The application perspective of mutation testing

Zhu, Qianqian

DOI
10.4233/uuid:116a487e-c14d-47f8-b1f5-8e9738d263d0

Publication date
2020

Document Version
Final published version

Citation (APA)
Zhu, Q. (2020). The application perspective of mutation testing. https://doi.org/10.4233/uuid:116a487e-c14d-47f8-b1f5-8e9738d263d0

Important note
To cite this publication, please use the final published version (if applicable). Please check the document version above.

Copyright
Other than for strictly personal use, it is not permitted to download, forward or distribute the text or part of it, without the consent of the author(s) and/or copyright holder(s), unless the work is under an open content license such as Creative Commons.

Takedown policy
Please contact us and provide details if you believe this document breaches copyrights. We will remove access to the work immediately and investigate your claim.
THE APPLICATION PERSPECTIVE OF MUTATION TESTING
THE APPLICATION PERSPECTIVE OF MUTATION TESTING

Proefschrift

ter verkrijging van de graad van doctor
aan de Technische Universiteit Delft,
op gezag van de Rector Magnificus prof. dr. ir. T.H.J.J. van der Hagen,
voorzitter van het College voor Promoties,
in het openbaar te verdedigen op woensdag 24 juni 2020 om 12:30 uur

door

Qianqian ZHU

Master of Science in Computer Science,
Imperial College London, Verenigd Koninkrijk,
geboren te Wenzhou, China.
Dit proefschrift is goedgekeurd door de
promotoren: prof. dr. A. Zaidman, prof. dr. A. van Deursen
copromotor: dr. A. Panichella

Samenstelling promotiecommissie:

Rector Magnificus, voorzitter
Prof. dr. A. Zaidman, Technische Universiteit Delft
Prof. dr. A. van Deursen, Technische Universiteit Delft
dr. A. Panichella, Technische Universiteit Delft

Onafhankelijke leden:
Prof. dr. ir. R.L. Lagendijk Technische Universiteit Delft
Prof. dr. T.E.J. Vos Technical University of Valencia, Spain & Open University, the Netherlands.
Prof. dr. R. Feldt Chalmers University of Technology, Sweden
Prof. dr. M. Monperrus KTH Royal Institute of Technology, Sweden.
Prof. dr. E. Visser Technische Universiteit Delft, reservelid

The work in the thesis has been carried out under the auspices of the research school IPA (Institute for Programming research and Algorithmics) and was financed by the Nederlandse Organisatie voor Wetenschappelijk Onderzoek (NWO), project TestRoots, grant number 016.133.324.

Keywords: Software Testing, Mutation Testing, Software Quality...
Printed by: Gildeprint
Front & Back: Beautiful cover art that captures the entire content of this thesis in a single illustration.

Copyright © 2020 by Q. Zhu
ISBN 000-00-0000-000-0
An electronic version of this dissertation is available at http://repository.tudelft.nl/.
# Contents

Summary xi

Acknowledgements xi

1 Introduction 1
   1.1 Mutation Testing 2
   1.2 Research Questions 4
   1.3 Research Methodology 8
   1.4 Contributions and Thesis Outline 10

2 A SLR of How Mutation Testing Supports Quality Assurance Processes 13
   2.1 Introduction 14
   2.2 Background 15
      2.2.1 Basic Concepts 15
      2.2.2 Historical Overview 18
      2.2.3 Comparisons with existing literature surveys 19
   2.3 Research Method 20
      2.3.1 Research Questions 21
      2.3.2 Study Selection Strategy 23
      2.3.3 Data Extraction Strategy 25
      2.3.4 Review Protocol Validation 34
   2.4 Review Results 35
      2.4.1 RQ2.1: How is MT used in quality assurance processes? 36
      2.4.2 RQ2.2: How are empirical studies related to mutation testing designed and reported? 43
      2.4.3 Summary of Research Questions 57
      2.4.4 Recommendation for Future Research 59
   2.5 Threats to the Validity of this Review 61
      2.5.1 Article Selection 62
      2.5.2 Attribute Framework 62
      2.5.3 Article Characterisation 63
      2.5.4 Result Interpretation 63
   2.6 Conclusion 63

3 An Investigation of Compression Techniques to Speed up MT 65
   3.1 Introduction 66
   3.2 Background and Related Work 67
      3.2.1 Mutation Reduction Strategies 67
      3.2.2 Mutant Compression 69
3.3 Approach .................................................. 70
  3.3.1 Overall Methodology ........................................ 70
  3.3.2 overlapped grouping ....................................... 71
  3.3.3 Mutation Knowledge ....................................... 72
3.4 Experimental study ............................................ 72
  3.4.1 Experimental setup ........................................ 73
  3.4.2 Evaluation Metrics ....................................... 74
3.5 Results .................................................. 76
  3.5.1 RQ3.1: accuracy ......................................... 76
  3.5.2 RQ3.2: speed-up ......................................... 79
  3.5.3 RQ3.3: trade-offs ....................................... 81
  3.5.4 Discussion .............................................. 82
3.6 Threats to Validity .......................................... 83
3.7 Conclusions ................................................ 83

4 An Exploratory Study on the Impact of Code Observability on MT .................................................. 87
  4.1 Introduction ............................................... 88
  4.2 Background .............................................. 89
    4.2.1 Mutation Testing .................................... 89
    4.2.2 Existing Object-Oriented Metrics for Testability ............. 90
    4.2.3 Code Observability ................................... 90
  4.3 Experimental Setup ......................................... 95
    4.3.1 Mutation Testing .................................... 96
    4.3.2 Subject Systems ..................................... 97
    4.3.3 Tool implementation .................................. 97
    4.3.4 Design of Experiment ................................ 100
    4.3.5 Evaluation Metrics .................................. 102
  4.4 RQ4.1 - RQ4.3 testability versus observability versus combination .................... 103
    4.4.1 Spearman’s rank order correlation ....................... 103
    4.4.2 Random Forest ....................................... 105
  4.5 RQ4.4 Code Refactoring .................................... 109
    4.5.1 Case 1: plot.MeterPlot: :drawValueLabel from JFreeChart .................. 112
    4.5.2 Case 2: axis.SymbolAxis: :drawGridBands from JFreeChart .......... 113
    4.5.3 Case 3: builder.IDKey: :hashCode from Apache Commons Lang ....... 114
    4.5.4 Case 4: AbstractCategoryItemRenderer: :drawOutline from JFreeChart .......... 114
    4.5.5 Case 5: builder.ToStringStyle: :setUseShortClassName from Apache Commons Lang ....... 115
    4.5.6 Case 6: exception.TooManyEvaluationsException: :<init> from Apache Commons Math ....... 116
    4.5.7 RQ4.4 Summary ....................................... 118
    4.5.8 Discussion ........................................... 118
  4.6 Threats to Validity ........................................ 119
  4.7 Related work ............................................. 120
  4.8 Conclusion & Future Work ................................ 121
5 Mutation Testing for Physical Computing 123
   5.1 Introduction ................................................. 124
   5.2 Background and motivation .................................. 124
       5.2.1 Physical computing ...................................... 125
       5.2.2 Mutation Testing ........................................ 125
       5.2.3 Characteristics of Physical Computing ................. 125
   5.3 Designing Mutation Operators ................................ 126
   5.4 Tool Implementation ......................................... 129
   5.5 Empirical Evaluation ........................................ 129
       5.5.1 Case Studies with Raspberry Pi ....................... 130
       5.5.2 Case Studies with Arduino ............................ 139
       5.5.3 Summary ................................................ 143
   5.6 Threats to Validity ......................................... 144
   5.7 Related work ................................................. 144
   5.8 Conclusion & Future Work .................................... 145

6 Applying Mutation Testing to GPU Programs 147
   6.1 Introduction ................................................. 148
   6.2 Background ................................................ 149
       6.2.1 GPU computing .......................................... 149
       6.2.2 Example of GPU Programming ......................... 150
   6.3 Motivation ................................................ 151
   6.4 Mutation Operators for GPU Programming .................. 152
       6.4.1 GPU-Specific Mutation Operators ..................... 152
       6.4.2 Conventional Mutation Operators .................... 156
       6.4.3 GPU-specific v.s. Conventional Mutation Operators . 156
   6.5 Tool Implementation ........................................ 157
   6.6 Empirical Evaluation ....................................... 158
       6.6.1 Subject Systems ....................................... 158
       6.6.2 Experimental Setup ................................... 158
   6.7 Results ...................................................... 159
   6.8 Threats To Validity ....................................... 166
   6.9 Related Work .............................................. 167
   6.10 Conclusion and Future Work ................................. 167

7 Conclusion 169
   7.1 Research Questions Revisited ............................... 169
   7.2 Threats to Validity ....................................... 171
   7.3 Recommendations for future work ......................... 172

References 175

Curriculum Vitae 207

List of Publications 209
The main goal of this thesis is to investigate, improve and extend the applicability of mutation testing. To seek the potential directions of how to improve and extend the applicability of mutation testing, we have started with a systematic literature review on the current state of how mutation testing is applied. The results from the systematic literature review have further guided us towards three directions of research: (1) speeding up mutation testing; (2) deepening our understanding of mutation testing; (3) exploring new application domains of mutation testing.

For the first direction, we have leveraged compression techniques and weak mutation information to speed up mutation testing. The results have shown our proposed mutant compression techniques can effectively speed up strong mutation testing up to 94.3 times with an accuracy > 90%. Given the second direction, we are interested in gaining a better understanding of mutation testing especially in the situation where engineers cannot kill all the mutants by just adding test cases. We have investigated the relationships between code quality regarding the testability and observability, and the mutation score. We have observed a correlation between observability metrics and the mutation score. Furthermore, relatively simple refactoring operations/adding tests enable an increase in the mutation score.

As for the third direction, we have explored two new application domains: one is physical computing, and the other is GPU programming. In both application domains, we have designed new mutation operators based on our observations of the common mistakes that could happen during the implementation of the software. We have found promising results in that mutation testing can help in revealing weaknesses of the test suite for both application domains.

In summary, we have improved the applicability of mutation by proposing a new speed-up approach and investigating the relationship between testability/observability and mutation testing. Also, we have extended the applicability of mutation testing in physical computing and GPU programming domains.
ACKNOWLEDGEMENTS

First of all, I would like to thank my supervisor and promotor Prof. Dr. Andy Zaidman for his great support during my 4-year PhD research. Without his offer, I would never have this opportunity to start a PhD journey. Also, despite his busy schedule, he is always willing to answer my endless questions and give me numerous helpful suggestions during the four years. He is unstinting in his expertise and experience to guide me: to set my topic, to frame each of my chapters and to work towards this thesis in a structured way. In the meanwhile, he encouraged me and praised me for every progress I made for my research.

I am also greatly indebted to my family who supports my oversea study not only financially but also mentally. They never stop encouraging me and cheering me up from the distance. Thank you is not enough for my husband, Ce, who always supports me unconditionally and listens to my endless nagging.

Finally, I would like to thank all my friends and colleagues for accompanying me and providing great help during my PhD research. Without them, the four years would not have been so colourfully and unforgettable.
Software testing has always been a hot topic in the research field of software engineering [77]. The critical goal of software testing is to ensure high quality and reliable software programs. In 1972, Dijkstra made the well-known statement that “program testing can be used to show the presence of bugs, but never to show their absence” [124]. His saying indicates that testing is not the silver bullet for software quality. Later, Goodenough and Gerhart [159] proved that properly structured tests are capable of demonstrating the absence of errors in a program. This finding opened up the new research domain of “test criteria” [386]. Various test criteria have been proposed and studied over the last four decades, such as statement coverage, branch coverage and mutation adequacy [386]. The first two criteria, statement coverage and branch coverage, are both under the category of structural coverage criteria; this category specifies testing requirements in terms of the coverage of a particular set of elements in the structure of the program or the specification [386]. Different from structural coverage criteria, mutation adequacy is introduced by mutation testing (or mutation analysis) [117, 168, 230], a fault-based testing technique that assesses the test suite quality by systematically introducing small artificial faults [197]. The mutation adequacy score is used to measure the effectiveness of a test set in terms of its ability to detect faults.

Mutation testing originated in the 1970s with works from Lipton [230], DeMillo et al. [117] and Hamlet [168] and has been a very active research field over the last few decades. The activeness of the field is in part evidenced by the extensive survey of more than 390 papers on mutation testing that Jia and Harman published in 2011 [197]. Jia and Harman’s survey highlights the research achievements that have been made over the years, including theories, problems, cost reduction techniques, applications, empirical evaluation, and tools [197]. This literature review was later extended by Papadakis et al. [289] with more recent advances in mutation testing.

While existing surveys (e.g., [197, 241, 279]) provide us with a great overview of the most influential realisations in research, we lack insight into how mutation testing is actually applied. This thesis focuses on the applicability of mutation testing. We first aim to understand the current state of how mutation testing is applied in a research context,
thereby not excluding industrial practice, and then improve and extend the applicability of mutation testing.

1.1. Mutation Testing

The idea behind mutation testing is based on two fundamental hypotheses: the Competent Programmer Hypothesis [117] and the Coupling Effect [117, 268]. DeMillo et al. [117] introduced the Competent Programmer Hypothesis in 1978: “The competent programmers create programs that are close to being correct.” This hypothesis implies that the potential faults in the programs delivered by the competent programmers are just very simple mistakes; these defects can be corrected by a few simple syntactical changes. Thereby, mutation testing typically applies small syntactical changes to original programs to resemble faults made by “competent programmers”.

The Coupling Effect further strengthens the first hypothesis by stating: “Test data that distinguishes all programs differing from a correct one by only simple errors is so sensitive that it also implicitly distinguishes more complex errors” [117]. This means complex faults are coupled to simple faults. As a result, the mutants used in traditional mutation testing are only limited to first-order mutants, which are created by applying the mutation operator to the original program once.

The most widely-known mutation operators (also called mutant operators or mutation rules) include Arithmetic Operator Replacement (AOR), Relational Operator Replacement (ROR) and Absolute Value Insertion (ABS). Here is an example of AOR mutation operator: \( x = a + b \) is mutated to \( x = a - b \), \( x = a \times b \), and \( x = a ÷ b \).

The execution results of \( T \) on \( P_m \) are compared with \( P \): (1) if the output of \( P_m \) is different from \( P \), then \( P_m \) is killed by \( T \); (2) otherwise, i.e., the output of \( P_m \) is the same as \( P \), this leads to either (2.1) \( P_m \) being equivalent to \( P \), which means that they are syntactically different but functionally equivalent; or (2.2) \( T \) being not adequate to detect the mutants, which requires test case augmentation. The result of mutation testing can be represented by the mutation score (also referred to as mutation coverage or mutation adequacy), which is defined as:

\[
\text{mutation score} = \frac{\# \text{killed mutants}}{\# \text{nonequivalent mutants}} \quad (1.1)
\]

A mutation testing system can be regarded as a language system [47] since the pro-
1.1. Mutation Testing

grams under test must be parsed, modified and executed. The main components of mutation testing consist of the mutant creation engine, the equivalent mutant detector, and the test execution runner. There have been numerous mutation testing tools developed for different programming languages, such as Proteum [113] for C, Mujava [240] and PiTest [13] for Java, and SQLMutation [342] for SQL.

The benefits of mutation testing have been extensively investigated and can be summarised as [197]: 1) having better fault exposing capability compared to other test coverage criteria [144, 228, 244], 2) being an excellent alternative to real faults and providing a good indication of the fault detection ability of a test suite [50]. However, the limita-
tions of mutation testing are inherent. Firstly, it requires to re-run the test suites against each mutant, whose number increases exponentially with the size of the program under test [93]. Also, the equivalent mutant detection is an inevitable stage of mutation testing which is a prominent undecidable problem [91], thereby requiring human effort to investigate. In summary, the major limitations of mutation testing are as follows: 1) the high computational cost caused by generating and executing the numerous mutants and, 2) the tremendous time-consuming human investigation required for equivalent mutant detection.

To address the issue of high computational cost, several methods have been proposed and these can be classified in three main categories [277]: (do fewer) selecting fewer mutants to evaluate [41, 271], (do smarter) using run-time information to avoid unnecessary test executions [185, 200], (do faster) reducing the execution time for each single mutant [344]. As for the equivalent mutant problem, in Madeyski et al. [241]’s survey, they classified three main research directions: (1) detecting equivalent mutants, such as Baldwin and Sayward [63] (using compiler optimisations), and Martin and Xie [242] (through change-impact analysis); (2) avoiding equivalent mutant generation, such as Mresa and Bottaci [258] (through selective mutation), and Harman et al. [174] (using program dependence analysis); (3) suggesting equivalent mutants, such as dynamic invariants analysis [312], and coverage change examination (e.g., [314]).

More recently, the usefulness of mutants [203] has resulted in an increasing interest by researchers. Several studies claimed that the majority of the mutants generated by existing mutation operators are equivalent, trivial and redundant [88, 198, 203, 219, 295], which reduces the efficacy of the mutation score. To address this knowledge gap, numerous studies have investigated how useful mutants are. Example studies include mutant subsumption [219], stubborn mutants [373], and real-fault coupling [201, 295]. Mutant subsumption, which was proposed by Bob Kurtz et al. [219], is a graph model to describe the relationships among mutants, and can thus be used to eliminate the redundant mutants. Stubborn mutants are a set of mutants that remain alive and that cannot be shown to be equivalent [177]. Yao et al. [373] reported on the causes and prevalence of equivalent mutants and their relationship to stubborn mutants based on a manual analysis of 1230 mutants. The investigations on the relation between mutants and real faults (real-fault coupling) can be dated back to 1992 [118]. Recent works are based on large-scale empirical studies using real-world programs, such as Just et al. [201] and Papadakis et al. [295].

1.2. RESEARCH QUESTIONS

In this section, we summarise the research questions we propose for this thesis in order to achieve our goal: to investigate, improve and extend the applicability of mutation testing.

The first step is to investigate the current state of how mutation testing is applied. To understand how mutation testing is actually applied (RQ21 in Chapter 2), we start with a systematic literature review to summarise existing evidence concerning the main

---

1 We number our research questions according to the chapter number of this thesis, thereby our research question starting from 2.
applications of mutation testing and identify limitations and gaps in current research. This is important because the existing surveys (e.g., [197, 241, 279]) only provide us with an overview of the most influential realisations of mutation testing in research, thereby omitting the perspective of how mutation testing is applied and what limitations are encountered in research. To achieve our goal, we first would like to identify and classify the main quality assurance processes where mutation testing is applied. This leads to RQ2.1:

**RQ2.1 How is mutation testing used in quality assurance processes?**

During the synthesis of the empirical evidence related to mutation testing, we also became interested in how the related empirical studies are reported, so that we can provide guidelines for applying and reporting on mutation testing and recommendations for future work. RQ2.2 addresses exactly this concern:

**RQ2.2 How are empirical studies related to mutation testing designed and reported?**

Based on a collection of 191 papers published between 1981 and 2015, our systematic literature review presents a detailed analysis of the application perspective of mutation testing, where we only selected papers that use mutation testing as a tool for evaluating or improving other quality assurance processes rather than focusing on the development of mutation tools, operators or challenges and open issues for mutation testing. Among the results, three further points attract our attention:

1. The high computational cost issue of mutation testing is not well-solved in the context of our research body.

2. A deeper understanding of mutation testing is required, such as what particular kinds of faults mutation testing is good at finding and what makes it hard to do mutation testing.

3. Most studies use mutation testing as an assessment tool targeting unit tests; as such, we feel that the application domain is quite limited.

The first item points us to the issue of the high computational cost when applying mutation testing. We investigate *whether we can use compression techniques to speed up mutation testing* (RQ3 in Chapter 3). More specifically, we devise six compression techniques based on two clustering algorithms and three mutant selection strategies. The clustering algorithms we adopt to cluster mutants are *overlapped grouping* and *Formal Concept Analysis (FCA)*. The *overlapped* method is the simplest and strictest clustering method, i.e., elements are only grouped together if they are identical. Formal Concept Analysis (FCA) was originally a data analysis method and has shown to be a powerful mathematical technique to convey and summarise large amounts of information [364].

---

2The quality assurance processes include testing activities [71] and debugging [74] in general. In more specific, the quality assurance processes include all the daily work responsibilities of test engineers (e.g. designing test inputs, producing test case values, running test scripts, analysing results, and reporting results to developers and managers) [37].
INTRODUCTION

FCA produces the concept lattice or concept hierarchy from a collection of objects and their properties. In the mutation testing context, our FCA-based compression technique only considers the maximal concepts that are directly connected to the exit point in the lattice hierarchy, the so-called maximal groupings.

To select mutants for execution, we leverage the knowledge of mutation locations and mutation operator types. To steer our investigation, we propose the following three research questions:

**RQ3.1** How accurate are different compression techniques?
**RQ3.2** How do compression techniques perform in terms of speed-up?
**RQ3.3** What is the trade-off between accuracy and speed-up for the compression techniques?

The second point from our literature review addresses the necessity to deepen the understanding of mutation testing. The current research considers the mutation score mostly related the test suite quality and mutant usefulness [201, 219, 295, 373]. However, how can production code quality in terms of testability and observability influence the mutation score? (RQ4 in Chapter 4) has rarely been explored. To answer this question, we investigate the relationship between testability and observability metrics and mutation testing. More specifically, we conjecture that software testability [89, 191] and code observability [80, 328] are two key factors. The following three research questions steer our investigation into the relationship between testability, observability and the mutation score:

**RQ4.1** What is the relation between testability metrics and the mutation score?
**RQ4.2** What is the relation between observability metrics and the mutation score?
**RQ4.3** What is the relation between the combination of testability and observability metrics and the mutation score?

After investigating the relationship between testability, observability and the mutation score, we still lack insight into how these relationships can be made actionable for software engineers in practice. That is why, based on the observations from RQ4.1-RQ4.3, we define anti-patterns or indicators that software engineers can apply to their code to ensure that mutants can be killed. This leads us to RQ4.4:

**RQ4.4** To what extent does the refactoring of anti-patterns based on testability and observability help in improving the mutation score?

The third message from our literature review indicates that the application domain of mutation testing is limited; this inspires us to explore more diverse applications for mutation testing: the one is mutation testing for physical computing, and the other is applying mutation testing to GPU programs.

For the first new application domain we have explored physical computing which builds interactive systems between the physical world and computers [282]. Physical computing, has been widely used in a wide variety of domains and applications, e.g., the
Internet of Things (IoT), wherein sensors and actuators blend seamlessly with the environment around us, and the information is shared across platforms [166]. Examples of physical computing applications (or cyber-physical systems) include medical devices and systems, aerospace systems, transportation vehicles and intelligent highways, defense systems, robotic systems, process control, factory automation, building and environmental control and smart spaces [302]. Compared to conventional software projects, the costs associated with failing physical computing systems are often even bigger, as bugs can result in real-life accidents [186]. For example, a robotic arm might accidentally hurt the human if the programmer does not set up the initial state properly. Therefore, to develop a rigorous and sound physical computing system, a high-quality test suite becomes crucial. This brings us to mutation testing, which has been shown to perform well in exposing faults [144, 228, 244].

To investigate whether physical computing can benefit from mutation testing (RQ5 in Chapter 5), we propose a novel mutation testing approach for physical computing systems. Specifically, we define a set of mutation operators based on common mistakes that we have observed when developing physical computing systems. To assess the efficacy of our mutation testing approach, we implement a mutation testing tool for physical computing systems (coined MUTPHY) to answer the following questions:

**RQ5.1** How effective is MUTPHY in evaluating the existing test suite?  
**RQ5.2** How efficient is MUTPHY in generating non-equivalent mutants?  
**RQ5.3** Is it possible to kill all non-equivalent surviving mutants by adding extra test cases?

