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.

Authors with affiliations:

- Pham, N.H., College of Technology, Vietnam National University, Hanoi (VNU), 144 Xuan Thuy, Cau Giay, Hanoi, Viet Nam

- Nguyen, V.H., College of Technology, Vietnam National University, Hanoi (VNU), 144 Xuan Thuy, Cau Giay, Hanoi, Viet Nam

- Aoki, T., School of Information Science, Japan Advanced Institute of Science and Technology (JAIST), Nomi-shi, 923-1292, Japan

- Katayama, T., School of Information Science, Japan Advanced Institute of Science and Technology (JAIST), Nomi-shi, 923-1292, Japan

References:

- (2009) A Minimized Assumption Generation Tool for Modular Verification of Component-Based Software, , http://www.jaist.ac.jp/s0620204/MAGTool/

- Angluin, D., Learning regular sets from queries and counterexamples (1987) Inf. Comput., 75 (2), pp. 87-106. , Nov

- 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

- 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

- Chaki, S., Strichman, O., Three optimizations for assumeguarantee reasoning with L* (2008) Formal Methods in System Design, 32 (3), pp. 267-284. , June

- Clarke, E.M., Grumberg, O., Peled, D., (1999) Model Checking, , The MIT Press

- Cobleigh, J.M., Giannakopoulou, D., Pasareanu, C., Learning assumptions for compositional verification (2003) Proc. 9th TACAS, pp. 331-346. , Poland, April

- 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

- 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

- 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

- 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

- 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

- Magee, J., Kramer, J., (1999) Concurrency: State Models & Java Programs, , John Wiley & Sons

- Nerode, A., Linear automaton transformations (1958) Proc. American Mathematical Society, (9), pp. 541-544

- (2004) French National Institute for Research in Computer Science and Control (INRIA), , http://caml.inria.fr/ocaml/index.en.html, Objective caml

- 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

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