Locating Software Faults Based on Minimum Debugging Frontier Set

Feng Li, Zhiyuan Li, Wei Huo and Xiaobing Feng

Abstract—In this article, we propose a novel state-based fault-localization approach. Given an observed failure that is reproducible under the same program input, this new approach uses two main techniques to reduce the state exploration cost. Firstly, the execution trace to be analyzed for the observed failure is successively narrowed by making the set of trace points in each step a cut of the dynamic dependence graph. Such a cut divides the remaining trace into two parts and, based on the *sparse symbolic exploration* outcome, one part is removed from further exploration. This process continues until reaching where the fault is determined to be. Secondly, the cut in each step is chosen such that the union of the program states from the members of the cut is of the minimum size among all candidate cuts. The set of statement instances in the chosen cut is called a *minimum debugging frontier set* (MDFS). To evaluate our approach, we apply it to 16 real bugs from real world programs and compare our fault reports with those generated by state-of-the-art approaches. Results show that the MDFS approach obtains high quality fault reports for these test cases with considerably higher efficiency than previous approaches.

Index Terms—Fault Localization, Minimum Debugging Frontier Set, Sparse Symbolic Exploration, Dynamic Dependence Graph

- *F. Li is with the State Key Laboratory of Computer Architecture, Institute of Computing Technology, Chinese Academy of Sciences. E-mail: lifeng2005@ ict.ac.cn.*
- *Z. Li is with the Department of Computer Science, Purdue University. E-mail: zhiyuanli@purdue.edu.*
- *H. Wei is with the Institute of Information Engineering, Chinese Academy of Sciences. E-mail: huowei@iie.ac.cn.*
- *X. Feng is with the State Key Laboratory of Computer Architecture, Institute of Computing Technology, Chinese Academy of Sciences. E-mail: fxb@ ict.ac.cn.*