**GPU computing**, the other application domain we have targeted, aims to use a GPU as a co-processor to accelerate CPUs for general-purpose scientific and engineering computing [283]. Compared to the CPU, the GPU contains many more transistors devoted to data processing rather than data caching and flow control [267]. Thus, the GPU is especially well-suited for compute-intensive, highly parallel computation.

Thanks to rapid advances in programmability and performance, we have observed that GPUs have been widely applied in High-Performance Computing (HPC) [134, 336], as well as safety-critical domains (e.g., medical science [332]). This attracts increasing attention in terms of quality assurance for GPU applications [158, 303]. Again, we come up with mutation testing, to investigate if mutation testing can help in GPU program testing (RQ6 in Chapter 6). To enable mutation testing for GPU applications, we develop a mutation testing tool named MUTGPU. We steer our investigation along the four research questions:

**RQ6.1** How frequently can GPU-specific mutation operators be applied?  
**RQ6.2** How effective are conventional mutation operators in evaluating the test suite of GPU programs?  
**RQ6.3** How effective are GPU-specific mutation operators in evaluating the test suite of GPU programs?  
**RQ6.4** How do GPU-specific mutation operators compare with conventional mutation operators in terms of the improvement?
To sum up, we present an overview of our research questions in Figure 1.2. As shown in Figure 1.2, we start with RQ2 which seeks to find out how mutation testing is actually applied. We answer RQ2 by conducting a systematic literature review, resulting in three interesting findings for further investigation. The first point “The issue of high computation cost is not well solved” leads us to RQ3. RQ4 is generated from the second finding which requires us to deepen the understanding of mutation testing. More specifically, we investigate the relationship between production code quality in terms of testability/observability and mutation testing. The last message indicating that the current application domain is limited inspires us to explore new applications for mutation testing RQ5 and RQ6.

1.3. RESEARCH METHODOLOGY

The main goal of this thesis is to explore ways to improve and extend the applicability of mutation testing. Therefore, our first step is to synthesise existing studies to gain insights into the state-of-the-art research regarding the application perspective of mutation testing. As systematic literature reviews [212] have been shown to be good tools to summarise existing evidence concerning a technology and identify gaps in current research [222], we follow this approach for reaching our objectives of RQ2.

The results from our systematic literature inspire and lead us to three directions of
research: (1) speeding up mutation testing via compression techniques (RQ3); (2) deepening understanding of mutation testing by investigation of the relationship between testability, observability and the mutation score (RQ4); and (3) exploring new application domains of mutation testing (RQ5 and RQ6). To answer RQ3 to RQ6, we conduct a series of empirical studies by employing a combination of quantitative and qualitative approaches. Because quantitative strategies such as experimental studies are appropriate when testing the effect of some manipulation or activity, while a qualitative study of beliefs and understandings are appropriate to find out why the results from a quantitative investigation as they are [105]. We adopt different empirical methods to evaluate our proposed approaches or hypotheses, e.g., experiment (e.g., Chapter 3) and case study (e.g., Chapter 4).

In the following section, we would like to present an overview of the research methodology to show that we use different research methods in this thesis. For each research question, we are going to describe our research methods in more detail.

Chapter 2 For RQ2, we perform a systematic literature review [212] to investigate how mutation testing is actually applied. Unlike the general literature review, the systematic literature review aims to eliminate bias and incompleteness through a systematic mechanism [222]. We follow Kitchenham [212]’s guidelines for applying the systematic literature review specifically in the field of software engineering. To answer RQ2.1 and RQ2.2, we generate an attribute framework to characterise each paper. The attribute framework consists of seven facets of interest that are highly relevant to the information we need to answer the questions. In this way, we can also show quantitative results for each attribute to support our answers.

Chapter 3 The goal of RQ3 is to verify whether we can use compression techniques to speed up mutation testing. To achieve that, we conduct an experimental study with 20 open-source Java projects and using the test suites manually written by the original developers. To answer RQ3.1 to RQ3.3, we evaluate six compression techniques together with two baselines: mutation sampling and weak mutation. This study mainly adopts quantitative research approaches by comparing the performance of different techniques in terms of accuracy and speed-up. In addition to a set of quantitative evaluation metrics, such as the absolute error and the overhead, we also adopt Friedman’s test [304] with $\alpha = 0.05$ to assess whether the differences among the eight strategies are statistically significant or not. Also, in case we observe exceptions to the major findings, we also conduct a qualitative analysis to understand why.

Chapter 4 To answer RQ4.1 to RQ4.3, we aim to investigate the relationship between testability/observability metrics and mutation testing. Thereby, we conduct an experimental study using six systems publicly available on GitHub. In this experiment, we first adopt Spearman’s rank-order correlation to statistically measure the correlation between each metric (both existing code metrics and our newly proposed mutant observability metrics) and the mutation score of the corresponding methods or classes. Moreover, except for the pair-wise correlations between each metric and the mutation score, we are also interested in how those metrics interact with each other. To do so, we adopt
Random Forest to predict the mutation score based on those metrics. For RQ4.4, we perform a case study involving 16 code fragments to investigate whether the refactoring of anti-patterns improves the mutation score.

Chapter 5 To investigate RQ5, we first need a prototype tool to enable mutation testing for physical computing systems. So, we develop a mutation testing tool coined MUTPHY working on Raspberry Pi and Arduino platforms. To assess the efficacy of our mutation testing approach, we conducted an experimental study. To answer RQ5.1 and RQ5.2, we compare the mutation score and the number of equivalent mutants quantitively. As for RQ5.3, we analyse the non-equivalent surviving mutants in detail and try to engineer new test cases to kill these mutants manually.

Chapter 6 Similar to RQ5, the first step to answer RQ6 is to implement a tool to apply mutation testing in GPU programs, and then we conduct an experimental study using our self-implemented tool named MUTGPU. To answer RQ6.1, we evaluate the frequency of each mutation operator based on the number of generated mutants and the mutation score. For RQ6.2 and RQ6.3, we determine the effectiveness of the mutation operators in assessing test quality of GPU programs based on non-equivalent surviving mutants, where we use both quantitative (by comparing the mutation scores) and qualitative (by manually analysing non-equivalent mutants) methods. To compare the conventional mutation operators with GPU-specific ones (RQ6.4), we first engineer new test cases to obtain a C-sufficient test suite for each system. Then, we manually analyse the remaining GPU mutants that cannot be detected by the C-sufficient test suites.

1.4. Contributions and Thesis Outline

In this section, we are going to summarise the contributions of this thesis, and then present the outline of the thesis.

An in-depth literature survey on the application perspective of mutation testing (Chapter 2). We conduct a systematic literature review of 191 studies that apply mutation testing in scientific experiments, clearly contrasting previous literature reviews that surveyed the main development of mutation testing, and that did not specifically go into how mutation testing is applied (e.g., [197, 241, 279]).

A detailed attribute framework that generalises and details the essential elements related to the actual use of mutation testing (Chapter 2). Through a detailed reading of this research body, we derive an attribute framework that is consequently used to characterise the studies in a structured manner. The resulting attribute framework can be used as a reference for researchers when describing how they apply mutation testing.

A series of recommendations for future work including valuable suggestions on how to report mutation testing in testing experiments in an appropriate manner (Chapter 2). Based on the results of the literature review, we provide (1) guidelines on how to apply and subsequently report on mutation testing in testing experiments and (2) recommendations for future work.

A detailed investigation of different compression techniques to speed up mutation testing (Chapter 3). We propose six mutation compression strategies by leveraging mu-
tant clustering algorithms and weak mutation. To evaluate the efficacy of our methods, we conduct a study on 20 open source projects. The overall results indicate that mutation compression techniques are a better choice than random sampling and weak mutation in practice: they can effectively speed up strong mutation 6.3 to 94.3 times with an accuracy of >90%.

**A detailed investigation of the relationship between testability and observability metrics and the mutation score (Chapter 4).** We collect 64 existing source code quality metrics for testability, and propose a set of metrics that specifically target mutant observability. Then, we use statistical analysis on open-source Java projects to investigate the relationship between testability, observability, and the mutation score. Last, we perform a case study involving 16 code fragments to investigate whether the refactoring of anti-patterns based on the aforementioned metrics can improve the mutation score.

**A generic mutation testing approach for physical computing systems (Chapter 5).** We propose a novel mutation testing approach for physical computing systems. Specifically, we define a set of mutation operators based on common mistakes that we observe when developing physical computing systems. Also, we implement a mutation testing tool coined MUTPHY for physical computing systems. We present an initial evaluation of our approach on the Raspberry Pi and Arduino platforms, which shows promising results.

**A generic mutation testing approach for GPU programs (Chapter 6).** First, we design nine new GPU-specific mutation operators in addition to conventional mutation operators. We develop a mutation testing tool named MUTGPU especially for GPU applications in the CUDA programming model. We perform an empirical study involving six GPU projects.

The remainder of the thesis is organised as follows: Chapter 2 presents a systematic literature review on the application of mutation testing. Chapter 3 investigates six mutation compression techniques to speed up mutation testing. Chapter 4 describes a detailed investigation of the relationship between testability and observability metrics and the mutation score. Chapter 5 introduces a novel mutation testing approach for physical computing systems, while Chapter 6 provides a study on applying mutation testing in GPU programming. Chapter 7 concludes the thesis.
A SYSTEMATIC LITERATURE REVIEW OF HOW MUTATION TESTING SUPPORTS QUALITY ASSURANCE PROCESSES

Mutation testing has been very actively investigated by researchers since the 1970s and remarkable advances have been achieved in its concepts, theory, technology and empirical evidence. While the most influential realisations have been summarised by existing literature reviews, we lack insight into how mutation testing is actually applied. Our goal is to identify and classify the main applications of mutation testing and analyse the level of replicability of empirical studies related to mutation testing. To this aim, this chapter provides a systematic literature review on the application perspective of mutation testing based on a collection of 191 papers published between 1981 and 2015. In particular, we analysed in which quality assurance processes mutation testing is used, which mutation tools and which mutation operators are employed. Additionally, we also investigated how the inherent core problems of mutation testing, i.e., the equivalent mutant problem and the high computational cost, are addressed during the actual usage. The results show that most studies use mutation testing as an assessment tool targeting unit tests, and many of the supporting techniques for making mutation testing applicable in practice are still underdeveloped. Based on our observations, we made nine recommendations for future work, including an important suggestion on how to report mutation testing in testing experiments in an appropriate manner.

This chapter has been published in Software Testing Verification Reliability (STVR) [393].
2.1. INTRODUCTION

Mutation testing is defined by Jia and Harman [197] as a fault-based testing technique which provides a testing criterion called the mutation adequacy score. This score can be used to measure the effectiveness of a test set in terms of its ability to detect faults [197]. The principle of mutation testing is to introduce syntactic changes into the original program to generate faulty versions (called mutants) according to well-defined rules (mutation operators) [279]. Mutation testing originated in the 1970s with works from Lipton [230], DeMillo et al. [117] and Hamlet [168] and has been a very active research field over the last few decades. The activeness of the field is in part evidenced by the extensive survey of more than 390 papers on mutation testing that Jia and Harman published in 2011 [197]. Jia and Harman’s survey highlights the research achievements that have been made over the years, including the development of tools for a variety of languages and empirical studies performed [197]. Additionally, they highlight some of the actual and inherent problems of mutation testing, amongst others: (1) the high computational cost caused by generating and executing the numerous mutants and (2) the tremendous time-consuming human investigation required by the test oracle problem and equivalent mutant detection.

While existing surveys (e.g., [197, 241, 279]) provide us with a great overview of the most influential realisations in research, we lack insight into how mutation testing is actually applied. Specifically, we are interested in analysing in which quality assurance processes mutation testing is used, which mutation tools are employed and which mutation operators are used. Additionally, we want to investigate how the aforementioned problems of the high computational cost and the considerable human effort required are dealt with when applying mutation testing. In order to steer our research, we aim to fulfil the following objectives:

- to identify and classify the applications of mutation testing in quality assurance processes;
- to analyse how the main problems are coped with when applying mutation testing;
- to provide guidelines for applying mutation testing in testing experiments;
- to identify gaps in current research and to provide recommendations for future work.

As systematic literature reviews have been shown to be good tools to summarise existing evidence concerning a technology and identify gaps in current research [212], we follow this approach for reaching our objectives. We only consider the articles which provide sufficient details on how mutation testing is used in their studies, i.e., we require at least a brief specification about the adopted mutation tool, mutation operators or mutation score. Moreover, we selected only papers that use mutation testing as a tool for evaluating or improving other quality assurance processes rather than focusing on the development of mutation tools, operators or challenges and open issues for mutation testing. This resulted in a collection containing 191 papers published from 1981 to 2015. We analysed this collection in order to answer the following two research questions:

**RQ2.1:** How is mutation testing used in quality assurance processes?
This research question aims to identify and classify the main software testing tasks where mutation testing is applied. In particular, we are interested in the following key aspects: (1) in which circumstances mutation testing is used (e.g., assessment tool), (2) which quality assurance processes are involved (e.g., test data generation, test case prioritisation), (3) which test level it targets (e.g., unit level) and (4) which testing strategies it supports (e.g., structural testing). The above four detailed aspects are defined to characterise the essential features related to the usage of mutation testing and the quality assurance processes involved. With these elements in place, we can provide an in-depth analysis of the applications of mutation testing.

RQ2.2: How are empirical studies related to mutation testing designed and reported?

The objective of this question is to synthesise empirical evidence related to mutation testing. The case studies or experiments play an inevitable role in a research study. The design and demonstration of the evaluation methods should ensure the replicability. For replicability, we mean that the subject, the basic methodology, as well as the result, should be clearly pointed out in the article. In particular, we are interested in how the articles report the following information related to mutation testing: (1) mutation tools, (2) mutation operators, (3) mutant equivalence problem, (4) techniques for reduction of computational cost and (5) subject programs used in the case studies. After gathering this information, we can draw conclusions from the distribution of related techniques adopted under the above five facets and thereby provide guidelines for applying mutation testing and reporting the used setting/tools.

The remainder of this review is organised as follows: Section 2.2 provides an overview on background notions on mutation testing. Section 2.3 details the main procedures we followed to conduct the systematic literature review and describes our inclusion and exclusion criteria. Section 2.4 presents the discussion of our findings, particularly Section 2.4.3 summarises the answers to the research questions, while Section 2.4.4 provides recommendations for future research. Section 2.5 discusses the threats to validity, and Section 2.6 concludes the chapter.

2.2. BACKGROUND

In order to level the playing field, we first provide the basic concepts related to mutation testing, i.e., its fundamental hypothesis and generic process, including the Competent Programmer Hypothesis, the Coupling Effect, mutation operators and the mutation score. Subsequently, we discuss the benefits and limitations of mutation testing. After that, we present a historical overview of mutation testing where we mainly address the studies that concern the application of mutation testing.

2.2.1. BASIC CONCEPTS

Fundamental Hypothesis

Mutation testing starts with the assumption of the Competent Programmer Hypothesis (introduced by DeMillo et al. [117] in 1978): “The competent programmers create programs that are close to being correct.” This hypothesis implies that the potential faults in the programs delivered by the competent programmers are just very simple mistakes; these defects can be corrected by a few simple syntactical changes. Inspired by the above
hypothesis, mutation testing typically applies small syntactical changes to original programs, thus implying that the faults that are seeded resemble faults made by “competent programmers”.

At first glance, it seems that the programs with complex errors cannot be explicitly generated by mutation testing. However, the Coupling Effect, which was coined by De-Millo et al. \[117\] states that “Test data that distinguishes all programs differing from a correct one by only simple errors is so sensitive that it also implicitly distinguishes more complex errors”. This means complex faults are coupled to simple faults. This hypothesis was later supported by Offutt \[268, 269\] through empirical investigations over the domain of mutation testing. In his experiments, he used first-order mutants, which are created by applying the mutation operator to the original program once, to represent simple faults. Conversely, higher-order mutants, which are created by applying mutation operators to the original program more than once, stand for complex faults. The results showed that the test data generated for first-order mutants killed a higher percentage of mutants when applied to higher-order mutants, thus yielding positive empirical evidence about the Coupling Effect. Besides, there has been a considerable effort in validating the coupling effect hypothesis, amongst others the theoretical studies of Wah \[358–360\] and Kapoor \[208\].

THE GENERIC MUTATION TESTING PROCESS.

After introducing the fundamental hypotheses of mutation testing, we are going to give a detailed description of the generic process of mutation testing:

Given a program \(P\) and a test suite \(T\), a mutation engine makes syntactic changes to the program \(P\): the rule that specifies syntactic variations are defined as a mutation operator, and the result of one application of a mutation operator is a set of mutants \(M\). After that, each mutant \(P_m \in M\) is executed against \(T\) to verify whether test cases in \(T\) fail or not.

Here is an example of a mutation operator, i.e., Arithmetic Operator Replacement (AOR), on a statement \(X=a+b\). The produced mutants include \(X=a-b\), \(X=a\times b\), and \(X=a\div b\).

The execution results of \(T\) on \(P_m \in M\) are compared with \(P\): (1) if the output of \(P_m\) is different from \(P\), then \(P_m\) is killed by \(T\); (2) otherwise, i.e., the output of \(P_m\) is the same as \(P\), this leads to either (2.1) \(P_m\) is equivalent to \(P\), which means that they are syntactically different but functionally equivalent; or (2.2) \(T\) is not adequate to detect the mutants, which requires test case augmentation.

The result of mutation testing can be summarised using the mutation score (also referred to as mutation coverage or mutation adequacy), which is defined as:

\[
\text{mutation score} = \frac{\# \text{killed mutants}}{\# \text{nonequivalent mutants}} \tag{2.1}
\]

From the equation above, we can see that the detection of equivalent mutants is done before calculating the mutation score, as the denominator explicitly mentions non-equivalent mutants. Budd and Angluin \[91\] have theoretically proven that the equivalence of two programs is not decidable. Meanwhile, in their systematic literature survey, Madeyski
et al. [241] have also indicated that the equivalent mutant problem takes an enormous amount of time in practice.

A mutation testing system can be regarded as a language system [47] since the programs under test must be parsed, modified and executed. The main components of mutation testing consist of the mutant creation engine, the equivalent mutant detector, and the test execution runner. The first prototype of a mutation testing system for Fortran was proposed by Budd and Sayward [90] in 1977. Since then, numerous mutation tools have been developed for different languages, such as Mothra [210] for Fortran, Proteum [113] for C, Mujava [240] for Java, and SQLMutation [342] for SQL.

**Benefits & Limitations**

Mutation testing is widely considered as a “high end” test criterion [47]. This is in part due to the fact that mutation testing is extremely hard to satisfy because of the massive number of mutants. However, many empirical studies found that it is much stronger than other test adequacy criteria in terms of fault exposing capability, e.g., Mathur and Wong [244], Frankl et al. [144] and Li et al. [228]. In addition to comparing mutation testing with other test criteria, there have also been empirical studies comparing real faults and mutants. The most well-known research work on such a topic is by Andrews et al. [50]: they suggest that when using carefully selected mutation operators and after removing equivalent mutants, mutants can provide a good indication of the fault detection ability of a test suite. As a result, we consider the benefits of mutation testing to be:

- better fault exposing capability compared to other test coverage criteria, e.g., all-use;
- a good alternative to real faults which can provide a good indication of the fault detection ability of a test suite.

The limitations of mutation testing are inherent. Firstly, both the generation and execution of a vast number of mutants are computationally expensive. Secondly, the equivalent mutant detection is also an inevitable stage of mutation testing which is a prominent undecidable problem, thereby requiring human effort to investigate. Thus, we consider the major limitations of mutation testing to be:

- the high computational cost caused by the large number of mutants;
- the undecidable Equivalent Mutant Problem resulting in the difficulty of fully automating the equivalent mutant analysis.

To deal with the two limitations above, a lot of research effort has been devoted to reduce the computational cost and to propose heuristics to detect equivalent mutants. As for the high computational cost, Offutt and Untch [277] performed a literature review in which they summarised the approaches to reduce computational cost into three strategies: do fewer, do smarter and do faster. These three types were later classified into two classes by Jia and Harman [197]: reduction of the generated mutants and reduction of the execution cost. Mutant sampling (e.g., [41, 367]), mutant clustering (e.g., [188, 195])
and selective mutation (e.g., [258, 271, 322]) are the most well-known techniques for reducing the number of mutants while maintaining efficacy of mutation testing to an acceptable degree. For reduction of the execution expense, researchers have paid much attention to weak mutation (e.g., [116, 185, 272]) and mutant schemata (e.g., [344, 345]).

To overcome the Equivalent Mutant Problem, there are mainly three categories classified by Madeyski et al. [241]: (1) detecting equivalent mutants, such as Baldwin and Sayward [63] (using compiler optimisations), Hierons et al. [177] (using program slicing), Martin and Xie [242] (through change-impact analysis), Ellims et al. [132] (using running profile), and du Bousquet and Delaunay [129] (using model checker); (2) avoiding equivalent mutant generation, such as Mresa and Bottaci [258] (through selective mutation), Harman et al. [174] (using program dependence analysis), and Adamopoulos et al. [42] (using co-evolutionary search algorithm); (3) suggesting equivalent mutants, such as bayesian learning [350], dynamic invariants analysis [312], and coverage change examination (e.g. [314]).

2.2.2. Historical Overview

In this subsection, we are going to present a chronological overview of important research in the area of mutation testing. As the focus of our review is the application perspective of mutation testing, we mainly address the studies that concern the application of mutation testing. In the following paragraphs, we will first give a brief summary of the development of mutation testing, and — due to the sheer size of the research body — we will then highlight some notable studies on applying mutation testing.

Mutation testing was initially introduced as a fault-based testing method which was regarded as significantly better at detecting errors than the covering measure approach [92]. Since then, mutation testing has been actively investigated and studied thereby resulting in remarkable advances in its concepts, theory, technology and empirical evidence. The main interests in the area of mutation testing include (1) defining mutation operators [43], (2) developing mutation testing systems [185, 210, 240], (3) reducing the cost of mutation testing [271, 345], (4) overcoming the equivalent mutant detection problem [241], and (5) empirical studies with mutation testing [50]. For more literature on mutation testing, we refer to the existing surveys of DeMillo [115], Offutt and Untch [277], Jia and Harman [197] and Offutt [279].

In the meanwhile, mutation testing has also been applied to support other testing activities, such as test data generation and test strategy evaluation. The early application of mutation testing can be traced back to the 1980s [130, 264–266]). Ntafos is one of the very first researchers to use mutation testing as a measure of test set effectiveness. Ntafos applied mutation operators (e.g., constant replacement) to the source code of 14 Fortran programs [265]. The generated test suites were based on three test strategies, i.e., random testing, branch testing and data-flow testing, and were evaluated regarding mutation score.

DeMillo and Offutt [116] are the first to automate test data generation guided by fault-based testing criteria. Their method is called Constraint-based testing (CBT). They transformed the conditions under which mutants will be killed (necessity and sufficiency condition) to the corresponding algebraic constraints (using constraint template table). The test data was then automatically generated by solving the constraint satisfaction
problem using heuristics. Their proposed constraint-based test data generator is limited and was only validated on five laboratory-level Fortran programs. Other remarkable approaches of the automatic test data generation includes a paper by Zhang et al. [382], who adopted Dynamic Symbolic Execution, and a framework by Papadakis and Malevris [293] in which three techniques, i.e., Symbolic Execution, Concolic Testing and Search-based Testing, were used to support the automatic test data generation.

