Researches on Automatic Techniques for Specification-Based Testing and Fault Localization

WANG, Rong / 王, 榕

(開始ページ / Start Page)
1
(終了ページ / End Page)
143
(発行年 / Year)
2022-03-24
(学位授与番号 / Degree Number)
32675甲第547号
(学位授与年月日 / Date of Granted)
2022-03-24
(学位名 / Degree Name)
博士(理学)
(学位授与機関 / Degree Grantor)
法政大学 (Hosei University)
(URL)
https://doi.org/10.15002/00025230

博士学位論文
論文内容の要旨および審査結果の要旨

論文題目	Researches on Automatic Techniques for Specification-Based Testing and Fault Localization
氏名	WANG　Rong
学位の種類	博士（理学）
学位番号	第 547 号
学位授与年月日	2022 年 3 月 24 日
学位授与の要件	法政大学学位規則第 5 条第 1 項第 1 号該当者（甲）
論文審査委員	主　査　馬　　建華　　教授
	副　査　細部　博史　　教授
	副　査　佐藤　裕二　　教授
	副　査　劉　　少英　　教授（広島大学）

１．論文内容の要旨

To address the problems of difficulty in generating an appropriate test suite and path explosion during an exhausted test data generation, the doctoral thesis presents a specification-based incremental testing method with symbolic execution, called SIT-SE, to provide a much more rigorous way to automatically check the functional correctness of all the discovered program paths within limited time. Moreover, the thesis presents a strategy of fault localization called TRIACFL to give useful hints to pinpoint the faults in a small set of statements. The thesis also gives a test data generation method that integrates formal specification with a genetic algorithm as supplementary to the SIT-SE for dealing with exceptional cases. Several experiments are conducted with the proposed methods, and the experimental results demonstrate that these proposed methods together facilitate an effective automatic bug detection.

２．審査結果の要旨

Automatic testing is very important in software verification to automatically evaluate quality of programs, check bug existence and further locate bugs in the programs. There have been a lot of studies and tools, but the challenges remain, especially the low precision in detecting existence of various bugs and the high computational cost in locating faults. To tackle with the two challenges, a specification-based incremental testing method with symbolic execution (SIT-SE) has been proposed to automatically verify the correctness of all the discovered representative program paths. Different from traditional symbolic testing methods using assertions, the proposed SIT-SE introduces theorems for checking path

correctness and provides a Branch Sequence Coverage (BSC) algorithm for guiding a moderate path exploration. The proposed method has made a good balance between a path condition and the specification in a theorem to reduce the monotonous path exploration.

To make use of the information on the correctness of program paths provided by the SIT-SE, a strategy of triple interaction-based fault localization (TRIACFL) is further proposed with integrating an elementary fault location generation algorithm and an attentional shift-based review. Experimental results have demonstrated that the proposed approach can help testers to effectively pinpoint the fault on a smaller set of suspicious locations in the meantime inspect fewer lines of codes and fewer program paths.

Moreover, a new method for effective test data generation is proposed based on mutated pre-post style formal specifications. The method is characterized by the integration of the functional scenario-based testing, a genetic algorithm (GA) and the mutation testing. The two classic case studies have been carried out to evaluate the performance of this method, and the results have demonstrated that the proposed approach is capable of effectively generating useful test data to kill as many program mutants as possible, which outperforms the conventional data generation method.

In the pre-examination period, the pre-examination committee gave various questions/comments on further improvements of the first submitted doctoral thesis. These comments were mainly in following three aspects.

1) Clearer illustrations of special features or differences of proposed methods from existing research done by others. Such as, what is the biggest advantage of SIT-SE over traditional specification-based testing technology? what is the most challenging thing if you build a tool to automatically support this method? Why did you select KLEE and SBFL-SSE as the references for comparison? What is the difference from the other's method also using GA?
2) More sufficient descriptions on considerations and conditions in experiments or case studies. Such as, how did you collect programs for your experiments? are the classic programs enough to prove your proposal? what kinds of bugs were included in the programs? is it better to make a table about the bugs?
3) Better presentations in showing some result and remaining work. Such as, Figure 4.27 includes different scales, better to use tables. And, there are not enough discussions on technical problems remained and how to possibly handle them.

The detailed responses to the above comments have been reported to the committee, and the corresponding revisions in the final submission of doctoral thesis have checked and confirmed by this examination committee.

In summary, the submitted doctoral thesis has shown its novelty in the proposed methods as well as solid results by the experiments and the case studies. In addition, the questions raised in the dissertation defense have been well answered by the applicant. Based on all of these, this examination committee is unanimous that the submitted doctoral thesis is fully qualified as a Doctor of Philosophy (Science).

以上