp. 596-619. , Oct
13. Magee, J., Kramer, J., (1999) Concurrency: State Models & Java Programs, , John Wiley & Sons
14. Nerode, A., Linear automaton transformations (1958) Proc. American Mathematical Society, (9), pp. 541-544
15. (2004) French National Institute for Research in Computer Science and Control (INRIA), , http://caml.inria.fr/ocaml/index.en.html, Objective caml

16. Pnueli, A., In transition from global to modular temporal reasoning about programs (1985) Logics and Models of Concurrent Systems, 13, pp. 123-144. , ed. K.R. Apt, Nato Asi Series F: Computer and Systems Sciences, Springer-Verlag New York

17. Stark, E.W., A proof technique for rely/guarantee properties (1985) Proc. 5th Conf. on Found. of Soft. Tech. and Theoretical Computer Science, pp. 369-391

18. Rivest, R.L., Schapire, R.E., Inference of finite automata using homing sequences (1993) Inf. Comput., 103 (2), pp. 299-347. , April