Apart from test data generation, mutation testing is widely adopted to assess the cost-effectiveness of different test strategies. The work above by Ntafos [265] is one of the early studies on applying mutation testing. Recently, there has been a considerable effort in the empirical investigation of structural coverage and fault-finding effectiveness, including Namin and Andrews [262] and Inozemtseva et al. [189]. Zhang and Mesbah [384] proposed assertion coverage, while Whalen et al. [362] presented observable modified condition/decision coverage (OMC/DC); these novel test criteria were also evaluated via mutation testing.

Test case prioritisation is one of the practical approaches to reducing the cost of regression testing by rescheduling test cases to expose the faults as earlier as possible. Mutation testing has also been applied to support test case prioritisation. Among these studies, two influential papers are Rothermel et al. [307] and Elbaum et al. [131] who proposed a new test case prioritisation method based on the rate of mutants killing. Moreover, Do and Rothermel [127, 128] measured the effectiveness of different test case prioritisation strategies via mutation faults since Andrews et al.’s empirical study suggested that mutation faults can be representative of real faults [50].

The test-suite reduction is another testing activity we identified which is supported by mutation testing. The research work of Offutt et al. [275] is the first to target test-suite reduction strategies, especially for mutation testing. They proposed Ping-Pong reduction heuristics to select test cases based on their mutation scores. Another notable work is Zhang et al. [381] that investigated test-suite reduction techniques on Java programs with real-world JUnit test suites via mutation testing.

Another portion of the application of mutation testing is debugging, such as fault localisation. Influential examples include an article by Zhang et al. [361] in which mutation testing is adopted to investigate the effect of coincidental correctness in the context of a coverage-based fault localisation technique, and a novel fault localisation method by Papadakis et al. [290], [291] who used mutants to identify the faulty program statements.

2.2.3. Comparisons with existing literature surveys
In this section, we summarise the existing literature surveys on mutation testing and compare these surveys to our literature review. Table 2.1 lists seven literature surveys which we have found so far, including the years which the survey covered, whether the survey is a systematic literature review and the survey’s main idea.

First of all, the scope of our literature review is different from the existing literature surveys. The surveys of DeMillo [115], Woodward [368], Offutt and Untch [277], Offutt [279] and Jia and Harman [197] focused on the development of mutation testing, where they summarised and highlighted the most influential realisations and findings on mutation testing. In the insightful works of Offutt and Untch [277], Offutt [279] and Jia and Harman [197], they only mentioned some of the most crucial studies which
applied mutation testing to support quality assurance processes, thus, the relevant research questions posed by us could not be answered by their reviews. Madeyski et al. [241] reviewed the equivalent mutant problem which is a subarea of mutation testing. Compared to their survey work, we are more interested in how approaches for detecting equivalent mutant are actually used in a research context. Hanh et al. [170] analysed the literature on mutation-based test data generation, which is a subset of our literature review. Our literature review not only covers the test data generation but also other quality assurance processes, e.g., test case prioritisation and debugging.

Moreover, our literature review follows the systematic literature review (SLR) methodology [85] which is not the case for six other literature reviews (Madeyski et al. [241] being the exception): we aim to review the existing articles in a more systematic way and provide a more complete list of the existing works on how mutation testing is actually applied in quality assurance processes. It is important to mention, though, that taking a subset of Offutt and Untch [277], Offutt [279] and Jia and Harman [197]’s results regarding quality assurance applications will not give as complete a view on quality assurance applications as our SLR actually does.

### 2.3. Research Method

In this section, we describe the main procedures we took to conduct this review. We adopted the methodology of the systematic literature review. A systematic literature review [212] is a means of aggregating and evaluating all the related primary studies under a research scope in an unbiased, thorough and trustworthy way. Unlike the general literature review, the systematic literature review aims to eliminate bias and incompleteness through a systematic mechanism [222]. Kitchenham [212] presented comprehensive and reliable guidelines for applying the systematic literature review to the field of software engineering. The guidelines cover three main phases: (i) planning the review, (ii) conducting the review, and (iii) reporting the review. Each step is well-defined and well-structured. By following these guidelines, we can reduce the likelihood of gener-
The principle of the systematic literature review [85] is to convert the information collection into a systematic research study; this research study first defines several specific research questions and then searches for the best answers accordingly. These research questions and search mechanisms (consisting of study selection criteria and data extraction strategy) are included in a review protocol, a detailed plan to perform the systematic review. After developing the review protocol, the researchers need to validate this protocol for further resolving the potential ambiguity.

Following the main stages of the systematic review, we will introduce our review procedure in four parts: we will first specify the research questions, and then present the study selection strategy and data extraction framework. In the fourth step, we will show the validation results of the review protocol. The overview of our systematic review process is shown in Figure 2.1.

### 2.3.1. Research Questions

The research questions are the most critical part of the review protocol. The research questions determine study selection strategy and data extraction strategy. In this review, our objective is to examine the primary applications of mutation testing and identify limitations and gaps. Therefore, we can provide guidelines for applying mutation testing and recommendations for future work. To achieve these goals and starting with our most vital interests, the application perspective of mutation testing, we naturally further divide it into two aspects: (1) how mutation testing is used and (2) how the related empirical studies are reported. For the first aspect, we aim to identify and classify the main applications of mutation testing:
RQ2.2.1: How is mutation testing used in quality assurance processes?  

To understand how mutation testing is used, we should first determine in which circumstances it is used. The usages might range from using mutation testing as a way to assess how other testing approaches perform or mutation testing might be a building block of an approach altogether. This leads to RQ2.1.1:

RQ2.1.1: Which role does mutation testing play in quality assurance processes?

There is a broad range of quality assurance processes that can benefit from the application of mutation testing, e.g., fault localisation and test data generation. RQ1.2 seeks to uncover these activities.

RQ2.1.2: Which quality assurance process does mutation testing support?

In Jia and Harman's survey [197] of mutation testing, they found that most approaches work at the unit testing level. In RQ2.1.3 we investigate whether the application of mutation testing is also mostly done at the unit testing level, or whether other levels of testing have been also investigated in the literature.

RQ2.1.3: Which test level does mutation testing target?

Jia and Harman [197] have also indicated that mutation testing is most often used in a white-box testing context. In RQ2.1.4 we explore what other testing strategies can also benefit from the application of mutation testing.

RQ2.1.4: Which testing strategies does mutation testing support?

For the second aspect, we are going to synthesise empirical evidence related to mutation testing:

RQ2.2: How are empirical studies related to mutation testing designed and reported?

A plethora of mutation testing tools exist and have been surveyed by Jia and Harman [197]. Little is known which ones are most applied and why these are more popular. RQ2.2.1 tries to fill this knowledge gap by providing insight into which tools are used more frequently in a particular context.

RQ2.2.1: Which mutation testing tools are being used?

The mutation tools that we surveyed implement different mutation operators. Also, the various mutation approaches give different names to virtually the same mutation operators. RQ2.2.2 explores what mutation operators each method or tool has to offer and how mutation operators can be compared.

1The quality assurance processes include testing activities and debugging in general. In more specific, the quality assurance processes include all the daily work responsibilities of test engineers (e.g., designing test inputs, producing test case values, running test scripts, analyzing results, and reporting results to developers and managers) [47].
**RQ2.2.2: Which mutation operators are being used?**

The equivalent mutant problem, i.e., the situation where a mutant leads to a change that is not observable in behaviour, is one of the most significant open issues in mutation testing. Both Jia and Harman [197] and Madeyski et al.[241] highlighted some of the most remarkable achievements in the area, but we have a lack of knowledge when it comes to how the equivalent mutant problem is coped with in practice when applying mutation testing during quality assurance activities. RQ2.2.3 aims to seek answers for exactly this question.

**RQ2.2.3: Which approaches are used to overcome the equivalent mutant problem when applying mutation testing?**

As mutation testing is computationally expensive, techniques to reduce costs are important. Selective Mutation and Weak Mutation are the most widely studied cost reduction techniques [197], but it is unclear which reduction techniques are actually used when applying mutation testing, which is the exact topic of RQ2.2.4.

**RQ2.2.4: Which techniques are used to reduce the computational cost when applying mutation testing?**

To better understand in which context mutation testing is applied, we want to look into the programming languages that have been used in the experiments. However, also the size of the case study systems is of interest, as it can be an indication of the maturity of certain tools. Finally, we are also explicitly looking at whether the case study systems are available for replication purposes (in addition to the check for availability of the mutation testing tool in RQ2.2.1).

**RQ2.2.5: What subjects are being used in the experiments (regarding programming language, size, and data availability)?**

### 2.3.2. Study Selection Strategy

**Initial Study Selection.** We started with search queries in online platforms, including Google Scholar, Scopus, ACM Portal, IEEE Explore as well as Springer, Wiley, Elsevier Online libraries, to collect papers containing the keywords “mutation testing” or “mutation analysis” in their titles, abstracts, and keywords. Meanwhile, to ensure the high quality of the selected papers, we considered the articles published in seven top journals and ten top conferences (as listed in Table 2.2) dating from 1971 as data sources. The above 17 venues are chosen because they report a high proportion of research on software testing, debugging, software quality and validation. Moreover, we excluded article summaries, interviews, reviews, workshops^2, panels and poster sessions from the search. If the paper’s language is not English, we also excluded such a paper. After this step, 220 papers were initially selected.

**Inclusion/Exclusion Criteria.** Since we are interested in how mutation testing is applied in a research context, thereby not excluding industrial practice, we need selection

---

^2In the snowballing procedure, we took the “Mutation Testing” workshop series into consideration, since this is the closest venue to mutation testing.
criteria to include the papers that use mutation testing as a tool for evaluating or improving other quality assurance processes and exclude the papers focusing on the development of mutation tools and operators, or challenges and open issues for mutation testing. Moreover, the selected articles should also provide sufficient evidence for answering the research questions. Therefore, we define two inclusion/exclusion criteria for study selection. The inclusion/exclusion criteria are as follows:

1. The article must focus on the supporting role of mutation testing in the quality assurance processes. This criterion excludes the research solely on mutation testing itself, such as defining mutation operators, developing mutation systems, investigating ways to solve open issues related to mutation testing and comparisons between mutation testing and other testing techniques.

2. The article exhibits sufficient evidence that mutation testing is used to support testing related activities. The sufficient evidence means that the article must clearly describe how the mutation testing is involved in the quality assurance processes. The author(s) must state at least one of the following details about the mutation testing process:

Table 2.2: Venues involved in study selection

<table>
<thead>
<tr>
<th>Type</th>
<th>Venue Name</th>
<th>No. of papers After Applying Search queries</th>
<th>No. of papers After Applying In./Ex. Criteria</th>
<th>No. of papers After Snowballing procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Journal</td>
<td>Journal of Empirical Software Engineering (EMSE)</td>
<td>4</td>
<td>3</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>Information and Software Technology (IST)</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Journal Software Maintenance and Evolution (JSME)</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Software Quality Journal (JSQ)</td>
<td>0</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>Journal of Systems and Software (ISS)</td>
<td>17</td>
<td>8</td>
<td>9</td>
</tr>
<tr>
<td></td>
<td>Journal on Software Testing, Verification and Reliability (STVR)</td>
<td>33</td>
<td>16</td>
<td>23</td>
</tr>
<tr>
<td></td>
<td>Transaction on Software Engineering and Methodology (TOSEM)</td>
<td>3</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>Transaction on Reliability (TR)</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Transaction on Software Engineering (TSE)</td>
<td>19</td>
<td>9</td>
<td>21</td>
</tr>
<tr>
<td>Conference</td>
<td>Proceedings Asia Pacific Software Engineering Conference (APSEC)</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>International Conference on Automated Software Engineering (ASE)</td>
<td>7</td>
<td>3</td>
<td>7</td>
</tr>
<tr>
<td></td>
<td>European Software Engineering Conference / International Symposium on the Foundations of Software Engineering (ESEC/FSE)</td>
<td>6</td>
<td>1</td>
<td>9</td>
</tr>
<tr>
<td></td>
<td>International Symposium on Empirical Software Engineering and Measurement (ESEM/ISESE)</td>
<td>2</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>International Conference on Software Engineering (ICSE)</td>
<td>29</td>
<td>9</td>
<td>22</td>
</tr>
<tr>
<td></td>
<td>International Conference on Software Maintenance and Evolution (ICSME/ICSM)</td>
<td>6</td>
<td>3</td>
<td>9</td>
</tr>
<tr>
<td></td>
<td>International Conference on Software Testing, Verification, Validation (ICST)</td>
<td>45</td>
<td>23</td>
<td>22</td>
</tr>
<tr>
<td></td>
<td>International Symposium on Software Reliability Engineering (ISRE)</td>
<td>26</td>
<td>10</td>
<td>20</td>
</tr>
<tr>
<td></td>
<td>International Symposium on Software Testing and Analysis (ISSTA)</td>
<td>14</td>
<td>3</td>
<td>12</td>
</tr>
<tr>
<td></td>
<td>Proceedings International Conference on Quality Software (QISIC)</td>
<td>8</td>
<td>5</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>Proceedings International Symposium on Search Based Software Engineering (ISBBSE)</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Proceedings of the International Conference on Testing Computer Software (TCS)</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Workshop</td>
<td>International Workshop on Mutation Analysis</td>
<td>0</td>
<td>0</td>
<td>9</td>
</tr>
<tr>
<td>Total</td>
<td></td>
<td>220</td>
<td>97</td>
<td>191</td>
</tr>
</tbody>
</table>

Note: the venues marked in bold font are not initially selected, but where added after the snowballing procedure. We listed the venues alphabetically according to their abbreviations, e.g., EMSE is ahead of IST.
testing in the article: mutation tool, mutation operators, mutation score\(^3\). This criterion also excludes theoretical studies on mutation testing.

The first author of this SLR then carefully read the titles and abstracts to check whether the papers in the initial collection belong to our set of selected papers based on the inclusion/exclusion criteria. If it is unclear from the titles and abstracts whether mutation testing was applied, the entire article especially the experiment part was read as well. After we have applied the inclusion/exclusion criteria, 97 papers remained.

**Snowballing Procedure.** After selecting 97 papers from digital databases and applying our selection criteria, there is still a high potential to miss articles of interest. As Brereton et al. [85] pointed out, most online platforms do not provide adequate support for systematic identification of relevant papers. To overcome this shortfall of online databases, we then adopted both backward and forward snowballing strategies [365] to find missing papers. Snowballing refers to using the list of references in a paper or the citations to the paper to identify additional papers [365]. Using the references and the citations respectively are referred to as backward and forward snowballing [365].

We used the 97 papers as the starter set and performed a backward and forward snowballing procedure recursively until no further papers could be added to our set. During the snowballing procedure, we extended the initially selected venues to minimise the chance of missing related papers. The snowballing process resulted in another 82 articles (and five additional venues). The International Workshop on Mutation Analysis was added during the snowballing procedure.

To check the completeness of the initial study collection, we first ran a reference check based on Jia et al.’s survey (among 264 papers) as our literature review was initially motivated from their paper. The results showed that: (1) 5 papers have already been included in our collection; (2) 3 additional papers that should be included; and (3) 246 papers are excluded. Again, we applied snowballing techniques to the additional three papers, and the three papers resulted in a total of 12 papers for our final collection (191 papers in total\(^4\)).

Furthermore, we ran a sanity check on our final collection to examine how many papers do not have the keywords “mutation analysis” or “mutation testing” in their abstracts, titles or keywords. The sanity check resulted in 112 papers; 15 papers are missing in the initial data collection by applying search queries in online platforms. Most of the missing papers (10 out of 15) (e.g., Offutt et al. [275] and Knauth et al. [213]) are not from the pre-considered 17 venues. The results of the sanity check indicate that there are potentials of missing papers based on search queries in online platforms; however, the snowballing procedure can minimise the risks of missing papers.

The detailed records of each step can be found in our GitHub repository [23].

### 2.3.3. Data Extraction Strategy

Data extracted from the papers are used to answer the research questions we formulated in Section 2.3.1. Based on our research questions, we draw seven facets of interest

\(^3\)The studies which merely adopted hand-seeded faults which are not based on a set of mutation operators are not part of this survey.

\(^4\)We did not control for double counting here as there are usually additional experiments and further discussion in the extended version.
that are highly relevant to the information we need to answer the questions. The seven facets are: (1) the roles of mutation testing in quality assurance processes; (2) the quality assurance processes; (3) the mutation tools used in experiments; (4) the mutation operators used in experiments; (5) the description of equivalent mutant problem; (6) the description of cost reduction techniques for mutation testing; (7) the subjects involved in experiments. An overview of these facets is given in Table 2.3.

For each facet, we first read the corresponding details in each paper and extracted the exact text from the papers. During the reading procedure, we started by identifying and classifying attributes of interest under each facet and assigned values to each attribute. The values of each attribute were generalised and modified during the reading process: we merged some values or divided one into several smaller groups. In this way, we generated an attribute framework, and then we used the framework to characterise each paper. Therefore, we can show quantitative results for each attribute to support our answers. Moreover, the attribute framework can also be further used for validation and replication of the review work. To categorise the attributes for each paper, all the abstracts, introductions, empirical studies and conclusions of the selected papers were carefully read. If these sections were not clear or were somehow confusing, we also took other sections from the paper into consideration. Furthermore, for categorising the test level attribute, to minimise misinterpretations of the original papers, we looked beyond the aforementioned sections to determine the test level (i.e., “unit”, “module”, “integration”, “system” and “acceptance” [47]). In particular, we used the former five words as keywords to search for the entire paper. If this search yielded no results, we did not necessarily categorise the paper as “n/a”. Instead, we read the entire paper, and if a study deals with a particular type of testing, e.g., testing of the grammar of a programming language or spreadsheet testing, we placed the paper in the category “others”. If the paper lacks any description of the test level, we classified the test level as “n/a”.

(1) roles of mutation testing in quality assurance processes:

The first facet concerns the role of mutation testing in quality assurance processes drawn from RQ2.1.1. We identified two classes for the function of mutation testing: assessment and guide. When mutation testing is used as a measure of test effectiveness concerning fault-finding capability, we classify this role as “assessment”. While for the “guide” role, mutation testing is adopted to improve the testing effectiveness as guidance, i.e., it is an inherent part of an approach.

To identify and classify the role of mutation testing, we mainly read the description of mutation testing in the experiment part of each paper. If we find the phrases which have the same meanings as “evaluate fault-finding ability” or “assess the testing effectiveness” in a paper, we then classify the paper into the class of “assessment”. In particular, when used as a measure of testing effectiveness, mutation testing is usually conducted at the end of the experiment; this means mutation testing is not involved in the generation or execution of test suites. Unlike the “assessment” role, if mutation testing is adopted to help to generate test suites or run test cases, we then classify the paper into the “guide” set. In this case, mutation testing is not used in the final step of the experiment.

(2) quality assurance processes:

The second facet focuses on quality assurance processes. Three attributes are relevant to quality assurance processes: the categories of quality assurance processes (RQ2.1.2),
test levels (RQ2.1.3) and testing strategies (RQ2.1.4). To identify the categories of quality assurance processes, we group similar quality assurance processes based on information in title and abstract. The quality assurance processes we identified so far consist of 12 classes: test data generation, test-suite reduction/selection, test strategy evaluation, test case minimisation, test case prioritisation, test oracle, fault localisation, program repairing, development scheme evaluation, model clone detection, model review, and fault tolerance. We classify the papers by reading the description appeared in title and abstract.

For test level, the values are based on the concept of test level and the authors’ specification. More precisely, we consider five test levels: unit, integration, system, others, and n/a. To characterise the test level, we search the exact words “unit”, “integration”, “system” in the article, as these four test levels are regular terms and cannot be replaced by other synonyms. If there is no relevant result after searching in a paper, we then classify the paper's test level into “n/a”, i.e., no specification regarding the test level. Also, for the paper which is difficult for us to categorise into any of the four phases (e.g., testing of the grammar of a programming language and spreadsheet testing) we mark this situation as “others”.

For testing strategies, a coarse-grained classification is adequate to gain an overview of the distribution of testing strategies. We identified five classes according to the test design techniques: structural testing, specification-based testing, similarity-based testing, hybrid testing and others [163, 346]. For the structural testing and specification-based testing classes, we further divided the classes into traditional and enhanced, based on whether other methods improve the regular testing.

To be classified into the “structural testing” class, the paper should either contain the keywords “structure-based”, “code coverage-based” or “white box”, or use structural test design techniques, such as statement testing, branch testing, and condition testing. For the “specification-based testing” class, the articles should either contain the keywords “black box”, “requirement-based” or “specification-based”, or use specification-based test design techniques, such as equivalence partitioning, boundary value analysis, decision tables and state transition testing. The similarity-based method aims to maximise the diversity of test cases to improve the test effectiveness; this technique is mainly based on test case relationship rather than software artefacts. Therefore, similarity-based testing does not belong to either structural testing or specification-based testing.

The grey-box testing combines structural testing and specification testing. Besides, several cases are using static analysis, code review or other techniques which cannot fit the above classes; in such situations, we mark the value as “others”.

Furthermore, to classify the “enhanced” version of structural and specification-based testing we rely on whether other testing methods were adopted to improve the traditional testing. For instance, Whalen et al. [362] combined the MC/DC coverage metric with a notion of observability to ensure the fault propagation conditions. Papadakis and Malevris [292] proposed an automatic mutation test case generation via dynamic symbolic execution. To distinguish such instances from the traditional structural and specification-based testing, we marked them as “enhanced”.

(3) mutation tools used in experiments:

For the mutation tools (derived from RQ2.2.1), we are interested in their types, but
also in their availability. Our emphasis on tool availability is instigated to address possible replication of the studies. The values of “Yes” or “No” for the tool availability depends on whether the mutation tool is open to the public. The tool type intends to provide further analysis of the mutation tool, which is based on whether the tool is self-developed and whether the tool itself is a complete mutation testing system. We identified five types of mutation tools: existing, partially-based, self-written, manual and n/a. The “existing” tool must be a complete mutation testing system, while “partially-based” means these tools are used as a base or a framework for mutation testing. The example for “partially-based” tools are EvoSuite [145], jFuzz [193], TrpAutoRepair [299], and GenProg [224]. The self-written tool category represents those tools that have been developed by the authors of the study. The “manual” value means the mutants were generated manually according to mutation operators in the studies. Besides, we defined “n/a” value in addition to the “tool types” attribute; the value of “n/a” marks the situation where lacks of a description of mutation tools including tool names/citations and whether manually generated or not.

(4) mutation operators used in experiments: As for the mutation operators (related to RQ2.2.2), we focus on two attributes: description level and generalised classification. The former is again designed to assess the repeatability issue related to mutation testing. The description degree depends on the way the authors presented the mutation operators used in their studies, consisting of three values: “well-defined”, “not sufficient” and “n/a”. If the paper showed the complete list of mutation operators, then we classify such a paper into “well-defined”. The available full list includes two main situations: (1) the authors listed each name of mutation operator(s) and/or specified how the mutation operators make changes to programs in the articles; (2) the studies adopted existing tools and mentioned the used mutation operator (including the option where all or the default set of mutation operators provided by that tool were used). Thus, the well-defined category enables the traceability of the complete list of mutation operators. Instead, if there is some information about the mutation operators in the article but not enough for the replication of the whole list of mutation operators, then we classify the paper into “not sufficient”. The typical example is that the author used such words as “etc.”, “such as” or, “e.g.” in the specification of the mutation operators; this indicates that only some mutation operators are explicitly listed in the paper, but not all. Finally, we use the label “n/a” when no description of the mutation operators was given in the paper at all.

