Essential Spectrum-based Fault Localization

Xiaoyuan Xie • Baowen Xu

Essential Spectrum-based Fault Localization

Springer

Xiaoyuan Xie
School of Computer Science
Wuhan University
Wuhan, Hubei, China

Baowen Xu
Department of Computer Science
and Technology
Nanjing University
Nanjing, Jiangsu, China

ISBN 978-981-33-6178-2 ISBN 978-981-33-6179-9 (eBook)
https://doi.org/10.1007/978-981-33-6179-9

Foreword

I never forget the day when I first realized the importance of software quality. It was in 1979 when I was doing my undergraduate study and introduced to programming language. One day, I learned the story about Mariner 1, the first spacecraft in the American Mariner program, which was launched on July 22, 1962, but had to be destroyed after veering off course due to equipment failure and an error in coded computer instructions. The post-flight review found that a missing hyphen in coded computer instructions allowed transmission of incorrect guidance signals. Even though this mission was later achieved by Mariner 2, the loss of Mariner 1 was as high as 18.5 million US dollars. Significantly, this epic software bug impressed me and influenced my following academic career.

After I started my master's degree program supervised by Prof. Zhenyu Wang, I gained a deeper understanding of programming languages (such as Ada, AED, ALGOL60, ALGOL68, ALGOL W, APL, BASIC, BCPL, BLISS, C, CLU, COBOL, Concurrent Pascal, CORAL66, Edison, Eiffel, Euclid, Euler, FORTH, FORTRAN IV, FORTRAN 77, GPSS, JOVIAL, LIS, LISP, Modula, Modula-2, Modula-3, NPL, Oberon, Pascal, PL/I, PL/M, PLZ/SYS, PROLOG, SETL, SIMULA, SmallTalk, SNOBOL, SPL/I). In that age, though programs were not in large scale or with complex structures, testing and debugging were actually very challenging due to the lack of supporting mechanisms and facilities. Initiated by my study on programming language principles, design, and implementation, a belief that I should also do studies on software quality assurance becomes stronger and stronger.

I was one of the first researchers who systematically studied software quality in China. In 1986, I published the first paper in China, enumerating various issues in C programming languages that can introduce risks in software. I also compared several popular programming languages in that age, such as Ada and Pascal, discussing principles and metrics for good programming languages. Right around the same time, I worked on program analysis and slicing. I proposed a method for backward dependence analysis. Under my supervision, my students also developed a series of methods for static and dynamic program analysis, dependence analysis in concurrent programs, monadic slicing for programs with pointers, etc.

Since 1995, we have started to realize the importance of software measurements in producing high-quality software systems. We proposed approaches to measuring class cohesion based on dependence analysis, package cohesion based on client usage, and methods to further improve software architecture design. Around 2000, we initiated our first project on software testing. After that, my research group kept putting many efforts in this area, and have harvested abundant achievements over the past two decades, which cover combinatorial testing, regression testing, evolutionary testing, metamorphic testing, web testing, and test case prioritization and reduction. We also cared about software reliability and security. Based on the accumulations in testing and analysis, our group was able to develop a series of theories and methodologies in software fault localization and defect prediction, which have exerted profound influences in these areas. Recently, we expanded our directions to testing and debugging for artificial intelligent systems, crowdsourcing software engineering, empirical software engineering, and knowledge graph.

Over the past 30 years, our group has obtained many important research results, which are highly praised by international peers and exert great impact in relevant fields. We have undertaken over 70 research projects from the National Natural Science Foundation of China, the Ministry of Education, the Ministry of Science and Technology, Jiangsu Province, institutions, and famous enterprises. The group has published more than 500 papers, including top venues such as *ACM Transactions on Software Engineering and Methodology*, *IEEE Transactions on Software Engineering*, the International Conference on Software Engineering, The ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering, and the International Joint Conference on Artificial Intelligence. We have also built close connections and collaboration with many prestigious universities and institutes, including Purdue University, Nanyang Technological University, University of California Irvine, University College London, and Columbia University.

We have developed multiple systems including CRL/Ada language and its generation system, Ada program analysis and understanding system (APAUS), software maintenance and support system for Ada reverse engineering (ARMS), embedded software testing support system (ETS), software quality assurance system (SQAS), and testing platform for large and complex systems (Testeres). Through participation in various projects, we also built up large-scale benchmarks of real-life data. From these data, we conducted empirical studies and have provided useful and convincing insights.

Such a long period of research gives us good accumulation in both theory and practice. And hence we are planning a series of books on relevant areas of program analysis, testing, and evolution. We hope they will appear in the near future.

Nanjing University, China Baowen Xu

Preface

Program debugging has always been a difficult and time-consuming task in software development. Back in the 1970s, when researchers proposed the concept of program slicing, automatic program fault localization became an ambition for efficiently debugging the program. Since then, various trials were performed to get closer to this goal, among which spectrum-based fault localization (SBFL) is one of the most widely studied families of techniques.

SBFL was first proposed around 2000. Different from traditional slicing-based methods, SBFL became popular because of its lightweight and practicability. Since 2000, this area has seen thousands of techniques derived from various perspectives. As a consequence, it becomes very important and urgent to compare the actual performance among different SBFL techniques. In fact, before 2013, many empirical studies were conducted to investigate this question. However, they were strongly dependent on the experimental setup, and hence can hardly be considered as sufficiently comprehensive due to the huge number of possible combinations of various factors in SBFL. In other words, these empirical studies did not reveal the essence of SBFL performance.

Therefore, we propose to draft this book, whose orientation is not to introduce various SBFL techniques, or to compare their empirical performance. Instead, this book aims to provide a deep understanding on the essence of this area, talking about its essential theories. Specifically, this book introduces a series of set-based theoretical frameworks, which reveal the intrinsic performance hierarchy among different SBFL techniques. In addition, this book also discusses two emerging challenges of "oracle problem" and "multiple faults" and introduces promising solutions.

The target audience of this book are mainly graduate students and researchers who work in the areas of software analysis, testing, debugging, and repairing, and are seeking deep comprehension of SBFL.

Wuhan University, China — Xiaoyuan Xie
Nanjing University, China — Baowen Xu

Acknowledgments

Our research is partially supported by the National Natural Science Foundation of China under Grant numbers 61832009, 61972289, 61772263, 61572375, 61472178, 91418202, 61170071.

We want to express our gratitude to our long-term collaborators (alphabetic order on the surnames):

- Prof. Tsong Yueh Chen (Swinburne University, Australia)
- Prof. Yang Liu (Nanyang Technological University, Singapore)
- Prof. T. H. Tse (Hong Kong University)
- Prof. W. Eric Wong (University of Texas at Dallas, USA)
- Prof. Shin Yoo (Korea Advanced Institute of Science and Technology, South Korea)
- Prof. Xiangyu Zhang (Purdue University, USA)

We sincerely thank the graduate student Yi Song in our group for his contributions in editing. We also sincerely appreciate the constructive suggestions from the reviewers, as well as the efforts of Springer Editor Jane Li and Project Coordinator Priya Shankar.

Contents