To compare the mutation operators from different tools for different programming languages, and to analyse the popularity of involved mutation operators amongst the papers, we collected the information about mutation operators mentioned in the articles. Notably, we only consider the articles which are classified as “well-defined”. We excluded the papers with “not sufficient” label as their lists of mutation operators are not complete as this might result in biased conclusions based on incomplete information. Moreover, during the reading process, we found that different mutation testing tools use different naming conventions for their mutation operators. For example, in MuJava [240], the mutation operator which replaces relational operators with other relational operators is called “Relational Operator Replacement”, while that is named “Conditionals Boundary Mutator” in PIT [3]. Therefore, we saw a need to compose a generalised classification of mutation operators, which enables us to more easily compare mutation
operators from different tools or definitions.

The method we adopted here to generate the generalised classification is to group the similar mutation operators among all the existing mutation operators in the literature based on how they mutate the programs. Firstly, mutation testing can be applied to both program source code and program specification. Thus, we classified the mutation operators into two top-level groups: program mutation and specification mutation operators, in a similar vein to Jia and Harman’s survey. As we are more interested in program mutation, we further analysed this area and summarised different mutation operators based on literature. More specifically, we first followed the categories and naming conventions of MuJava [237, 238] and Proteum [43] as their mutation operator groups are more complete than the others. Based on the mutation operator groups from MuJava and Proteum, we further divided the program mutation operators into three subcategories: expression-level, statement-level, and others. The expression-level mutation operators focus on the inner components of the statements, i.e., operators (method-level mutation operators in MuJava [238]) and operands (Constant and Variable Mutations in Proteum [43]), while the statement-level ones mutate at least a single statement (Statement Mutations in Proteum [43]). As we are interested in a more generalised classification independent of the programming language, we came up with the class of “others” to include mutation operators related to the programming language’s unique features, e.g., Objected-Oriented specific and Java-specific mutation operators (Class Mutation in MuJava [237]). It is important to note that our generalised classification of mutation operators aims to provide an overall distribution of different mutation operator groups. Thus, we did not look into lower-level categories. If the paper used one of the mutation operators in one group, we assign the group name to the paper. For example, while the PIT tool only adopts a small number of arithmetic operators [3], we still assign PIT with the “arithmetic operator”.

Our generalised classification of mutation operators is as follows:

Listing 1 Generalised classification of mutation operators

1. Specification mutation

2. Program mutation
   (a) Expression-level
      i. **arithmetic operator**: it mutates the arithmetic operators (including addition “+”, subtraction “-”, multiplication “*”, division “/”, modulus “%”, unary operators “+”, “-”, and short-cut operators “++”, “--”)\(^1\) by replacement, insertion or deletion.
      ii. **relational operator**: it mutates the relational operators (including “>”, “>=”, “<”, “<=”, “==”, “!=”) by replacement.
      iii. **conditional operator**: it mutates the conditional operators (including “&&”, “||”, “&&”, “||”, and negation “!”) by replacement, insertion or deletion.

\(^1\) The syntax of these operators might vary slightly in different languages. Here we just used the operators in Java as an example. So as the same in (ii) - (vi) operators.
iv. **shift operator**: it mutates the shift operators (including “>>, “<<” and “>>>”) by replacement.

v. **bitwise operator**: it mutates the bitwise operators (including bitwise and “&”, bitwise or “|”, bitwise exclusive or “ˆ” and bitwise negation “˜”) by replacement, insertion or deletion.

vi. **assignment operator**: it mutates the assignment operators (including the plain operator “=” and short-cut operators “+=”, “-=”, “*=”, “/=”, “%=”, “&=”, “|=”, “ˆ=”, “<<=”, “>>=”, “>>>=”) by replacement. Besides, the plain operator “=” is also changed to “==” in some cases.

vii. **absolute value**: it mutates the arithmetic expression by preceding unary operators including ABS (computing the absolute value), NEGABS (compute the negative of the absolute value) and ZPUSH (testing whether the expression is zero. If the expression is zero, then the mutant is killed; otherwise execution continues and the value of the expression is unchanged)².

viii. **constant**: it changes the literal value including increasing/decreasing the numeric values, replacing the numeric values by zero or swapping the boolean literal (true/false).

ix. **variable**: it substitutes a variable with another already declared variable of the same type and/or of a compatible type.³

x. **type**: it replaces a type with another compatible type including type casting.⁴

xi. **conditional expression**: it replaces the conditional expression by true/false so that the statements following the conditional always execute or skip.

xii. **parenthesis**: it changes the precedence of the operation by deleting, adding or removing the parentheses.

(b) **Statement-level**

i. **return statement**: it mutates return statements in the method calls including return value replacement or return statement swapping.

ii. **switch statement**: it mutates switch statements by making different combinations of the switch labels (case/default) or the corresponding block statement.

iii. **if statement**: it mutates if statements including removing additional semicolons after conditional expressions, adding an else branch or replacing last else if symbol to else.

iv. **statement deletion**: it deletes statements including removing the method calls or removing each statement⁵.

²The definition of this operator is from the Mothra¹⁰ system. In some cases, this operator only applies the absolute value replacement.

³The types of the variables varies in different programming languages.

⁴The changes between the objects of the parent and the child are excluded which belongs to “OO-specific”

⁵To maintain the syntactical validity of the mutants, semicolons or other symbols, such as continue in Fortran, are retained.
v. **statement swap**: it swaps the sequences of statements including rotating the order of the expressions under the use of the comma operator, swapping the contained statements in `if-then-else` statements and swapping two statements in the same scope.

vi. **brace**: it moves the closing brace up or down by one statement.

vii. **goto label**: it changes the destination of the `goto` label.

viii. **loop trap**: it introduces a guard (trap after n\textsuperscript{th} loop iteration) in front of the loop body. The mutant is killed if the guard is evaluated the n\textsuperscript{th} time through the loop.

ix. **bomb statement**: it replaces each statement by a special `Bomb()` function. The mutant is killed if the `Bomb()` function is executed which ensures each statement is reached.

x. **control-flow disruption (break/continue)**: it disrupts the normal control flow by adding, removing, moving or replacing `continue/break` labels.

xi. **exception handler**: it mutates the exception handlers including changing the `throws`, `catch` or `finally` clauses.

xii. **method call**: it changes the number or position of the parameters/arguments in a method call, or replace a method name with other method names that have the same or compatible parameters and result type.

xiii. **do statement**: it replaces `do` statements with `while` statements.

xiv. **while statement**: it replaces `while` statements with `do` statements.

(c) Others

i. **OO-specific**: the mutation operators related to O(bject)-O(riented) Programming features [237], such as Encapsulation, Inheritance, and Polymorphism, e.g. `super` keyword insertion.

ii. **SQL-specific**: the mutation operators related to SQL-specific features [342], e.g. replacing `SELECT` to `SELECT DISTINCT`.

iii. **Java-specific**: the mutation operators related to Java-specific features [237] (the operators in Java-Specific Features), e.g. `this` keyword insertion.

iv. **JavaScript-specific**: the mutation operators related to JavaScript-specific features [252] (including DOM, JQUERY, and XMLHTTPREQUEST operators), e.g. `var` keyword deletion.

v. **SpreadSheet-specific**: the mutation operators related to SpreadSheet-specific features [61], e.g. changing the range of cell areas.

vi. **AOP-specific**: the mutation operators related to A(spect)-O(riented)-P(rogramming) features [110, 372], e.g. removing pointcut.

vii. **concurrent mutation**: the mutation operators related to concurrent programming features [182, 183], e.g. replacing `notifyAll()` with `notify()`.

viii. **Interface mutation**: the mutation operators related to Interface-specific features [184, 375], suitable for use during integration testing.

---

6This set of mutation operators originated from Java features but not limited to Java language, since other languages can share certain features, e.g., `this` keyword is also available in C++ and C#, and `static` modifier is supported by C and C++ as well.
(5) description of the equivalent mutant problem & (6) description of cost reduction techniques for mutation testing:

The fifth and sixth facets aim to show how the most significant problems are coped with when applying mutation testing (related to RQ2.2.3 and RQ2.2.4 respectively). We composed the list of techniques based on both our prior knowledge and the descriptions given in the papers. We identified seven methods for dealing with the equivalent mutant problem and five for reducing computational cost except for “n/a” set (more details are given in Table 2.3).

For the equivalent mutant problem, we started by searching the keywords “equivalent” and “equal” in each paper to target the context of the equivalent mutant issue. Then we extracted the corresponding text from the articles. If there are no relevant findings in a paper, we mark this article as “n/a” which means the authors did not mention how they overcame the equivalent mutant problem. Here, it should be noted that we only considered the description related to the equivalent mutant problem given by the authors; this means we excluded the internal heuristic mechanisms adopted by the existing tools if the author did not point out such internal approaches. For example, the tool of JAVALANCHE [313] ranks mutations by impact to help users detect the equivalent mutants. However, if the authors who used JAVALANCHE did not specify that internal feature, we do not label the paper into the class that used the approach of “ranking the mutations”.

For the cost reduction techniques, we read the experiment part carefully to extract the reduction mechanism from the papers. Also, we excluded runtime optimisation and selective mutation. The former one, runtime optimisation, is an internal optimisation adopted during the tool implementation, therefore such information is more likely to be reported in the tool documentation. We did not consider the runtime optimisation to avoid incomplete statistics. As for the second one, selective mutation, we assume it is adopted by all papers since it is nearly impossible to implement and use all the operators in practice. If a paper does not contain any description of the reduction methods in the experiment part, we mark this article as “n/a”.

(7) subjects involved in the experiment:

For the subject programs in the evaluation part, we are interested in three aspects: programming language, size, and data availability. From the programming language, we can obtain an overall idea of how established mutation testing is in each programming language domain and what the current gap is. From the subject size, we can see the scalability issue related to mutation testing. From the data availability situation, we can assess the replicability of the studies.

For the programming language, we extracted the programming language of the subjects involved in the experiment in these articles, such as Java, C, SQL, etc. If the programming language of the subject programs is not clearly pointed out, we mark it as “n/a”. Note, more than one languages might be involved in a single experiment.

For the subject size, we defined four categories according to the lines of code (LOC): preliminary, small, medium and large. If the subject size is less than 100 LOC, then we classify it into the “preliminary” category. If the size is between 100 to 10K LOC, we consider it “small”, while between 10K and 1M LOC we appraised it as “medium”. If the size is greater than 1M LOC, we consider it as “large”. Since our size scale is based on LOC,
if the LOC of the subject is not given, or other metrics are used, we mark it as “n/a”. To assign the value to paper, we always take the biggest subjects used in the papers.

For the data available, we defined two classes: Yes and No. “Yes” means all subjects in the experiments can be openly accessible; this can be identified either from the keywords “open source”, SIR [126], GitHub7, SF100 [146] or SourceForge8, or from the open link provided by the authors. It is worth noting that if one of the subjects used in a study is not available, we classify the paper as “No”.

The above facets of interest and corresponding attributes and detailed specification of values are listed in Table 2.3.

<table>
<thead>
<tr>
<th>Facet</th>
<th>Attribute</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rules</td>
<td>classification</td>
<td>assessment</td>
<td>assessing the fault-finding effectiveness improving other quality assurance processes as guidance</td>
</tr>
<tr>
<td></td>
<td>guide</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Quality assurance processes</td>
<td>category</td>
<td>test data generation</td>
<td>creating test input data reducing the test suite size while maintaining its fault detection ability</td>
</tr>
<tr>
<td></td>
<td></td>
<td>test-suite reduction/selection</td>
<td>evaluating test strategies by carrying out the corresponding whole testing procedure, including test pool creation, test case selection and/or augmentation and testing results analysis</td>
</tr>
<tr>
<td></td>
<td></td>
<td>test strategy evaluation</td>
<td>simplifying the test case by shortening the sequence and removing irrelevant statements</td>
</tr>
<tr>
<td></td>
<td></td>
<td>test-case minimisation</td>
<td>reordering the execution sequence of test cases generating or selecting test oracle data</td>
</tr>
<tr>
<td></td>
<td></td>
<td>test case prioritisation</td>
<td>reordering the execution sequence of test cases generating or selecting test oracle data</td>
</tr>
<tr>
<td></td>
<td></td>
<td>test oracle</td>
<td>defining the detective part of a program given the test execution information granting patches to correct detective part of a program</td>
</tr>
<tr>
<td></td>
<td></td>
<td>program repair</td>
<td>evaluating the practice of software development process via observational studies or controlled experiments, such as Test-Driven Development (TDD)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>development scheme evaluation</td>
<td>evaluating the quality of the model at specification level using static analysis techniques</td>
</tr>
<tr>
<td></td>
<td></td>
<td>model clone detection</td>
<td>identifying similar model fragments within a given context</td>
</tr>
<tr>
<td></td>
<td></td>
<td>model review</td>
<td>determining the quality of the model at specification level using static analysis techniques</td>
</tr>
<tr>
<td></td>
<td></td>
<td>fault tolerance</td>
<td>assessing the ability of the system to continue operating properly in the event of failure</td>
</tr>
<tr>
<td></td>
<td>test level</td>
<td>unit</td>
<td>quality assurance processes focus on unit level. A typical example of unit testing includes: using unit testing tools, such as Junit and Nunit, intra-method testing, intra-class testing</td>
</tr>
<tr>
<td></td>
<td></td>
<td>integration</td>
<td>quality assurance processes focus on integration level. A typical example of integration testing includes: caller/callee and inter-class testing</td>
</tr>
<tr>
<td></td>
<td></td>
<td>system</td>
<td>quality assurance processes focus on system level. A typical example of system testing include: high-level model-based testing techniques and high-level specification abstraction methods</td>
</tr>
<tr>
<td></td>
<td></td>
<td>others</td>
<td>quality assurance processes are not related to source code. A typical example includes: grammar</td>
</tr>
<tr>
<td></td>
<td></td>
<td>n/a</td>
<td>no specification about the testing level in the article.</td>
</tr>
<tr>
<td></td>
<td>testing strategy</td>
<td>structural</td>
<td>white-box testing uses the internal structure of the software to derive test cases, such as statement testing, branch testing, and condition testing</td>
</tr>
<tr>
<td></td>
<td></td>
<td>enhanced structural</td>
<td>adopting other methods to improve the traditional structural testing, mutation-based techniques, information retrieval knowledge, observation notations and assertion coverage</td>
</tr>
<tr>
<td></td>
<td></td>
<td>specification-based</td>
<td>viewing software as a black box with input and output, such as equivalence partitioning, boundary value analysis, decision tables and state transition testing</td>
</tr>
<tr>
<td></td>
<td></td>
<td>enhanced specification-based</td>
<td>adopting other methods to improve the traditional specification-based testing, such as mutation testing, maximising the diversity of test cases to improve the test effectiveness combining structural testing and specification testing together using static analysis, or focusing on other testing techniques which cannot fit in above six classes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>similarity-based</td>
<td>white-box testing uses the internal structure of the software to derive test cases, such as statement testing, branch testing, and condition testing</td>
</tr>
<tr>
<td></td>
<td></td>
<td>grey-box</td>
<td>white-box testing uses the internal structure of the software to derive test cases, such as statement testing, branch testing, and condition testing</td>
</tr>
<tr>
<td></td>
<td></td>
<td>others</td>
<td>white-box testing uses the internal structure of the software to derive test cases, such as statement testing, branch testing, and condition testing</td>
</tr>
<tr>
<td>Mutation Tools</td>
<td>availability</td>
<td>Yes/No</td>
<td>Yes: open to the public; No: no valid open access</td>
</tr>
<tr>
<td>type</td>
<td>existing tool</td>
<td>yes/No</td>
<td>a complete mutation testing system used as a base or framework for mutation testing developed by the authors and the open link of the tool is also accessible</td>
</tr>
<tr>
<td></td>
<td>partially-based</td>
<td>self-written</td>
<td>generating mutants manually based on the mutation operators</td>
</tr>
<tr>
<td></td>
<td>manual</td>
<td>n/a</td>
<td>no description of the adopted mutation testing tool</td>
</tr>
<tr>
<td>Mutation Operators</td>
<td>description Level</td>
<td>well-defined</td>
<td>the complete list of mutation operators is available the article provides some information about mutation operators but the information is not enough for replication</td>
</tr>
<tr>
<td></td>
<td>not sufficient</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

7https://github.com/  
8https://sourceforge.net/

<table>
<thead>
<tr>
<th>Equivalence Solver</th>
<th>methods</th>
<th>no description of the mutation operators</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>not killed as equivalent</td>
<td>treating mutants not killed as equivalent</td>
</tr>
<tr>
<td></td>
<td>not killed as non-equivalent</td>
<td>treating mutants not killed as non-equivalent</td>
</tr>
<tr>
<td></td>
<td>no investigation</td>
<td>no distinguishing between equivalent mutants and non-equivalent ones</td>
</tr>
<tr>
<td></td>
<td>manual</td>
<td>manual investigation</td>
</tr>
<tr>
<td></td>
<td>model checker</td>
<td>using model checker to remove functionally equivalent mutants</td>
</tr>
<tr>
<td></td>
<td>reduce likelihood</td>
<td>generating mutants that are less likely to be equivalent, such as using behaviour-affecting variables, carefully-designed mutation operators, and constraints binding</td>
</tr>
<tr>
<td></td>
<td>deterministic model</td>
<td>adopting the deterministic model to make the equivalence problem decidable</td>
</tr>
<tr>
<td></td>
<td>n/a</td>
<td>no description of mutant equivalence detector</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Reduction Technique</th>
<th>methods</th>
<th>random selection technique</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>mutant sample</td>
<td>randomly select a subset of mutants for testing execution based on fixed selection ratio</td>
</tr>
<tr>
<td></td>
<td>fixed number</td>
<td>select a subset of mutants based on a fixed number</td>
</tr>
<tr>
<td></td>
<td>weak mutation</td>
<td>compare internal state of the mutant and the original program immediately after the mutated statement(s)</td>
</tr>
<tr>
<td></td>
<td>higher-order</td>
<td>reduce the number of mutants by selecting higher-order mutants which contain more than one fault</td>
</tr>
<tr>
<td></td>
<td>selection strategy</td>
<td>generate fewer mutants by selecting where to mutate based on a random algorithm or other techniques</td>
</tr>
<tr>
<td></td>
<td>n/a</td>
<td>no description of reduction techniques (except for runtime optimisation and selective mutation)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Subject</th>
<th>language</th>
<th>various programming languages</th>
</tr>
</thead>
<tbody>
<tr>
<td>size (maximum)</td>
<td>preliminary</td>
<td>&lt;100 LOC</td>
</tr>
<tr>
<td></td>
<td>small</td>
<td>100 – 10K LOC</td>
</tr>
<tr>
<td></td>
<td>medium</td>
<td>10K – 1M LOC</td>
</tr>
<tr>
<td></td>
<td>large</td>
<td>&gt; 1M LOC</td>
</tr>
<tr>
<td></td>
<td>n/a</td>
<td>no description of program size regarding LOC</td>
</tr>
</tbody>
</table>

Table 2.3: Attribute framework

2.3.4. Review Protocol Validation

The review protocol is a critical element of a systematic literature review and researchers need to specify and carry out procedures for its validation [85]. The validation procedure aims to eliminate the potential ambiguity and unclear points in the review protocol specification. In this review, we conduct the review protocol validation among the three authors. We also used the results to improve our review protocol. The validation focuses on selection criteria and attribute framework, including the execution of two pilot runs of study selection procedure and data extraction process.

Selection Criteria Validation.

We performed a pilot run of the study selection process, for which we randomly generated ten candidate papers from selected venues (including articles out of our selection scope) and carried out the paper selection among the three authors independently based on the inclusion/exclusion criteria. After that, the three authors compared and discussed the selection results. The results show that for 9 out of 10 papers, the authors had an immediate agreement. The three authors discussed the one paper that showed disagreement, leading to a revision of the first inclusion/exclusion criterion. In the first exclusion criterion, we added “solely” to the end of the sentence “...This criterion excludes the research on mutation testing itself...”. By adding “solely” to the first criterion, we include articles whose main focus is mutation testing, but also cover the application of mutation testing.
To execute the pilot run of the data extraction process, we randomly select ten candidate papers from our selected collection. These 10 papers are classified by all three authors independently using the attribute framework that we defined earlier. The discussion that follows from this process leads to revisions of our attribute framework. Firstly, we clarified that the information extracted from the papers must have the same meaning as described by the authors; this mainly means that we cannot further interpret the information. If the article does not provide any clear clue for a certain attribute, we use the phrase “not specified” (“n/a”) to mark this situation. By doing so, we minimise the potential misinterpretation of the articles.

Secondly, we ensured that the values of the attribute framework are as complete as possible so that for each attribute we can always select a value. For instance, when extracting quality assurance processes information from the papers, we can simply choose one or several options of the 12 categories provided by the predefined attribute framework. The purpose of providing all possible values to each attribute is to assist data extraction in an unambiguous and trustworthy manner. Through looking at the definitions of all potential values for each attribute, we can easily target unclear or ambiguous points in data extraction strategy. If there are missing values for certain attributes, we can only add the additional data definition to extend the framework. The attribute framework can also be of clear guideline for future replication. Furthermore, we can then present quantitative distributions for each attribute in our later discussion to support our answers to research questions.

To achieve the above two goals, we made revisions to several attributes as well as values. The specified modifications are listed as follows:

**Mutation Tools:** Previously, we combined tool availability and tool types by defining three values: self-written, existing and not available; this is not clear to distinguish available tools from unavailable ones. Therefore, we further defined two attributes, i.e., tool availability and tool types.

**Mutation Operators:** We added “description level” to address the interest of how mutation operators are specified in the articles; this also helps in the generalisation of mutation operator classification.

**Reduction Techniques:** We added the “fixed number” value to this attribute which means the fixed number of selected mutants.

**Subjects:** We changed the values of “data availability” from “open source”, “industrial” or “self-defined” to “Yes” or “No”. Since the previous definitions cannot distinguish between available and unavailable datasets.

### 2.4. Review Results

After developing the review protocol, we conducted the task of article characterisation accordingly. Given the attribute assignment under each facet, we are now at the stage of interpreting the observations and reporting our results. In the following section, we discuss our review results following the sequence of our research questions. While Section 2.4.1 deals with the observations related to how mutation testing is applied (RQ2.1), Section 2.4.2 will present the RQ2.2-related discussion. For each sub-research question, we will first show the distribution of the relevant attributes and our interpretation of the
Table 2.4: Summary of quality assurance processes

<table>
<thead>
<tr>
<th>Testing Activity</th>
<th>No. of papers classified as “assessment”</th>
<th>No. of papers classified as “guide”</th>
<th>No. of papers</th>
</tr>
</thead>
<tbody>
<tr>
<td>test data generation</td>
<td>38</td>
<td>36</td>
<td>75</td>
</tr>
<tr>
<td>test strategy evaluation</td>
<td>63</td>
<td>6</td>
<td>70</td>
</tr>
<tr>
<td>test oracle</td>
<td>13</td>
<td>5</td>
<td>18</td>
</tr>
<tr>
<td>test case prioritisation</td>
<td>11</td>
<td>6</td>
<td>17</td>
</tr>
<tr>
<td>test-suite selection/reduction</td>
<td>10</td>
<td>5</td>
<td>15</td>
</tr>
<tr>
<td>fault localisation</td>
<td>8</td>
<td>4</td>
<td>12</td>
</tr>
<tr>
<td>program repairing</td>
<td>2</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>test case minimisation</td>
<td>1</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>fault tolerance</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>development scheme evaluation</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>model clone detection</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>model review</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Total</td>
<td>134</td>
<td>57</td>
<td>191</td>
</tr>
</tbody>
</table>

results (marked as Observation). Each answer to a sub-research question is also summarised at the end. More detailed characterisations results of all the surveyed papers are presented in our GitHub repository [23].

2.4.1. RQ2.1: HOW IS MT USED IN QUALITY ASSURANCE PROCESSES?

RQ2.1.1 & RQ2.1.2: WHICH ROLE DOES MUTATION TESTING PLAY IN EACH QUALITY ASSURANCE PROCESS?

Observation.

We opt to discuss the two research questions RQ2.1.1 and RQ2.1.2 together, because it gives us the opportunity to analyse per quality assurance (e.g., test data generation) whether mutation testing is used as a way to guide the technique, or whether mutation testing is used as a technique to assess some (new) approach. Consider Table 2.4, in which we report the role mutation testing plays in the two columns “Assessment” and “Guide” (see Table 2.3 for the explanation about our attribute framework), while the quality assurance processes are projected onto the rows. The table is then populated with our survey results, with the additional note that some papers belong to multiple categories.

As Table 2.4 shows, test data generation and test strategy evaluation occupy the majority of quality assurance processes (accounting for 75.9%) and test suite reduction/selection (7.9%). Only two instances studied test-case minimisation; this shows mutation testing has not been widely used to simplify test cases by shortening the test sequence and removing irrelevant statements.

As the two roles (assessment and guide) are used quite differently depending on the quality assurance processes, we will discuss them separately. Also, for the “guide” role,
for which we see an increasing number of applications in recent decades, we find a number of hints and insights for future researchers to consider, which explains why we will analyse this part in a more detailed way when compared to the description of mutation testing as a tool for assessment.

(1) Assessment.

We observed that mutation testing mainly serves as an assessment tool to evaluate the fault-finding ability of the corresponding test or debug techniques (70.2%) as it is widely considered as a "high end" test criterion [47]. To this aim, mutation testing typically generates a significant number of mutants of a program, which are sometimes also combined with natural defects or hand-seeded ones. The results of the assessment are usually quantified as metrics of fault-finding capability: mutation score (or mutation coverage, mutation adequacy) [51, 53] and killed mutants [76, 107] are the most common metrics in mutation testing. Besides, in test-case prioritisation, the Average Percentage of Faults Detected (APFD) [52, 306], which measures the rate of fault detection per percentage of test suite execution, is also popular.

Amongst the papers in our set, we also found 19 studies that performed mutant analysis, which means that the researchers tried to get a better understanding about mutation faults, e.g., which faults are more valuable in a particular context. A good example of this mutant analysis is the hard-mutant problem investigated by Czemerinski et al. [108] where they analysed the failure rate for the hard-to-kill mutants (killed by less than 20% of test cases) using the domain partition approach.

(2) Guide.

To provide insight into how mutation testing acts as guidance to improve testing methods per quality assurance process, we will highlight the most significant research efforts to demonstrate why mutation testing can be of benefit as a building block to guide other quality assurance processes. In doing so, we hope the researchers in this field can learn from the current achievements so as to explore other interesting applications of mutation testing in the future.

Firstly, let us start with test data generation, which attracts most interest when mutation testing is adopted as a building block (36 instances). The main idea of mutation-based test data generation is to generate test data that can effectively kill mutants. For automatic test data generation, killing mutants serves as a condition to be satisfied by test data generation mechanisms, such as constraint-based techniques and search-based algorithms; in this way, mutation-based test data generation can be transformed into the structural testing problem. The mutation killable condition can be classified into three steps as suggested by Offutt and Untch [277]: reachability, necessity, and sufficiency. When observing the experiments contained in the papers that we surveyed (except the model-based testing), we see that with regard to the killable mutant condition most papers (73.3%) are satisfied with a weak mutation condition (necessity), while a strong mutation condition (sufficiency) appears less (33.3%). The same is true when comparing first-order mutants (93.3%) to higher-order mutants (6.7%). Except for the entirely automatic test data generation, Baudry et al.[67–69] focused on the automation of the test case enhancement phase: they optimised the test cases regarding mutation score via genetic and bacteriological algorithms, starting from an initial test suite. Von Mayrhauser
et al.[356] and Smith and Williams[324] augmented test input data using the requirement of killing as many mutants as possible. Compared to the existing literature survey of Hanh et al. [170], which shed light on mutation-based test data generation, we cover more studies and extend their work to 2015.

The second-most-frequent use cases when applying mutation testing to guide the testing efforts come from test case prioritisation (6 instances) and test strategy evaluation (6 instances). For test case prioritisation, the goal is to detect faults as early as possible in the regression testing process. The incorporation of measures of fault-proneness into prioritisation techniques is one of the directions to overcome the limitation of the conventional coverage-based prioritisation methods. As relevant substitutes of real faults, mutants are used to approximate the fault-proneness capability to reschedule the testing sequences. Qu et al. [300] ordered test cases according to the prior fault detection rate using both hand-seeded and mutation faults. Kwon et al. [221] proposed a linear regression model to reschedule test cases based on Information Retrieval and coverage information, where mutation testing determines the coefficients in the model. Moreover, Rothermel et al. [306, 307] and Elbaum et al. [131] compared different approaches of test-case prioritisation, which included the prioritisation in order of the probability of exposing faults estimated by the killed mutant information. In Qi et al. [299]’s study, they adopted a similar test-case prioritisation method to improve patch validation during program repairing.

Zooming in on the test strategy evaluation (6 instances), we observe, on the one hand, the idea of incorporating an estimation of fault-exposure probability into test data adequacy criteria intrigued some researchers. Among them are Chen et al. [97]: in their influential work they examined the fault-exposing potential (FEP) coverage adequacy which is estimated by mutation testing with four software testers to explore the cost-effectiveness of mutation testing for manually augmenting test cases. Their results indicate that mutation testing was regarded as an effective but relatively expensive technique for writing new test cases.

When it comes to the test oracle problem (5 instances), mutation testing can also be of benefit for driving the generation of assertions, as the prerequisite for killing the mutant is to distinguish the mutant from the original program. In Fraser and Zeller [150]’s study, they illustrated how they used mutation testing to generate test oracles: assertions, as commonly used oracles, are generated based on the trace information of both the unchanged program and the mutants recorded during the executions. First, for each difference between the runs on the original program and its mutants, the corresponding assertion is added. After that, these assertions are minimised to find a sufficient subset to detect all the mutants per test case; this becomes a minimum set covering problem. Besides, Staats et al. [326] and Gay et al. [155] selected the most “effective” oracle data by ranking variables (trace data) based on their killed mutants information.

Mutation-based test-suite reduction (5 instances) relies on the number of killed mutants as a heuristic to perform test-suite reduction, instead of the more frequently used traditional coverage criteria, e.g., statement coverage. The intuition behind this idea is that the reduction based on the mutation faults can produce a better-reduced test suite with less or no loss in fault-detection capability. The notable examples include an empirical study carried out by Shi et al. [319] who compared the trade-offs among various
test-suite reduction techniques based on statement coverage and killed mutants.

As for the fault localisation (4 instances), the locations of mutants are used to assist the localisation of “unknown” faults (the faults which have been detected by at least one test case, but that have still to be located [290]). The motivation of this approach is based on the following observation: “Mutants located on the same program statements frequently exhibit a similar behaviour” [290]. Thus, the identification of an “unknown” fault could be obtained thanks to a mutant at the same (or close) location. Taking advantage of the implicit link between the behaviour of “unknown” faults with some mutants, Murtaza et al. [260] used the traces of mutants and prior faults to train a decision tree to identify the faulty functions. Also, Papadakis et al. [290, 291] and Moon et al. [253] ranked the suspiciousness of “faulty” statements based on their passing and failing test executions of the generated mutants.

From the aforementioned guide roles of the quality assurance processes, we can see that mutation testing is mainly used as an indication of the potential defects: either (1) to be killed in test data generation, test case prioritisation, test-suite reduction, and test strategy evaluation, or (2) to be suspected in the fault localisation. In most cases, mutation testing serves as where-to-check constraints, i.e., introducing a modification in a certain statement or block. In contrast, only four studies applied mutation testing to solving the test oracle problem, which targets the what-to-check issue. The what-to-check problem is not an issue unique to mutation testing, but rather an inherent challenge of test data generation. As mentioned above, mutation testing cannot only help in precisely targeting at where to check but also suggesting what to check for [150] (see the first recommendation labelled as R1 in Section 2.4.4). In this way, mutation testing could be of benefit to improve the test code quality.

After we had analysed how mutation testing is applied to guide various quality assurance processes, we are now curious to better understand how these mutation-based testing methods were evaluated, especially because mutation testing is commonly used as an assessment tool. Therefore, we summed up the evaluation fault types among the articles labelled as “guide” in Table 2.5. We can see 43 cases (75.4%), which is the addition of the first and the third rows in Table 2.5 (39 + 4), still adopted mutation faults to assess the effectiveness. Among these studies, four instances [155, 172, 232, 326] realised the potentially biased results caused by the same set of mutants being used in both guidance and assessment. They partitioned the mutants into different groups and used one as evaluation set. Besides, one study [382] used a different mutation tool, while the other [184] adopted different mutation operators to generate mutants intending to eliminate bias. These findings signal an open issue: how to find an adequate fault set instead of mutation faults to effectively evaluate mutation-based testing methods? (see the second recommendation labelled as R2 in Section 2.4.4) Although hand-seeded faults and real bugs could be an option, searching for such an adequate fault set increases the difficulty when applying mutation testing as guidance.

**Summary.**
Test data generation and test strategy evaluation occupy the majority of quality assurance processes when applying mutation testing (75.9%). While as guidance, mutation testing is primarily used in test data generation (36 instances), test strategy evaluation
(6 instances) and test-case prioritisation (6 instances). From the above observations, we draw one open issue and one recommendation for the “guide” role of mutation testing. The open issue is how to find an adequate fault set instead of mutation faults to effectively evaluate mutation-based testing methods. The recommendation is that mutation testing can suggest not only where to check but also what to check. Where to check is widely used to generate killable mutant constraints in different quality assurance processes, while what to check is seldom adopted to improve the test data quality.

RQ2.1.3: Which test level does mutation testing target?

**Observations.**

Table 2.6 presents the summary of the test level distribution across the articles. We observe that the authors of 84 papers do not provide a clear clue about the test level they target (the class marked as “n/a”). For example, Aichernig et al.[44]’s study: they proposed a fully automated fault-based test case generation technique and conducted two empirical case studies derived from industrial use cases; however, they did not specify which test level they targeted. One good instance that clearly provides the information of the test level is Jee et al.[194] where they specified that their test case generation technique for FBD programs is at unit testing level. This is an open invitation for future investigations in the area to be clearer about the essential elements of quality assurance processes such as the test level. For the remainder of our analysis of RQ2.1.3, we excluded the papers labelled as “n/a” when calculating percentages, i.e., our working set is 107 (191 – 84) papers.

Looking at Table 2.6, mutation testing mainly targets the unit-testing level (72.0%), an observation which is in accordance with the results of Jia and Harman’s survey [197]. One of the underlying causes for the popularity of the unit level could be the origin
of mutation testing. The principle of mutation testing is to introduce small syntactic changes to the original program; this means the mutation operators only focus on small parts of the program, such as arithmetical operators and return statements. Thus, such small changes mostly reflect the abnormal behaviour of unit-level functionality.

While unit testing is by far the most observed test level category in our set of papers, higher-level testing, such as integration testing (15 instances), can also benefit from the application of mutation testing. Here we highlight some research works as examples: Hao et al. [171] and Do and Rothermel [128] used the programs with system test cases as their subjects in case studies. Hou et al. [184] studied interface-contract mutation in support of integration testing under the context of component-based software. Li et al. [229] proposed a two-tier testing method (one for integration level, the other for system level) for graphical user interface (GUI) software testing. Rutherford et al. [310] defined and evaluated adequacy criteria under system-level testing for distributed systems. In Denaro et al. [120]'s study, they proposed a test data generation approach using data flow information for inter-procedural testing of object-oriented programs.

The important point we discovered here is that all the aforementioned studies did not restrict mutation operators to model integration errors or system ones. In other words, the traditional program mutations can be applied to higher-level testing. Amongst these articles, the mutation operators adopted are mostly at the unit level, e.g., Arithmetic Mutation Replacement, Relational Mutation Replacement. The mutation operators designed for higher-level testing, e.g., [112, 243], are seldom used in these studies. The only three exceptions in our collections are Flores and Polo [141], Vincenzi et al. [349] and Flores and Polo [142], who adopted interface mutation to evaluate the integration testing techniques. This reveals a potential direction for future research: the cross-comparison of different levels of mutation operators and quality assurance processes at different test levels (see the third recommendation labelled as R3 in Section 2.4.4). The investigation of different levels of mutants can explore the effectiveness of mutation faults at different test levels, such as the doubts whether the integration-level mutation is better than unit-level mutation when assessing testing techniques at the integration level. In the same vein, an analysis of whether mutants are a good alternative to real/hand-seeded ones (proposed by Andrews et al. [50]) at higher levels of testing also seems like an important avenue to check out.

In addition, we created a class "others" in which we list 9 papers that we found hard to classify in any of the other four test phases. These works can be divided into three groups: grammar-based testing [75, 95, 176], spreadsheet-related testing [61, 179, 180] and SQL-related testing [207, 249, 343]. The application of mutation testing on the "other" set indicates that the definition of mutation testing is actually quite broad, thus potentially leading to even more intriguing possibilities [279]: what else can we mutate?

**Summary.**
The application of mutation testing is mostly done at the unit-level testing (44.0% of papers did not clearly specify their target test level(s)). For reasons of clarity, understandability and certainly replicability, it is very important to understand exactly at what level the quality assurance processes take place. It is thus a clear call to arms to researchers to better describe these essential testing activity features.
Table 2.7: Summary of testing strategies

<table>
<thead>
<tr>
<th>Testing Strategies</th>
<th>Number of papers</th>
</tr>
</thead>
<tbody>
<tr>
<td>structural testing</td>
<td>57</td>
</tr>
<tr>
<td>specification-based testing</td>
<td>52</td>
</tr>
<tr>
<td>structural testing (enhanced)</td>
<td>52</td>
</tr>
<tr>
<td>others</td>
<td>21</td>
</tr>
<tr>
<td>specification-based testing (enhanced)</td>
<td>13</td>
</tr>
<tr>
<td>hybrid testing</td>
<td>7</td>
</tr>
<tr>
<td>similarity-based testing</td>
<td>3</td>
</tr>
</tbody>
</table>

RQ2.1.4: WHICH TESTING STRATEGIES DOES MUTATION TESTING SUPPORT?

OBSERVATIONS.

In Table 2.7 we summarised the distribution of testing strategies based on our coarse-grained classification (e.g., structural testing, specification-based testing) as mentioned in Table 2.3. Looking at Table 2.7, structure-based testing (including the first and the third rows in Table 2.7), 109 instances). The underlying cause could be that structural testing is still the main focus of testing strategies in the software testing context. The other testing strategies have also been supported by mutation testing: (1) specification-based testing (including the second and the fifth rows in Table 2.7) accounts for 65 cases; (2) hybrid testing (combination of structural and structure-based testing) for seven instances, e.g., Briand et al. [86] investigated how data flow information can be used to improve the cost-effectiveness of state-based coverage criteria; (3) three cases applying mutation testing in similarity-based testing; (4) 21 instances in others, e.g., static analysis.

One interesting finding is that enhanced structural testing ranks third, including mutation-based techniques, information retrieval knowledge, observation notations and assertion coverage. The popularity of enhanced structural testing reveals the awareness of the shortage of conventional coverage-based testing strategies has increased.

Compared to enhanced structural testing, enhanced specification-based testing did not attract much interest. The 13 instances mainly adopted mutation testing (e.g., Qu et al. [300] and Papadakis et al. [287]) to improve the testing strategies.

SUMMARY.

Mutation testing has been widely applied in support of different testing strategies. From the observation, the testing strategies other than white box testing can also benefit from the application of mutation testing, such as specification-based testing, hybrid testing, and similarity-based testing. However, structural testing is more popular than the others (57.1%). Moreover, techniques like mutation-based techniques and information retrieval knowledge are also being adopted to improve the traditional structural-based testing, which typically only relies on the coverage information of software artefacts; this serves an indication of the increasing realisation of the limitations of coverage-based testing strategies.
2.4. Review Results

Table 2.8: Summary of mutation tool availability

<table>
<thead>
<tr>
<th>Availability</th>
<th>Types</th>
<th>Number of papers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>existing</td>
<td>96</td>
</tr>
<tr>
<td></td>
<td>partially-based</td>
<td>7</td>
</tr>
<tr>
<td></td>
<td>self-written</td>
<td>1</td>
</tr>
<tr>
<td>No</td>
<td>n/a (no information)</td>
<td>44</td>
</tr>
<tr>
<td></td>
<td>existing (given the name/citation)</td>
<td>22</td>
</tr>
<tr>
<td></td>
<td>self-written</td>
<td>14</td>
</tr>
<tr>
<td></td>
<td>manual</td>
<td>12</td>
</tr>
</tbody>
</table>

2.4.2. RQ2.2: How are empirical studies related to mutation testing designed and reported?

RQ2.2.1: Which mutation testing tools are being used?

Observations.

We are interested in getting insight into the types (as defined in Table 2.3) of mutation testing tools that are being used and into their availability. Therefore, we tabulated the different types of mutation testing tools and their availability in Table 2.8. As shown in Table 2.8, 50.3% of the studies adopted existing tools which are open to the public; this matches our expectation: as mutation testing is not the main focus of the studies, if there exists a well-performing and open-source mutation testing tool, researchers are likely willing to use these tools. However, we also encountered 15 cases of using self-implemented tools and 12 studies that manually applied mutation operators. A likely reason for implementing a new mutation testing tool or for manually applying mutation operators is that existing tools do not satisfy a particular need of the researchers. Besides, most existing mutation testing tools are typically targeting one specific language and a specific set of mutation operators [279] and they are not always easy to extend, e.g., when wanting to add a newly-defined mutation operator. As such, providing more flexible mechanisms for creating new mutation operators in mutation testing tools is an important potential direction for future research [211, 279] (see the fourth recommendation labelled as R4 in Section 2.4.4).

Unfortunately, there are also still 92 studies (48.2%) that do not provide access to the tools, in particular, 44 papers did not provide any accessible information about the tools (e.g., Hong et al. [183], Belli et al. [76] and Papadakis and Malveris [294]), a situation that we marked as “n/a” in Table 2.8. This unclarity should serve as a notice to researchers: the mutation testing tool is one of the core elements in mutation testing, and lack of information on it seriously hinders replicability of the experiments.

Having discussed the tool availability and types, we are wondering which existing open-source mutation testing tools are most popular. The popularity of the tools cannot only reveal their level of maturity, but also provide a reference for researchers entering the field to help them choose a tool. To this end, we summarised the names of mutation tools for different programming languages in Table 2.9. Table 2.9 shows that we encountered 19 mutation tools in total. Most tools target one programming language (except
Table 2.9: Summary of existing mutation tools

<table>
<thead>
<tr>
<th>Language</th>
<th>Tool</th>
<th>Number of papers</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Java</strong></td>
<td>MuJava/μ-java/Muclipse</td>
<td>41</td>
</tr>
<tr>
<td></td>
<td>JAVALANCHE</td>
<td>9</td>
</tr>
<tr>
<td></td>
<td>MAJOR</td>
<td>9</td>
</tr>
<tr>
<td></td>
<td>PIT/PrTest</td>
<td>7</td>
</tr>
<tr>
<td></td>
<td>Jumble</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>Sofya</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Jester</td>
<td>1</td>
</tr>
<tr>
<td><strong>C</strong></td>
<td>Proteum</td>
<td>12</td>
</tr>
<tr>
<td></td>
<td>Proteum/IM</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>MiLu</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>SMT-C</td>
<td>1</td>
</tr>
<tr>
<td><strong>Fortran</strong></td>
<td>Mothra</td>
<td>4</td>
</tr>
<tr>
<td><strong>SQL</strong></td>
<td>SQLMutation/JDAMA</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>SchemaAnalyst</td>
<td>1</td>
</tr>
<tr>
<td><strong>C#</strong></td>
<td>GenMutants</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>PexMutator</td>
<td>1</td>
</tr>
<tr>
<td><strong>JavaScript</strong></td>
<td>MUTANDIS</td>
<td>3</td>
</tr>
<tr>
<td><strong>AspectJ</strong></td>
<td>AjMutator</td>
<td>2</td>
</tr>
<tr>
<td><strong>UML specification</strong></td>
<td>MoMuT::UML</td>
<td>1</td>
</tr>
</tbody>
</table>

for Mothra [210], which supports both C and Fortran). We encountered seven mutation tools for Java, with the top 3 most-used being MuJava [239], JAVALANCHE [313] and Major [204]. We found that four mutation tools for C are used, where Proteum [113] is the most-frequently applied. Proteum/IM [114] is a special mutation testing tool that targets interface mutation, which concerns integration errors. The integration errors are related to a connection between two units and the interactions along the connection, such as a wrong subprogram call.

In Jia and Harman [197]’s literature review, they summarised 36 mutation tools developed between 1977 and 2009. When comparing their findings (36 tools) to ours (19 tools), we find that there are 12 tools in common. The potential reason for us not covering the other 24 is that we only consider peer-reviewed conference papers and journals; this will likely filter some papers which applied the other 24 mutation tools. Also important to stress, is that the goal of Jia and Harman’s survey is different to ours: while we focus on the application of mutation tools, their study surveys articles that introduce mutation testing tools. In doing so, we still managed to discover 8 mutation tools which are not covered by Jia and Harman: (1) two tools are for Java: PIT and Sofya; (2) one for C: SMT-C; (3) one for SQL: SchemaAnalyst; (4) one for UML: MoMuT::UML; (5) two for C#: GenMutants and PexMutator; (6) one for JavaScript: MUTANDIS. Most of these tools
were released after 2009, which makes them too new to be included in the review of Jia and Harman. Moreover, we can also witness the trend of the development of the mutation testing for programming languages other than Java and C when compared to Jia and Harman’s data.

**Summary.**

50.3% of the articles that we have surveyed adopt existing (open access) tools, while in a few cases (27 in total) the authors implemented their own tools or seeded the mutants by hand. This calls for a more flexible mutation generation engine that allows to easily add mutation operators or certain types of constraints. Furthermore, we found 44 papers that did not provide any information about the mutation tools they used in their experiments; this should be a clear call to arms to the research community to be more precise when reporting on mutation testing experiments. We have also gained insight into the most popular tools for various programming languages, e.g., MuJava for Java and Proteum for C. We hope this list of tools can be a useful reference for new researchers who want to apply mutation testing.

**RQ2.2.2: Which mutation operators are being used?**

**Observations**

For the mutation operators, we first present the distribution of the three description levels (as mentioned in Table 2.3) in Table 2.10. As Table 2.10 shows, 62.3% (119 instances) of the studies that we surveyed specify the mutation operators that they use, while more than one-third of the articles do not provide enough information about the mutation operators to replicate the studies. These 61 instances are labelled as “n/a” (e.g., Briand et al., DeMillo and Offutt, and Shi et al.).

After that, based on our generalised classification of the mutation operators (as defined in Listing 1), we characterised the 119 papers labelled as “well-defined”. In addition to the overall distribution of the mutation operators regardless of the programming language, we are also interested in the differences of the mutation operators for different languages as the differences could indicate potential gaps in the existing mutation operator sets for certain programming languages. In Table 2.11 we project the various languages onto seven columns and our predefined mutation operator categories onto the rows, thus presenting the distribution of the mutation operators used in the literature under our research scope.

Overall, we can see that program mutation is more popular than specification mutation from Table 2.11. Among the program mutation operators, the arithmetic, rela-
Table 2.11: Mutation operators used in our collection

<table>
<thead>
<tr>
<th>Level</th>
<th>Operator</th>
<th>Java</th>
<th>C</th>
<th>C++</th>
<th>C#</th>
<th>Fortran</th>
<th>SQL</th>
<th>JavaScript</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specification Mutation</td>
<td></td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>23</td>
</tr>
<tr>
<td>Program Mutation</td>
<td></td>
<td>55</td>
<td>12</td>
<td>4</td>
<td>3</td>
<td>2</td>
<td>5</td>
<td>1</td>
<td>95</td>
</tr>
<tr>
<td></td>
<td>arithmetic operator</td>
<td>51</td>
<td>10</td>
<td>4</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>-</td>
<td>-79</td>
</tr>
<tr>
<td></td>
<td>relational operator</td>
<td>47</td>
<td>8</td>
<td>4</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>-</td>
<td>-74</td>
</tr>
<tr>
<td></td>
<td>conditional operator</td>
<td>47</td>
<td>7</td>
<td>4</td>
<td>2</td>
<td>2</td>
<td>3</td>
<td>-</td>
<td>-72</td>
</tr>
<tr>
<td></td>
<td>bitwise operator</td>
<td>36</td>
<td>4</td>
<td>2</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-43</td>
</tr>
<tr>
<td></td>
<td>assignment operator</td>
<td>33</td>
<td>4</td>
<td>2</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-39</td>
</tr>
<tr>
<td></td>
<td>constant</td>
<td>18</td>
<td>5</td>
<td>2</td>
<td>-</td>
<td>2</td>
<td>3</td>
<td>-</td>
<td>-37</td>
</tr>
<tr>
<td></td>
<td>shift operator</td>
<td>33</td>
<td>2</td>
<td>2</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-36</td>
</tr>
<tr>
<td></td>
<td>variable</td>
<td>15</td>
<td>4</td>
<td>2</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td>31</td>
<td></td>
</tr>
<tr>
<td></td>
<td>absolute value</td>
<td>19</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>-</td>
<td>-31</td>
</tr>
<tr>
<td></td>
<td>conditional expression</td>
<td>9</td>
<td>3</td>
<td>-</td>
<td>1</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-14</td>
</tr>
<tr>
<td></td>
<td>parenthesis</td>
<td>1</td>
<td>2</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-3</td>
</tr>
<tr>
<td></td>
<td>type</td>
<td>-</td>
<td>3</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>Expression-level</td>
<td>statement deletion</td>
<td>11</td>
<td>4</td>
<td>2</td>
<td>2</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-23</td>
</tr>
<tr>
<td></td>
<td>method call</td>
<td>11</td>
<td>-</td>
<td>2</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>1</td>
<td>16</td>
</tr>
<tr>
<td></td>
<td>return statement</td>
<td>10</td>
<td>3</td>
<td>-</td>
<td>2</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-16</td>
</tr>
<tr>
<td></td>
<td>control-flow disruption</td>
<td>6</td>
<td>2</td>
<td>2</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-9</td>
</tr>
<tr>
<td></td>
<td>exception handler</td>
<td>1</td>
<td>-</td>
<td>1</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-5</td>
</tr>
<tr>
<td></td>
<td>goto label</td>
<td>-</td>
<td>3</td>
<td>-</td>
<td>2</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-6</td>
</tr>
<tr>
<td></td>
<td>statement swap</td>
<td>2</td>
<td>2</td>
<td>-</td>
<td>2</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-5</td>
</tr>
<tr>
<td></td>
<td>bomb statement</td>
<td>-</td>
<td>2</td>
<td>-</td>
<td>2</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-5</td>
</tr>
<tr>
<td></td>
<td>switch statement</td>
<td>2</td>
<td>3</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-5</td>
</tr>
<tr>
<td></td>
<td>do statement</td>
<td>-</td>
<td>2</td>
<td>-</td>
<td>2</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-5</td>
</tr>
<tr>
<td></td>
<td>brace</td>
<td>-</td>
<td>3</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-3</td>
</tr>
<tr>
<td></td>
<td>loop trap</td>
<td>-</td>
<td>3</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-3</td>
</tr>
<tr>
<td></td>
<td>while statement</td>
<td>-</td>
<td>3</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-3</td>
</tr>
<tr>
<td></td>
<td>if statement</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>Statement-level</td>
<td>OO-specific</td>
<td>23</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-26</td>
</tr>
<tr>
<td></td>
<td>Java-specific</td>
<td>17</td>
<td>-</td>
<td>1</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-17</td>
</tr>
<tr>
<td></td>
<td>Interface mutation</td>
<td>4</td>
<td>2</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-7</td>
</tr>
<tr>
<td></td>
<td>SQL-specific</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Concurrent mutation</td>
<td>4</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-4</td>
</tr>
<tr>
<td></td>
<td>AOP-specific</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-3</td>
</tr>
<tr>
<td></td>
<td>Spreadsheet-specific</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-2</td>
</tr>
<tr>
<td></td>
<td>JavaScript-specific</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

tional and conditional operators are the top 3 mutation operators. These three operators are often used together in most cases as their total number of applications are similar. The underlying cause of the popularity of these three operators could be that the three operators are among Offutt et al.[271]’s 5 sufficient mutation operators. Moreover, the expression-level operators are more popular than the statement-level ones. As for the statement-level mutation operators, statement deletion, method call, and return statement are the top 3 mutation operators.

When we compare the mutation operators used in different languages to our mutation operator categories, we see that there exist differences between different programming languages, just like we assumed. Table 2.11 leads to several interesting findings that reveal potential gaps in various languages (note that Table 2.11 only listed seven programming languages that have been widely used). Moreover, as Jia and Harman [197] also discussed mutation operators in their review, it is interesting to see whether their
summary agrees with our work. Therefore, we also compared our findings to Jia and Harman’s as follows:

1. For Java, seven mutation operators at the expression and statement level (except go to label which is not supported in Java) are not covered by our survey: type, bomb statement, do statement, brace, loop trap, while statement and if statement. Compared to Jia and Harman’s survey, Alexander et al. [45, 79]’s design of Java Object mutation cannot be found in our collection.

2. For C, only two operators are not covered by our dataset. The C programming language does not provide direct support for exception handling. There is no article applying mutation operators that target specific C program defects or vulnerabilities surveyed by Jia and Harman, such as buffer overflows [348] and format string bugs [318].

3. For C++, 3 expression-level, 10 statement-level and the OO-specific operators are not used in our dataset. Jia and Harman have not covered mutation operators for C++.

4. For C#, only a limited set of mutation operators are applied based on our dataset. Our collection has no application of OO-specific operators [123] summarised in Jia and Harman’s survey.

5. For Fortran, the earliest programming language mutation testing was applied to, the studies in our collection cover a basic set. These mutation operators agree with Jia and Harman’s work.

6. For SQL, since the syntax of SQL is quite different from imperative programming languages, only six operators at the expression level and SQL-specific ones are used in our dataset. Compared to Jia and Harman’s literature review, a set of mutation operators addressing SQL injection vulnerabilities [317] are not found in our collection.

7. For JavaScript, only three JavaScript-specific mutation operators are adopted in studies we selected. Mutation operators for JavaScript [251] have not been covered by Jia and Harman as the paper introducing them (i.e., Milani et al.[251]) is more recent.

8. For interface mutation, we have found studies solely targeting Java and C in our selection.

The comparison with Jia and Harman’s literature review has shown that for most programming languages (except for C++ and JavaScript), a few mutation operators summarised by Jia and Harman have no actual applications in our collection. As we only considered 22 venues, we might miss the studies that adopted these mutation operators in other venues. Without regard to the potential threat of missing papers in our dataset, these mutation operators that have no applications in our collection pose interesting questions for further exploration, e.g., why are these operators seldom used by
other researchers? What is the difference between these operators and other widely used operators?

Also, from the above findings, we can see that for different languages the existing studies did not cover all the mutation operators that we listed in Table 2.11: some are caused by the differences in the syntax, while the others could point to potential gaps. However, these potential gaps are just the initial results in which we neither did further analysis to chart the syntax differences of these languages nor investigate the possibility of the equivalent mutants caused by our classification. Moreover, for some languages, e.g., JavaScript, the relevant studies are too few to draw any definitive conclusions. We can only say that Table 2.11 can be a valuable reference for further investigations into mutation operator differences and gaps in different programming languages.

Furthermore, our generalised classification of the existing mutation operators can also be of benefit to compare mutation tools in the future. Thereby, we compared the existing mutation testing tools (as listed in Table 2.9) to our mutation operator categories in Table 2.12. Table 2.12 is based on the documentation or manuals of these tools. Here we used the definitions of mutation operator groups from Listing 1 (mainly based on MuJava [237, 238] and Proteum [43]) as the baseline: if there is a possible mutation missing in a group for a mutation testing tool, we marked “**” in Table 2.12. As there exist different syntaxes in different programming languages, we also consider syntactic differences when categorising the mutation operators of different tools. For example, there is no modulus operator “%” in Fortran (but a MOD function instead), therefore, when considering the arithmetic mutation operators for Fortran (Mothra), we do not require the modulus operator “%” to be included in Mothra.

It is important to mention that Table 2.9 is not the complete list of all the existing mutation tools that have been published so far; these tools are chosen to investigate how mutation testing supports quality assurance processes. We analyse them here as they are open to public and have been applied by researchers at least once. The analysis of mutation operators in these tools could also be a valuable resource for researchers in mutation testing to consider.

The result shows that none of the existing mutation testing tools we analysed can cover all types of operators we classified. For seven mutation testing tools for Java, they mainly focus on the expression-level mutations and only five kinds of statement-level mutators are covered. Furthermore, MuJava, PIT, and Sofya provide some OO-specific operators, whereas PIT only supports one type, the Constructor Calls Mutator. For the four mutation testing tools for C (including Mothra) that we have considered, Proteum covers the most mutation operators. SMT-C is an exceptional case of the traditional mutation testing which targets semantic mutation testing. Proteum/IM is the only mutation tool listed in Table 2.12 that supports interface mutation. For the tools designed for C#, OO-specific operators are not present.

Moreover, when we further analyse the missing mutations in each mutation operator group (marked as “**” in Table 2.12), we found that most tools miss one or several mutations compared to our generalised classification. Particularly for the arithmetic operator, only MuJava and Proteum apply all possible mutations. The other tools that adopt the arithmetic operator all miss Arithmetic Operator Deletion (as defined in MuJava [238]).

Another interesting finding when we compared Table 2.11 and Table 2.12, is that the
This reinforces our message of the need for “well-defined” mutation operators when re-

Table 2.12: Comparison of mutation operators in existing mutation tools

| Specification Mutation | arithmetic operator | relational operator | conditional operator | assignment operator | bitwise operator | shift operator | constant variable | absolute value | conditional expression | parenthesis | type | statement deletion | method call | return statement | if statement | exception handler | goto label | control-flow disruption | statement swap | bomb statement | switch statement | do statement | brace | loop trap | while statement | OO-specific | Java-specific | SQL-specific | JavaScript-specific | AOP-specific | interface mutation |
|------------------------|---------------------|---------------------|----------------------|---------------------|------------------|----------------|------------------|----------------|----------------------|-------------|--------|-------------------|-------------|------------------|--------------|------------------|-----------|-----------------|---------------|-----------------|-----------------|------------|-----------|----------|-----------------|----------------|------------------|
| MuJava | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - |
| PIT/Pitest [13, 14] | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - |
| MAJOR [2], [39] | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - |
| Jumble [19] | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - |
| PyTest [164] | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - |
| Proteum [14, 163] | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - |
| MiLu [10] | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - |
| ProMaT [15, 160] | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - |
| PIT/PITest [164] | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - |
| Jumble [19] | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - |
| Proteum [14, 163] | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - |
| MoMuT:UML [216] | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - |
| MoMuT::UML [216] | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - |

Note: the entry marked with * means the tool does not provide the full possible mutations. Our summary of the mutation tools is based on the available manuals and open repositories (if they exist) for the tools. If there are different versions of the tools, we only consider the newest one.

If statement mutator is not used in literature, but it is supported by SMT-C. This observation indicates that not all the operators provided by the tools are used in the studies when applying mutation testing. Therefore, we zoom in on this finding and investigate whether it is a common case that only a subset of the mutation operators from the existing mutation tools is adopted in studies based on our collection. The result shows that 21 studies out of 54 applied a subset of the mutation operators from the existing tools; this reinforces our message of the need for “well-defined” mutation operators when re-
porting mutation testing studies.

**Summary.**

For the mutation operators, we focused on two attributes: their description level and a generalised classification across tools and programming languages. When investigating the description level of the mutation operators that are used in studies, we found that 62.3% (119 instances) explicitly defined the mutation operators used; this leads us to strongly recommend improving the description level for the sake of replicability. Furthermore, the distribution of mutation operators based on our predefined categories shows the lacking of certain mutation operators in some programming languages among the existing (and surveyed) mutation testing tools. A possible avenue for future work is to see which of the *missing* mutation operators can be implemented for the programming languages lacking these operators.

**RQ2.2.3: Which approaches are used to overcome the equivalent mutant problem when applying mutation testing?**

**Observations.**

In Table 2.13, we summarised our findings of how the studies that we surveyed deal with the equivalent mutant problem. More specifically, Table 2.13 presents how many times we encountered each of the approaches for solving the equivalent mutant problem. When looking at the results, we first observe that in 56.5% of the cases we assigned “n/a”, such as Androutsopoulos et al.[52] and Flores and Polo[142].

As shown in Table 2.13, there are only 17 instances actually adopting equivalent mutant detectors by using automatic mechanisms. Specifically, 6 instances use “model checker” (e.g., Gay et al. [156]); 8 instances use “reduce likelihood” (e.g., Milani et al. [251]); and 3 instances apply “deterministic model” (Belli et al.[76]). In the remaining papers, the problem of equivalent mutants is solved by: (1) manual analysis (e.g., Liu et al. [231] and Xie et al. [371]); (2) making assumptions (treating mutants not killed as either equivalent or non-equivalent, e.g., Fang et al.[136] and Rothermel et al. [307]); (3) no investigation (e.g., Offutt and Liu [273], Chen et al [97] and Fraser and Zeller [150]). The manual investigation (38 instances) and the method of treating mutants not killed as equivalent (17 instances) are more commonly used than other methods. We also compared our results with Madeyski et al. [241]’s survey on the equivalent mutant problem. In their review, they reviewed 17 methods for overcoming the equivalent mutant problem. Among these 17 techniques, we found that only the model-checker approach [129] was adopted.

We can only speculate as to the reasons behind the situation above: Firstly, most studies use mutation testing as an evaluation mechanism or guiding heuristic, rather than their main research topic. So, the authors might be not willing to spare too much effort in dealing with problems associated with mutation testing. Moreover, looking at the internal features of existing tools used in literature (in Table 2.14), we found that only five tools adopt techniques to address the equivalent mutant problem. Most of the tools did not assist in dealing with the equivalent mutant problem. Therefore, in this chapter, we consider the aforementioned three solutions: (1) manual analysis, (2) making assumptions, or (3) no investigation. If there exists a well-developed auxiliary tool that can

---

2 The studies that are categorised as “yes” in the tool availability, “existing tool” in the tool type and “well-defined” in the mutation operator description level.
be seamlessly connected to the existing mutation systems for helping the authors detect equivalent mutants, this tool might be more than welcomed. We recommend that future research on the equivalent mutant problem can further implement their algorithms in such an auxiliary tool and make it open to the public (see the fifth recommendation labelled as R5 in Section 2.4.4).
Secondly, the mutation score is mainly used as a relative comparison for estimating the effectiveness of different techniques. Sometimes, mutation testing is only used to generate likely faults; equivalent mutants have no impact on the other measures such as the Average Percentage of Fault Detection rate (APFD) \([306]\). Furthermore, the definition of the mutation score is also modified by some authors (e.g., Rothermel et al.\([307]\)) : they used the total number of mutants as the denominator instead of the number of non-equivalent mutants. The equivalent mutant problem seems to not pose a significant threat to the validation of the testing techniques involved in these studies.

However, we should not underestimate the impact of the equivalent mutant problem on the accuracy of the mutation score. Previous empirical results indicated that 10 to 40 percent of mutants are equivalent \([270, 274]\). What’s more, Schuler and Zeller \([314]\) further claimed that around 45% of all undetected mutants turned out to be equivalent; this observation leads to the assumption that by simply treating mutants not killed as equivalent mutations, we could be overestimating the mutation score. Therefore, we recommend performing more large-scale investigations on whether the equivalent mutant problem has a strong impact on the accuracy of the mutation score.

**SUMMARY.**

The techniques for equivalent mutant detection are not commonly used when applying mutation testing. The main approaches that are used are the manual investigation and treating mutants not killed as equivalent. Based on the results, we recommend that further research on the equivalent mutant problem can develop a mature and useful auxiliary tool which can easily link to the existing mutation system. Such an extra tool assists people to solve the equivalent mutant problem when applying mutation testing more efficiently. Moreover, research on whether the equivalent mutant problem has a high impact on the accuracy of the mutation score is still needed, as the majority did not consider the equivalent mutant problem as a significant threat to the validation of the quality assurance processes. Also, 56.5% of the studies are lacking an explanation as to how they are dealing with overcoming the equivalent mutant problem; this again calls for more attention on reporting mutation testing appropriately.

**RQ2.2.4: Which techniques are used to reduce the computational cost when applying mutation testing?**

**Observations.**

Since mutation testing requires high computational demands, cost reduction is necessary for applying mutation testing, especially in an industrial environment. We summarized the use of such computational cost reduction techniques when using mutation testing in Table 2.15. Please note that we excluded the runtime optimisation and selective mutation techniques. We opted to exclude this because the runtime optimisation is related to tool implementation, which is not very likely to appear in the papers under our research scope, while the second one, selective mutation, is adopted by all the papers.

First of all, we noticed that 131 articles (68.6%) did not mention any reduction techniques, e.g., Außerlechner et al.\([61]\) and Baker and Habli\([62]\). If we take into account those papers that used the runtime optimisation and selective mutation, one plausible explanation for the numerous “n/a” instances is a lack of awareness of properly reporting mutation testing, as we mentioned earlier. Secondly, random selection of the mu-
Table 2.15: Summary of cost reduction

<table>
<thead>
<tr>
<th>Cost Reduction Technique</th>
<th>Number of papers</th>
</tr>
</thead>
<tbody>
<tr>
<td>n/a</td>
<td>131</td>
</tr>
<tr>
<td>fixed number</td>
<td>28</td>
</tr>
<tr>
<td>weak mutation</td>
<td>15</td>
</tr>
<tr>
<td>mutant sample</td>
<td>11</td>
</tr>
<tr>
<td>selection strategy</td>
<td>8</td>
</tr>
<tr>
<td>higher-order</td>
<td>1</td>
</tr>
</tbody>
</table>

Tants based on a fixed number comes next (28 instances, e.g., Namin and Andrews [262] and Staats et al. [327]), followed by weak mutation (15 instances, e.g., Hennessy and Power [176] and Vivanti et al. [353]) and mutant sampling (11 cases, e.g., Arcuri and Briand [54] and Stephan and Cordy [331]). However, why is the technique of using a “fixed number” of mutants more popular than the others? We speculate that this could be because choosing a certain number of mutants is more realistic in real software development: the total number of mutants generated by mutation tools is enormous; while, realistically, only a few faults are made by the programmer during implementation. By fixing the number of mutants, it becomes easier to control the mutation testing process. Instead, relying on the weak mutation condition would require additional implementation efforts to modify the tools. It is also important to note that the difference between the “fixed number” and “mutant sample” choice: while the first one implies a fixed number of mutants, the second one relies on a fixed sampling rate. Compared to using a fixed number, mutant sampling sometimes cannot achieve the goal of reducing the number of mutants efficiently. In particular, it is hard to set one sample ratio if the size of the subjects varies greatly. For example, consider the following situation: one subject has 100,000 mutants while the other has 100 mutants. When the sample ratio is set to 1%, the first subject still has 1000 mutants left, while the number of mutants for the second one is reduced to one.

We performed a further analysis of the mutation tools in Table 2.14. We find that most tools adopted some types of cost reduction techniques to overcome the high computational expense problem. For mutation testing tools for Java, bytecode translation is frequently adopted while Mutant Schemata Generation (MSG) is used in two tools, MuJava and JAVAFLANCHE. Another thing to highlight is that MiLu used a special test harness to reduce runtime [196]. This test harness is created containing all the test cases and settings for running each mutant. Therefore, only the test harness needs to be executed while each mutant runs as an internal function call during the testing process.

Selective mutation is also widely applied in almost all the existing mutation testing tools (as shown in Table 2.12). This brings us to another issue: *is the selected subset of mutation operators sufficient to represent the whole mutation operator set?* When adopting selective mutation, some configurations are based on prior empirical evidence, e.g., Offutt et al.’s five sufficient Fortran mutation operators [271], and Siami et al.’s 28 sufficient C mutation operators [322]. However, most of the articles are not supported by empirical or theoretical studies that show a certain subset of mutation operators can
represent the whole mutation operator set. As far as we know, most studies on selective mutation are merely based on Fortran \([258, 271, 367]\) and C \([65, 220, 261, 322]\) programs. Thereby, we recommend more empirical studies on selective mutation in programming languages other than Fortran.

Compared to Jia and Harman’s literature review \([197]\), most of the cost reduction techniques they surveyed have been adopted in our collection. Runtime optimisation techniques which they summarised, e.g., interpreter-based technique \([210]\), compiler-based approach \([113]\) and bytecode translation \([239]\) have been widely adopted in existing mutation testing tools. However, the articles we have reviewed did not apply Firm Mutation \([192]\) and advanced platforms support for mutation testing, such as SIMD \([215]\) and MIMD machines \([276]\). For Firm Mutation, there is no publicly available tool to support this method; thus, other researchers cannot adopt this approach conveniently. As for advanced platforms, these machines are not easy for other researchers in the mutation testing field to obtain. One exception is the cost reduction technique with a *fixed number*, which was not covered by Jia and Harman \([197]\). As mentioned earlier, the fixed-number-of-mutants technique is different from mutant sampling as the former selects a subset of mutants based on a fixed number rather than a ratio. We speculated the reason why Jia and Harm \([197]\) did not include this method is that reduction based on a fixed number is too simple to be considered as a real technique for cost reduction in mutation testing. However, such a technique is surprisingly popular among the applications of mutation testing.

**SUMMARY.**

Based on the above discussion, we infer that the problem of the high computational cost of mutation testing can be adequately controlled using the state-of-art reduction techniques, especially selective mutation and runtime optimisation. Selective mutation is the most widely used method for reducing the high computational cost of mutation testing. However, in most cases, there are no existing studies to support the prerequisite that selecting a particular subset of mutation operators is sufficient to represent the whole mutation operator set for other programming languages instead of C and Fortran. Therefore, one recommendation is to conduct more empirical studies on selective mutation in various programming languages. Random selection of the mutants based on a fixed number (28 papers) is the most popular technique used to reduce the computational cost. The other popular techniques are weak mutation and mutant sampling. Besides, a high percentage of the papers (68.6%) did not report any reduction techniques used to cope with computational cost when applying mutation testing; this again should serve as a reminder for the research community to pay more attention to *properly* reporting mutation testing in testing experiments.

**RQ2.2.5: WHAT SUBJECTS ARE BEING USED IN THE EXPERIMENTS (REGARDING PROGRAMMING LANGUAGE, SIZE, AND DATA AVAILABILITY)?**

**Observations.**

To analyse the most common subjects used in the experiments, we focus on three attributes of the subject programs, i.e., programming language, size and data availability. We will discuss these three attributes one by one in the following paragraphs.
Table 2.16 shows the distribution of the programming languages. We can see that Java and C dominate the application domain (66.0%, 126 instances). While JavaScript is an extensively used language in the web application domain, we only found three research studies in our datasets that applied mutation testing for this programming language. The potential reasons for this uneven distribution are unbalanced data availability and the complex nature of building a mutation testing system. The first cause, uneven data availability, is likely instigated by the fact that existing, well-defined software repositories such as SIR [126], SF100 [146] are based on C and Java. We have not encountered such repositories for JavaScript, C# or SQL. Furthermore, it is easier to design a mutation system targeting one programming language; this stands in contrast to many web applications, which are often composed out of a combination of JavaScript, HTML, CSS, etc; thus, this increases the difficulty of developing a mutation system for these combinations of programming languages. It is also worth noticing that we have not found any research on a purely functional programming language in our research scope.

When considering the size of the subject programs, in addition to our collection, we also summarise the data presented in Jia and Harman's survey [197] in Table 2.17. In Jia and Harman [197]'s survey, they summarised all the programs used in empirical studies related to mutation testing including the program size and the total number of uses. In Table 2.17, to summarise the data from Jia and Harman, we first categorise the programs into five classes (as shown in the first column) according to their size in LOC, and then add up the total number of usages (as shown in the third column). It is important to note that the program data in Jia and Harman's survey [197] is different from ours: they collected the programs from empirical studies which aimed to evaluate the effectiveness of mutation testing, e.g., Mathur and Wong compared data flow criteria with mutation testing [244]. These studies are not part of our research scope: we focus on the application perspective while these works target the development of mutation testing approaches. The purpose of the comparison of Jia and Harman's data is to investigate the difference between two perspectives of mutation testing, i.e., the development and the application perspective. Moreover, they listed all the possible programs used in empirical studies while we only collected the maximum size of the programs.

As for our collection, studies involving preliminary (<100 LOC), small (100–10K LOC) subjects or studies with no information about programs size (“n/a” instances in Table 2.17) represent 80.6%(154 instances) of papers in our collection. Among these “n/a” cases, some papers (e.g., Xie et al. [371]) did not provide any information about the subject size (LOC), and a few cases (e.g., Baudry et al [67]) report outdated links. This high percentage of preliminary, small and “n/a” subjects indicates that mutation testing is rarely applied to programs whose size is larger than 10K LOC. We did find that only 35 studies use medium size subjects, which corresponds to 29.9%3 of papers. Compared to Jia and Harman's data [197], preliminary programs account for 63.4%4 of the study set, which is much higher than in our study. There are two possible causes for this finding. The one is that we only consider the maximum size of the programs in each study, we could subtract many potential cases that used preliminary programs from our results. The other is that a considerable number of the empirical studies on mutation testing that Jia and Harman reviewed date back to the 1990s. These early-stage research works

\[ \text{Notice that we did not consider the number of "n/a" value when calculating the percentage.} \]
Table 2.16: Summary of programming languages

<table>
<thead>
<tr>
<th>Programming language</th>
<th>Number of papers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Java</td>
<td>92</td>
</tr>
<tr>
<td>C</td>
<td>34</td>
</tr>
<tr>
<td>Lustre/Simulink</td>
<td>8</td>
</tr>
<tr>
<td>C#</td>
<td>6</td>
</tr>
<tr>
<td>Fortran</td>
<td>6</td>
</tr>
<tr>
<td>n/a</td>
<td>6</td>
</tr>
<tr>
<td>C++</td>
<td>5</td>
</tr>
<tr>
<td>SQL</td>
<td>5</td>
</tr>
<tr>
<td>Eiffel</td>
<td>3</td>
</tr>
<tr>
<td>Spreadsheet</td>
<td>3</td>
</tr>
<tr>
<td>AspectJ</td>
<td>3</td>
</tr>
<tr>
<td>JavaScript</td>
<td>3</td>
</tr>
<tr>
<td>Enterprise JavaBeans application</td>
<td>2</td>
</tr>
<tr>
<td>C/C++</td>
<td>2</td>
</tr>
<tr>
<td>Ada</td>
<td>1</td>
</tr>
<tr>
<td>Kermeta</td>
<td>1</td>
</tr>
<tr>
<td>Delphi</td>
<td>1</td>
</tr>
<tr>
<td>ISO C++ grammar</td>
<td>1</td>
</tr>
<tr>
<td>PLC</td>
<td>1</td>
</tr>
<tr>
<td>Sulu</td>
<td>1</td>
</tr>
<tr>
<td>XACML</td>
<td>1</td>
</tr>
<tr>
<td>XML</td>
<td>1</td>
</tr>
<tr>
<td>HLPSL</td>
<td>1</td>
</tr>
<tr>
<td>PHP</td>
<td>1</td>
</tr>
<tr>
<td>other specification languages</td>
<td>10</td>
</tr>
</tbody>
</table>

on mutation testing mainly involving preliminary subjects. Also, we witness an increasing trend of medium and large size subject systems being used in studies on mutation testing; this shows the full potential of mutation testing in large-scale applications.

With regard to data availability, we observe the following: 49.7% of the studies provide open access to their experiments. Some studies, such as Staats et al.[328], used close-sourced programs from industry. There are also a few cases for which the source links provided by the authors are not accessible anymore, e.g., Jolly et al.[199]. We also found that several cases used open-source software corpora, such as SF110, but they only used a sample of the corpus (e.g., Rojas et al. [305]) without providing sample information. The others did not provide information about sources in their paper, e.g., Kanewala and Bieman[206].

Together with 6 instances of “n/a” in Table 2.16 and 74 in Table 2.17 (including subjects which cannot be measured as LOC, e.g., spreadsheet applications), it is worth noticing that subject programs used in the experiment should be clearly specified. Also, basic

4Similarly, we removed the cases of “n/a” here when calculating the percentage. (402 – 28 = 374).
Table 2.17: Summary of subject size

<table>
<thead>
<tr>
<th>Subject Size</th>
<th>No. of papers in our collection</th>
<th>No. of programs in Jia and Harman [197]</th>
</tr>
</thead>
<tbody>
<tr>
<td>n/a</td>
<td>74</td>
<td>28</td>
</tr>
<tr>
<td>small (100~10K LOC)</td>
<td>70</td>
<td>128</td>
</tr>
<tr>
<td>medium (10K~1M LOC)</td>
<td>35</td>
<td>9</td>
</tr>
<tr>
<td>preliminary (&lt;100 LOC)</td>
<td>10</td>
<td>237</td>
</tr>
<tr>
<td>large (&gt;1M LOC)</td>
<td>2</td>
<td>0</td>
</tr>
</tbody>
</table>

Note: The results of our collection are based on the maximum size of the programs used in each study while Jia and Harman’s is based on all the programs.

Table 2.18: Summary of data availability

<table>
<thead>
<tr>
<th>Data Availability</th>
<th>Number of papers</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>96</td>
</tr>
<tr>
<td>yes</td>
<td>95</td>
</tr>
</tbody>
</table>

information on the programming language, size and subject should also be clearly specified in the articles to ensure replicability.

**SUMMARY.**

For the subjects used in the experiments in our survey, we discussed three aspects: programming language, size of subject projects and data availability. For programming languages, Java and C are the most common programming languages used in the experiments when applying mutation testing. There is a clear challenge in creating more mutation testing tools for other programming languages, especially in the area of web applications and functional programming (see the recommendation labelled as R7 in Section 2.4.4).

As for the maximum size of subject programs, small to medium scale projects (100~1M) are widely used when applying mutation testing. Together with two large-scale cases, we can see the full potential of mutation testing as a practical testing tool for large industrial systems. We recommend more research on large-scale systems to further explore scalability issues (see the recommendation labelled as R8 in Section 2.4.4).

The third aspect we consider is data availability. Only 49.7% of the studies that we surveyed provide access to the subjects used; this again calls for more attention on reporting test experiments appropriately: the authors should explicitly specify the subject programs used in the experiment, covering at least the details of programming language, size, and source.

### 2.4.3. SUMMARY OF RESEARCH QUESTIONS

We now revisit the research questions and answer them in the light of our observations.
RQ2.1: How is mutation testing used in quality assurance processes?
Mutation testing is mainly used as a fault-based evaluation method (70.2%) in different quality assurance processes. It assesses the fault detection capability of various testing techniques through the mutation score or the number of killed mutants. Adopting mutation testing to improve other quality assurance processes as a guide was first proposed by DeMillo and Offutt [116] in 1991 when they used it to generate test data. As a “high end” test criterion, mutation testing started to gain popularity as a building block in different quality assurance processes, like test data generation (36 instances), test case prioritisation (6 cases) and test strategy evaluation (6 instances). However, using mutation testing as part of new test approaches raises a challenge in itself, namely how to efficiently evaluate mutation-based testing? Besides, we found one limitation related to the “guide” role of mutation testing: mutation testing usually serves as a where-to-check constraint rather than a what-to-check improvement. Another finding of the application of mutation testing is that it often targets unit-level testing (72.0%), with only a small number of studies featuring higher-level testing showing the overall benefit of mutation testing. As a result, we conclude that the current state of the application of mutation testing is still rather limited.

RQ2.2: How are empirical studies related to mutation testing designed and reported?
First of all, for the mutation testing tools and mutation operators used in literature, we found that 47.6% of the articles adopted existing (open-access) mutation testing tools, such as MuJava for Java and Proteum for C. In contrast, we did encounter a few cases (27 in total) where the authors implemented their own tools or seeded mutants by hand. Furthermore, to investigate the distribution of mutation operators in the studies, we created a generalised classification of mutation operators as shown in Listing 1. The results indicate that certain programming languages lack specific mutation operators, at least as far as the mutation tools that we have surveyed concern.

Moreover, when looking at the two most significant problems related to mutation testing, the main approaches to dealing with the equivalent mutant problem are (1) treating mutants not killed as equivalent and (2) not investigating the equivalent mutants at all. In terms of cost reduction techniques, we observed that the “fixed number of mutants” is the most popular technique, although we should mention that we did not focus on built-in reduction techniques.

The findings above suggest that the existing techniques designed to support the application of mutation testing are largely still under development: a mutation testing tool with a more complete set of mutation operators or a flexible mutation generation engine to which mutation operators can be added, is still needed [211, 279]. In the same vein, a more mature and efficient auxiliary tool for assisting in overcoming the equivalent mutant problem is needed. Furthermore, we have observed that we lack insight into the impact of the selective mutation on mutation testing; this suggests that a deeper understanding of mutation testing is required. For example, if we know what particular kinds of faults mutation is good at finding or how useful a certain type of mutant is when testing real software, we can then design the mutation operators accordingly, such as Just et al. [201].
Table 2.19: Summary of poorly-specified aspects in empirical studies

<table>
<thead>
<tr>
<th>The poorly-specified aspects in reporting mutation testing</th>
<th>Number of papers</th>
</tr>
</thead>
<tbody>
<tr>
<td>test level (see Section 2.4.1)</td>
<td>84</td>
</tr>
<tr>
<td>mutation tool source (see Section 2.4.2)</td>
<td>92</td>
</tr>
<tr>
<td>mutation operators (see Section 2.4.2)</td>
<td>72</td>
</tr>
<tr>
<td>equivalent mutant problem (see Section 2.4.2)</td>
<td>108</td>
</tr>
<tr>
<td>reduction problem (see Section 2.4.2)</td>
<td>131</td>
</tr>
<tr>
<td>subject program source (see Section 2.4.2)</td>
<td>96</td>
</tr>
</tbody>
</table>

Based on the distribution of subject programs used in testing experiments or case studies, Java and C are the most common programming languages used in the experiments. Also, small to medium scale projects (100~1M LOC) are the most common subjects employed in the literature.

From the statistics of the collection, we found that a considerable amount of papers did not provide a sufficiently clear or thorough specification when reporting mutation testing in their empirical studies. We summarised the poorly-specified aspects of mutation testing in Table 2.19. As a result, we call for more attention on reporting mutation testing appropriately. The authors should provide at least the following details in the articles: the mutation tool (preferably with a link to its source code), mutation operators used in experiments, how to deal with the equivalent mutant problem, how to cope with high computational cost and details of the subject program (see the ninth recommendation labelled as R9 in Section 2.4.4).

2.4.4. Recommendation for Future Research

In this section, we will summarise the recommendations for future research based on the insights obtained for the two main research questions (see Sections 2.4.1 through 2.4.3). We propose nine recommendations for future research:

- **R1: Mutation testing cannot only be used as where-to-check constraints but also to suggest what to check to improve test code quality.**

  As shown in Table 2.4 in Section 2.4.1, when mutation testing serves as a “guide”, mutants generated by the mutation testing system are mainly used to suggest the location to be checked, i.e., where-to-check constraints. For example, the location of mutants is used to assist the localisation of “unknown” faults in fault localisation. The mutation-based test data generation also used the position information to generate killable mutant conditions. However, mutation testing is not widely considered to be a benefit to improve test code quality by suggesting what to check, especially in the test oracle problem. The what-to-check direction can be one opportunity for future research in mutation testing as a ”guide” role.

- **R2: For testing approaches that are guided by a mutation approach, more focus can be given to finding an appropriate way to evaluate mutation-based testing in an efficient manner.**
When looking at the evaluation types in Table 2.5 in Section 2.4.1, we observe that 75.4% of the mutation-based testing techniques still adopt mutation faults to assess their effectiveness. This raises the question of whether the conclusions might be biased. As such, we open the issue of finding an appropriate way to evaluate mutation-based testing efficiently.

• **R3: Study the higher-level application of mutation testing.**

In Section 2.4.1 we observed that mutation testing seems to mainly target unit-level testing, accounting for 72.0% of the studies we surveyed. This reveals a potential gap in how mutation testing is currently applied. It is thus our recommendation that researchers pay more attention to higher-level testing, such as integration testing and system testing. The research community should not only investigate potential differences in applying mutation testing at the unit-level or at a higher level of testing but should also explore whether the conclusions based on unit-level mutation testing still apply to higher-level mutation testing. A pertinent question in this area could be, for example, whether an integration mutation fault can be considered as an alternative to a real bug at the integration level.

• **R4: The design of a more flexible mutation generation engine that allows for the easy addition of new mutation operators.**

As shown in Table 2.8 in Section 2.4.1, 50.3% of the articles adopted the existing tools which are open-source, while we also found 27 instances of researchers implementing their own tool or seeding the mutants by hand. Furthermore, in Table 5.1 and Table 2.12, we can see certain existing mutation testing tools lack certain mutation operators. These findings imply that existing mutation testing tools cannot always satisfy all kinds of needs, and new types of mutation operators are also potentially needed. Since most existing mutation testing tools have been initialized for one particular language and a specific set of mutation operators, we see a clear need for a more flexible mutation generation engine to which new mutation operators can be easily added [279].

• **R5: A mature and efficient auxiliary tool to detect equivalent mutants that can be easily integrated with existing mutation tools.**

In Section 2.4.2, the problem of equivalent mutants is mainly solved by manual analysis, assumptions (treating mutants not killed as either equivalent or non-equivalent) or no investigation at all during application. This observation leads to doubt about the efficacy of the state-of-art equivalent mutant detection. In the meanwhile, if there is a mature and efficient auxiliary tool which can easily link to the existing mutation system, the auxiliary tool can be a practical solution for the equivalent mutant problem when applying mutation testing. As a result, we call for a well-developed and easy to integrate an auxiliary tool for the equivalent mutant problem.

• **R6: More empirical studies on the selective mutation method can pay attention to programming languages other than Fortran and C.**
As mentioned in Section 2.4.2, selective mutation is used by all the studies in our research scope. However, the selection of a subset of mutation operators in most papers is not well supported by existing empirical studies, except for Fortran [258, 271, 367] and C [65, 220, 261, 322]. Selective mutation requires more empirical studies to explore whether a certain subset of mutation operators can be applied in different programming languages.

- **R7: More attention should be given to other programming languages, especially web applications and functional programming projects.**

  As discussed in RQ2.5 in Section 2.4.2, Java and C are the most common programming languages that we surveyed. While JavaScript and functional programming languages are scarce. JavaScript, as one of the most popular languages for developing web applications, calls for more attention from researchers. In the meanwhile, functional programming languages, such as Lisp and Haskell, are still playing an inevitable role in the implementation of programs; they thus deserve more focus in future studies.

- **R8: Application of mutation testing in large-scale systems to explore scalability issues.**

  From Table 2.17 in Section 2.4.2, we learn that the application of mutation testing to large-scale programs whose size is greater than 1M LOC rarely happens (only two cases). To effectively apply mutation testing in industry, the scalability issue of mutation testing requires more attention. We recommend future research to use mutation testing in more large-scale systems to explore scalability issues.

- **R9: Authors should provide at least the following details in the articles: mutation tool source, mutation operators used in experiments, how to deal with the equivalent mutant problem, how to cope with high computational cost and subject program source.**

  From Table 2.19 in Section 2.4.4, we remember that a considerable amount of papers inadequately reported on mutation testing. To help progress research in the area more quickly and to allow for replication studies, we all need to take care to be careful in how we report mutation testing in empirical research. We consider the above five elements to be essential when reporting mutation testing.

### 2.5. Threats to the Validity of This Review

We have presented our methodology for performing this systematic literature review and its findings in the previous sections. As conducting a literature review largely relies on manual work, there is the concern that different researchers might end up with slightly different results and conclusions. To eliminate this potential risk caused by researcher bias as much as possible, we follow the guidelines for performing systematic literature reviews by Kitchenman [212], Wohlin [365], and Brereton et al. [85]) whenever possible. In particular, we keep a detailed record of procedures made throughout the review process by documenting all the metadata from article selection to characterisation (see [23]).
In this section, we describe the main threats to the validity of this review and discuss how we attempted to mitigate the risks regarding four aspects: the article selection, the attribute framework, the article characterisation and the result interpretation.

### 2.5.1. Article Selection

Mutation testing is an active research field, and a plethora of realisations have been achieved as shown in Jia and Harman’s thorough survey [197]. To address the main interest of our review, i.e., the actual application of mutation testing, we need to define inclusion/exclusion criteria to include papers of interest and exclude irrelevant ones. But this also introduces a potential threat to the validity of our study: unclear article selection criteria. To minimise the ambiguity caused by the selection strategies, we carried out a pilot run of the study selection process to validate our selection criteria among the three authors. This selection criteria validation led to a tiny revision. Besides, if there is any doubt about whether a paper belongs in our selected set, we had an internal discussion to see whether the paper should be included or not.

The venues listed in Table 2.2 were selected because we considered them to be the key venues in software engineering and most relevant to software testing, debugging, software quality and validation. This presumption might result in an incomplete paper collection. In order to mitigate this threat, we also adopted snowballing to extend our set of papers from pre-selected venues to reduce the possibility of missing papers. Moreover, we also ran two sanity checks (as mentioned in Section 2.3.2) to examine the completeness of our study collection, and recorded the dataset in each step for further validation.

Although we made efforts to minimise the risks with regard to article selection, we cannot make definitive claims about the completeness of this review. We have one major limitation related to the article selection: we only considered top conference or journal papers to ensure the high quality while we excluded article summaries, interviews, reviews, workshops (except the International Workshop on Mutation Analysis), panels and poster sessions. Vice versa, sometimes we were also confronted with a vague use of the “mutation testing” terminology, in particular, some papers used the term “mutation testing”, while they are doing fault seeding, e.g., Lyu et al. [235]. The main difference between mutation testing and error seeding is the way how to introduce defects in the program [22]: mutation testing follows certain rules while error seeding adds the faults directly without any particular techniques.

### 2.5.2. Attribute Framework

We consider the attribute framework to be the most subjective step in our approach: the generalisation of the attribute framework could be influenced by the researcher’s experience as well as the reading sequence of the papers. To generate a useful and reasonable attribute framework, we followed a two-step approach: (1) we first wrote down the facets of interest according to our research questions and then (2) derived corresponding attributes of interest. Moreover, for each attribute, we need to ensure all possible values of each attribute are available, as well as a precise definition of each value. In this manner, we can target and modify the unclear points in our framework quickly. In particular, we conducted a pilot run for specifically validating our attribute framework. The results led
2.6. **Conclusion**

In this chapter, we have reported on a systematic literature review on the application perspective of mutation testing, clearly contrasting previous literature reviews that surveyed the main development of mutation testing, and that did not specifically go into how mutation testing is applied (e.g., [197, 241, 279]). We have characterised the studies that we have found on the basis of seven facets: (1) the role that mutation testing has in quality assurance processes; (2) the quality assurance processes (including categories, test level and testing strategies); (3) the mutation tools used in the experiments; (4) the mutation operators used in the experiments; (5) the description of the equivalent mutant problem; (6) the description of cost reduction techniques for mutation testing; and (7) the subject software systems involved in the experiments (in terms of programming language, size and data availability). These seven facets pertain to our two main research questions: **RQ1** How is mutation testing used in quality assurance processes? and **RQ2** How are empirical studies related to mutation testing designed and reported?

Figure 2.1 shows our main procedures to conduct this systematic literature review. To collect all the relevant papers under our research scope, we started with search queries in online libraries considering 17 venues. We selected the literature that focuses on the supporting role of mutation testing in quality assurance processes with sufficient evidence to suggest that mutation testing is used. After that, we performed a snowballing procedure to collect missing articles, thus resulting in a final selection of 191 papers from 22 venues. Through a detailed reading of this research body, we derived an attribute framework that was consequently used to characterise the studies in a structured manner. The resulting systematic literature review can be of benefit for researchers in the area of mutation testing. Specifically, we provide (1) guidelines on how to apply and subsequently report on mutation testing in testing experiments and (2) recommendations for future
The derived attribute framework is shown in Table 2.3. This attribute framework generalises and details the essential elements related to the actual application of mutation testing, such as in which circumstances mutation testing is used and which mutation testing tool is selected. In particular, a generic classification of mutation operators is constructed to study and compare the mutation operators used in the experiments described. This attribute framework can be used as a reference for researchers when describing mutation operators. We then presented the characterisation data of all the surveyed papers in our GitHub repository [23]. Based on our analysis of the results (in Section 2.4), four points are key to remember:

1. Most studies use mutation testing as an assessment tool; they target the unit level. Not only should we pay more attention to higher-level and specification mutation, but we should also study how mutation testing can be employed to improve the test code quality. Furthermore, we also encourage researchers to investigate and explore more interesting applications for mutation testing in the future by asking such questions as: what else can we mutate? (Sections 2.4.1—2.4.1)

2. Many of the supporting techniques for making mutation testing truly applicable are still under-developed. Also, existing mutation tools are not complete with regard to the mutation operators they offer. The two key problems, namely the equivalent mutant detection problem and the high computation cost of mutation testing issues, are not well-solved in the context of our research body (Sections 2.4.2—2.4.2).

3. A deeper understanding of mutation testing is required, such as what particular kinds of faults mutation testing is good at finding. This would help the community to develop new mutation operators as well as overcome some of the inherent challenges (Section 2.4.3).

4. The awareness of appropriately reporting mutation testing in testing experiments should be raised among the researchers (Section 2.4.3).

In summary, the work described in this chapter makes following contributions:

1. A systematic literature review of 191 studies that apply mutation testing in scientific experiments, which includes an in-depth analysis of how mutation testing is applied and reported on.

2. A detailed attribute framework that generalises and details the essential elements related to the actual use of mutation testing.

3. A generic classification of mutation operators that can be used to compare different mutation testing tools.

4. An actual characterisation of all the selected papers based on the attribute framework.

5. A series of recommendations for future work including valuable suggestions on how to report mutation testing in testing experiments in an appropriate manner.
Mutation testing is widely considered as a high-end test coverage criterion due to the vast number of mutants it generates. Although many efforts have been made to reduce the computational cost of mutation testing, in practice, the scalability issue remains. In this chapter, we explore whether we can use compression techniques to improve the efficiency of strong mutation based on weak mutation information. Our investigation is centred around six mutation compression strategies that we have devised. More specifically, we adopt overlapped grouping and Formal Concept Analysis (FCA) to cluster mutants and test cases based on the reachability (code coverage) and necessity (weak mutation) conditions. Moreover, we leverage mutation knowledge (mutation locations and mutation operator types) during compression. To evaluate our method, we conducted a study on 20 open source Java projects using manually written tests. We also compare our method with pure random sampling and weak mutation. The overall results show that mutant compression techniques are a better choice than random sampling and weak mutation in practice: they can effectively speed up strong mutation 6.3 to 94.3 times with an accuracy of >90%.

This chapter has been published in the Proceedings of the 12th International Workshop on Mutation Analysis (Mutation 2017) [391] (2017 IEEE International Conference on Software Testing, Verification and Validation Workshops) and Proceedings of the 11th International Conference on Software Testing, Verification, and Validation (ICST) [392].
3.1. Introduction

Mutation testing has been actively investigated as a technique to evaluate the quality of test suites [197]. The main idea is (i) to introduce small syntactic changes (mutants) into the production code using mutation operators, and (ii) to measure the ability of a given test suite in detecting them [279]. One of the benefits reported in literature is that mutation testing provides a better measure of the fault detection capability of test suites compared to other test coverage criteria [144, 228, 244]. Despite its well-known advantages, mutation testing remains an extremely expensive activity since it requires to re-run the test suites against each mutant, whose number increases exponentially with the size of the program under test [93].

To address this limitation, several methods have been proposed and these can be classified in three main categories [277]: (do fewer) selecting fewer mutants to evaluate [41, 271], (do smarter) using run-time information to avoid unnecessary test executions [185, 200], (do faster) reducing the execution time for each single mutant [344]. Techniques falling into the first category are the most investigated. Indeed, researchers have proposed various strategies to sample mutants, such as random sampling [195], mutation operator selection [271], clustering [188], static analysis [218], and machine learning based sampling [333].

Recently, Gopinath et al. [160] have challenged the effectiveness and efficiency of mutation reduction strategies: their empirical evaluation with eight common mutant reduction techniques showed that none of them provide any practical advantage over pure random sampling. Although some techniques showed small improvements in effectiveness, the gains do not compensate for the extra overhead. Therefore, there is a need for reduction techniques that are not only more effective, but also more efficient compared to random sampling.

This chapter originates from the insights of Gopinath et al. [160] and focuses on the mutant reduction technique recently proposed by our preliminary work [391]. We originally tackle the problem of reducing the cost of mutation testing by combining do fewer and do smarter techniques through data compression methods. First, weak mutation (do smarter) is used to determine which mutants lead to an infection state through one single execution of the test suite against the original program. Then, formal concept analysis [364] (FCA) is applied to derive the maximal groupings [391], which are two-way clusters of mutants and tests. Each maximal grouping is composed of a set of mutants $M$ and a set of tests $T$ with the property that any mutant in $M$ is weakly killed by any test in $T$. Finally, a do fewer strategy is applied by running one single test case (test selection) against one single mutant (mutant sampling) from each maximal grouping [391].

Our initial empirical study with five Java programs and automatically generated unit test suites showed that FCA reduces the execution time of mutation testing by up to 85%.

In this chapter, we spot two important limitations of FCA that can affect its ability to correctly estimate strong mutation. First, FCA groups mutants and tests according to weak mutation only: mutants leading to an infection state when running the same test case $t$ (or set of tests) are assumed to be redundant. This is why only one mutant in each maximal grouping is evaluated for strong mutation. However, mutants that are redundant in terms of weak mutation are not necessarily redundant in terms of strong mutation, because, for example, they are injected in different code locations (e.g., different
methods) or are generated by different mutation operators. Second, we previously [391] focused only on maximal groupings, which may leave some tests and/or some mutants not assigned to any maximal grouping. As consequence, the estimated mutation score may be inaccurate.

To overcome these limitations, we enhance FCA with (i) mutant location and (ii) mutation operator type information when grouping mutants and tests according to weak mutation. This prevents mutants infecting different statements or generated by different operators to be inserted in the same grouping. We also investigate maximal and non-maximal groupings to prevent final clusters from missing test cases and/or mutants.

To evaluate the benefits of our enhancements, we conducted an empirical study with 20 open-source Java projects and using the test suites manually written by the original developers. Then, we compare the different variants of the FCA-based technique with and without our enhancements and against weak mutation and pure random sampling (with 10% as sampling percentage).

Our results show that FCA with our enhancements is more accurate in estimating the (strong) mutation score compared to (i) the original FCA-based technique by our preliminary work [391], (ii) random sampling, and (iii) weak mutation. In particular, we find that the compression strategy based on non-maximal groupings and enriched with mutant location information (referred as overlap+mloc in the remainder of the chapter) estimates the strong mutation score with an average absolute error of 5% and an average accuracy of 93% while being five time faster than strong mutation, i.e., its average speed up is 5X. Instead, random sampling achieves a higher absolute error of 13% while requiring the same execution time of overlap+mloc, i.e., its average speed up is 5X as well. The other compression strategies lead to larger speed-up scores (up to 18X) but with the cost of having a larger absolute error, which ranges between 5% (i.e., the absolute error of overlap+mloc) and 13% (i.e., the absolute error of random sampling) on average. Therefore, our findings challenge prior results [160] as we find that mutation strategies based on compression methods (and FCA in particular) are more effective and/or more efficient than random sampling. Finally, weak mutation is the fastest technique but it also produces the largest absolute error of 23% on average.

As a final remark, we observe that all FCA-variants allow to estimate whether each individual mutant is strongly killed or not based on relatively few test executions by relying on the two-way clusters generated with FCA. Instead, random sampling does not take into account relationships between mutants and test cases, possibly also leading to underrepresented areas of production code in the estimation.

3.2. **Background and Related Work**

In this section, we begin with an overview of mutation reduction techniques in literature and the works that motivate our approach. Then, we introduce the crucial concepts and theories on which our approach is based.

3.2.1. **Mutation Reduction Strategies**

Techniques for reducing the high computational cost have been an active area of research. Offutt and Untch [277]’s literature review summarises these approaches into
three categories: do fewer, do smarter and do faster. The most well-known techniques for reducing the computational cost of mutation testing are random sampling [41], selective mutation [271], weak mutation [185] and mutant schema [345]. The aforementioned methods are independent of the program under test which can be flexibly combined with our methodology.

More recently, researchers have aimed to make further gains by including run-time information; a widely-adopted strategy is to execute the test suite on the original program before mutation execution to avoid unnecessary executions. Coverage-based optimisation filters out test executions when a test case does not cover the mutated statement; this optimisation is in use in existing tools such as JAVALANCHE [313], Major [204] and PIT/PITest [3]. Infection-based optimisation on the other hand only executes a test case on a mutant when the test infects the state of the mutant, filtering out weakly live mutants (whose execution states are different from the original code).

Just et al. [200] improved upon this by only executing a test on a mutant if the execution state of the mutated expression propagates to a top-level expression; they also partitioned mutants based on their intermediate results. Ma and Kim [236] applied a similar idea to cluster mutants for each test case by comparing the values of innermost expressions. Compared to Just et al. [200] and Ma and Kim [236]’s, we partition mutants for all test cases instead of targeting each test case.

Mutant clustering’s aim is to reduce the number of mutants based on the similarity of mutants instead of random sampling. Hussain [188] applied clustering algorithms (e.g. K-means), however, the approach requires the execution of all mutants against all the test cases, which cannot reduce the overhead during the mutation execution. Later, Ji et al. [195] measured the similarity of the mutants using domain analysis. They divide mutants based on static control flow analysis. But they only manually analysed the clustering accuracy without indicating the runtime overhead caused by the domain analysis. Different from these works, our approach groups mutants based on their reachability and necessity conditions against the tests.

An approach that eliminates redundant mutants is mutant subsumption (e.g. [46, 202, 219]). However, mutant subsumption requires full knowledge of the mutation kill matrix, which requires the execution of every mutant against every test. Computationally this process is more costly than traditional strong mutation, thus cannot be used to speed-up mutation execution. Furthermore, test prioritization and reduction are also used to speed up mutation testing, e.g. Zhang et al. [380].

Moreover, Zhang et al. have recently proposed Predictive Mutation Testing (PMT) to predict mutation testing results without execution [379]. They extracted 12 features from the programs and constructed a classification model to predict whether a mutant is killed or surviving. Their experiment showed that PMT could improve the efficiency of mutation testing by up to 151.4 times with a small loss in accuracy. Despite high efficiency, their approach needs to collect a series of program features, which requires different tools to fulfil; this is a substantial burden for the common programmer. Unlike Zhang et al. [379], we do not require any additional program features; the weak mutation information needed for our mutant clustering and data compression can be collected by our tool during the initial execution against the original program.

Our approach is an extension of our preliminary work [391]. Despite the encourag-
ing results, we have identified two important limitations of our initial methods as mentioned before (in Section 3.1), i.e., (1) weak mutation information is not enough; and (2) FCA could lead to missing mutants and/or tests. To address these limitations, we propose another compressing strategy, i.e., overlapped grouping, which is the simplest and strictest clustering method. Moreover, we take full advantage of mutation location and operator type knowledge when compressing.

3.2.2. Mutant Compression

We now describe the core concepts behind our approach: weak mutation and FCA-based compression technique [391].

**Weak Mutation.** For a test case \( t \) to kill a mutant \( m \) which mutates the statement \( s \) of a program \( P \), there are three conditions [278]: (i) reachability: the execution of \( t \) must cover \( s \); (ii) necessity: the execution state of \( m \) is different from the execution state of \( s \); (iii) sufficiency: the incorrect state of \( m \) must propagate to the output causing a failure in \( t \).

Weak mutation uses the necessity condition, i.e., a mutant is killed if its execution leads to a state change. For example, the expression \( c=a\times b \) and its mutated version \( c=a/b \) have different outcomes (i.e., the mutant is weakly killed) if \( a\neq 1, a\neq 0 \) and \( b\neq 1 \). Differently from strong mutation, weak mutation scores can be computed with one single execution of each test by instrumenting the mutated locations [149].

**FCA-based compression technique [391].** Formal Concept Analysis (FCA) was originally a data analysis method and has shown to be a powerful mathematical technique to convey and summarize large amounts of information [364]. It takes as input the formal context which is a structure \( C = (O, A, I) \) where \( O \) is the set of objects, \( A \) is the set of attributes while \( I \subseteq O \times A \) is a binary relation between \( O \) and \( A \). Then, FCA produces the concept lattice, which is a collection of formal concepts in the data ordered by sub-concept relations, i.e., from super-concepts to sub-concepts. Each formal concept is composed of (i) a group of objects sharing the same attributes, and (ii) all attributes that apply to the objects in the concept [364].

In mutation testing context, the objects in \( O \) are the mutants, the attributes in \( A \) are the test cases, and \( I \) is the mutant-by-test infection matrix. Then, FCA derives formal concepts that represent groups of mutants that are weakly killed by the same subset of tests. In other words, the output of FCA can be viewed as two-way clustering since mutants and tests are grouped in concepts such that all mutants in the same concept \( c \) are weakly killed by all tests in \( c \). Among these concepts, FCA-based compression technique only considers the maximal concepts that are directly connected to the exit point in the lattice hierarchy that are referred to as maximal groupings.

After obtaining the maximal groupings from the concept lattice, this approach first compresses the mutant-by-test infection matrix by condensing the rows, i.e., select one mutant from each maximal grouping. Then to further perform the compression on the columns, there are three approaches for test case selection: (i) random: randomly select one test from each maximal grouping; (ii) Set cover based: find a sufficient subset of test cases that weakly kill all possible mutants. i.e., at each stage, choose the test that weakly kills the largest number of uncovered maximal groupings; (iii) Sorting-based: select the test cases with the largest number of maximal groupings at each stage until all possible
Figure 3.1: Overall methodology of mutation compression strategies

mutants are covered.

However, as our preliminary study [391] show, applying test case selection on FCA groupings leads to a relatively small (5.89%) reduction in execution time. Therefore, in this chapter, we do not use test case selection. Instead, we apply dynamic coverage-based optimisation [3, 204, 313] and infection-based optimisation [200, 236] (see Sec. 3.2) to filter out unnecessary executions.

3.3. APPROACH

3.3.1. OVERALL METHODOLOGY

Our 6-step compression strategy is illustrated in Figure 3.1:

(1) Instrumentation. We instrument the original program to keep track of the mutation locations: at every mutation point we insert all the mutants (mutated codes) right after the original one and assign a unique id to each mutant for later activation (we applied the technique of the mutant schemata [344]). To perform weak mutation, we also insert the comparison instructions at each mutation point to compare the intermediate states of the original program and mutated part (we compare the state after the first execution of the innermost expression that surrounds the mutant). We insert additional instructions to record information of each mutant including its location, operator type and mutation details (e.g., $m_1$ on Line 12 applies replace constant operator: $0 \rightarrow 1$).

(2) Test execution. Once instrumented, the test suite is executed once on the original program. During this stage, we record the mutants that are touched by the tests, as well as the ones which are weakly killed by the tests. Only the instructions related to weak mutation and mutant information collection are executed at this stage. No mutants are activated.

(3) Reachability and necessity analysis. The results of the previous stage are stored in the mutant-by-test reachability and mutant-by-test necessity matrices. Let $P$ be the
program under analysis and let $T$ be the test suite; let $M$ be the set of mutants for the program $P$ generated by preselected mutation operators. A **mutant-by-test reachability** matrix is a $m \times n$ matrix where $m$ is the number of mutants, $n$ is the number of test cases in $T$, and an entry $x_{i,j}$ is a binary value indicating whether the statement containing the $i$-th mutant is executed ($x_{i,j} = 1$) or not ($x_{i,j} = 0$) by the $j$-th test $e \in T$. The **mutant-by-test necessity** matrix has the same size as the mutant-by-test reachability matrix, but the binary entry $x_{i,j}$ represents the outcome of weak mutation ($x_{i,j} = 1$ indicates weakly killed).

(4) **Mutant clustering.** Using the two aforementioned matrices, we apply clustering to group similar mutants together. We consider two clustering methods: (1) the overlapped grouping, and (2) FCA grouping from our preliminary study [391] (See Section 3.2.2).

(5) **Data compression.** The mutant clusters are then used to compress the mutant-by-test matrix. The resulting matrix is likely to have lower dimensionality: the rows denote groups of mutants belonging to the same clusters; similarly, tests are grouped into clusters to form the columns. The compressed matrix is then used to apply mutants and execute tests for the strong mutation analysis. We take mutation knowledge into consideration during compression to achieve higher accuracy.

(6) **Mutant Execution.** The compressed matrix from the previous step is then used for the strong mutation analysis. Here, we load each mutant by its id and run the actual mutation execution against the tests.

The details of overlapped grouping and how we use mutation knowledge are described in the next sub-sections.

### 3.3.2. **overlapped GROUPING**

As mentioned earlier, the FCA-based compression technique could result in missing mutants and/or tests. Therefore, we propose the overlapped grouping to overcome this. The overlapped method is the simplest and strictest clustering method, i.e., elements are only grouped together if they are identical. Specifically, we first identify distinct mutants with regard to their reachability and necessity conditions against all the test cases. Subsequently, we group mutants having the same reachability and necessity conditions into one cluster.

The main difference between overlapped and FCA grouping is that overlapped grouping is stricter than FCA grouping. The overlapped grouping does not lose any information in the matrix, i.e., the clustering contains all the mutants. While FCA grouping loses some information since the main idea of FCA is to find the maximal sub-matrixes (or formal concepts), and if a mutant or a test does not belong to a sub-matrix, FCA removes this mutant or test.

In our example in Figure 3.2, there are three maximal groupings, which are $\{m_5, m_6|t_1, t_2\}$, $\{m_4|t_3\}$, and $\{m_3|t_4\}$. The other concepts in the lattice (e.g., $\{m_2, m_5, m_6|t_1\}$ in Figure 3.2) are already included in the maximal grouping by the sub-concept relation which is graphically represented by the hierarchy in the lattice. As for the overlapped grouping, it generates five clusters, i.e. $\{m_1|t_2\}$, $\{m_2|t_1\}, \{m_3|t_4\}, \{m_4|t_3\}$ and $\{m_5, m_6|t_1, t_2\}$. The example shows that for the clusters generated by the overlapped grouping no mutants are discarded, while the FCA grouping discards $m_1$ and $m_2$. 

3.4. EXPERIMENTAL STUDY

We conducted an empirical study to evaluate the effectiveness of the different compression strategies presented in the previous section. The goal of the study is to answer the following research questions:

- **RQ3.1:** How accurate are different compression techniques? We assess the ability
3.4. **Experimental Study**

Table 3.1: Summary of compression strategies

<table>
<thead>
<tr>
<th>Strategy</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>overlap</td>
<td>The combination of overlapped grouping and random strategy in mutant selection.</td>
</tr>
<tr>
<td>overlap+mop</td>
<td>The combination of overlapped grouping and random strategy with the knowledge of the mutation operator type in mutant selection.</td>
</tr>
<tr>
<td>overlap+mloc</td>
<td>The combination of overlapped grouping and random strategy with the knowledge of the mutation location in mutant selection.</td>
</tr>
<tr>
<td>fca</td>
<td>The combination of FCA grouping and random strategy in mutant selection.</td>
</tr>
<tr>
<td>fca+mop</td>
<td>The combination of FCA grouping and random strategy with the knowledge of the mutation operator type in mutant selection.</td>
</tr>
<tr>
<td>fca+mloc</td>
<td>The combination of FCA grouping and random strategy with the knowledge of the mutation location in mutant selection.</td>
</tr>
</tbody>
</table>

of the six compression strategies to estimate the strong mutation scores. We also assess their performance in comparison with random sampling and weak mutation.

- **RQ3.2:** *How do compression techniques perform in terms of speed-up?* We investigate the speed-up in terms of execution time that can be obtained when using each compression strategy over strong mutation. We also consider random sampling and weak mutation as baselines.

- **RQ3.3:** *What is the trade-off between accuracy and speed-up for the compression techniques?* We evaluate to what extent the compression strategies can reduce execution time while maintaining an accurate estimation of the strong mutation scores.

3.4.1. **Experimental Setup**

To answer our research questions, we evaluated the six compression strategies using 20 open source projects publicly available on GitHub. Table 3.2 summarises the main characteristics of the selected projects. These projects have been randomly selected among the top 3000 GitHub repositories which (1) have most stars on 04/04/2017, (2) can be built using Maven, and (3) contain JUnit 4 test suites. In our study, we focus on the manually-written test suites available in the original project repositories.

As mentioned in Section 3.3, we first need one test execution against the original program to collect statement coverage (i.e., the mutant-by-test reachability) and the weak mutation information (i.e., the mutant-by-test necessity matrix). To collect weak and strong mutation information, we implemented our own prototype tool\(^2\). The instrumentation framework to generate mutants and detect the reachability and necessity condition is extracted from EvoSuite. Then, we integrated this instrumentation framework into our mutation testing runner. We record information about test cases (#id, method name, execution results, #touched mutants and #weakly killed mutants) and mutants

\(^2\)All the tools, scripts and metadata for this experimental study are available in our GitHub repository [387].
3. AN INVESTIGATION OF COMPRESSION TECHNIQUES TO SPEED UP MT

(#id, mutation operator type, location and detailed information) for further analysis. After that, we run each test case against each mutant of the class under test (strong mutation) to establish the mutant-by-test sufficiency matrix which is used to evaluate our methods.

The mutation operators we adopted in this experiment are six method-level operators: replace arithmetic, replace bitwise, replace comparison, replace variable, replace constant, and insert unary. Further details about these mutation operators can be found in the paper by Fraser and Arcuri [149]. We opted for the mutation engine available in EvoSuite [149] because it instruments the production code at bytecode level and allows to directly measure the infection state for each mutant (weak mutation). To the best of our knowledge, no publicly-available mutation tool provides utilities for computing the weak mutation scores.

To answer the three RQs, we selected another two mutation reduction techniques (see Section 3.2) for comparison: mutation sampling and weak mutation. We selected random sampling (do fewer strategy) as baseline because Gopinath et al. [160, 161] showed that none of the most common reduction strategies provide any practical advantage over pure random sampling. Moreover, we selected weak mutation (do smarter strategy) because it is one of the key components of all mutant compression techniques. Therefore, we considered it as an additional baseline to verify whether the other components of the compression strategies (e.g., computing the maximal groupings) are indeed needed. For random sampling, we set the sampling rate to 10% as suggested by Budd [93] and Acree [41]. They showed that 10% sampling could already estimate the mutation score with 99% of accuracy. It also corresponds to the sampling rate used by Gopinath et al. [160, 161]. Since random sampling and the mutant compression strategies involve random processing (i.e., in mutant selection), we carry out the corresponding random process 100 times for each project to address their randomised nature. In total, we compared eight mutation strategies: six compression strategies, random sampling (10%) and weak mutation.

3.4.2. EVALUATION METRICS

To answer RQ3.1, we selected two well-known performance metrics: the absolute error and the accuracy. Let M be a given mutation strategy (e.g., random sampling); let $strong_M(C, T)$ be the percentage of mutants for a class C that are strongly killed by the test suite T; let $estimated_M(C, T)$ be the estimated percentage of mutants that are killed according to the strategy M; the absolute error is defined as follows:

$$AE(C, T) = |strong_M(C, T) - estimated_M(C, T)|$$ (3.1)

While the compression techniques select only a subset of the mutants for strong mutation, they can also estimate whether the non-selected mutants are killable by leveraging the groupings generated by FCA. Therefore, we use the accuracy as further performance metric, which is defined as follows:

$$accuracy(C, T) = (TP + TN) / total$$ (3.2)

where TP denotes the number of mutants that are strongly killed by T and that are also correctly identified by a given method M (true positives); TN is the number of mutants
### Table 3.2: Subject Programs

<table>
<thead>
<tr>
<th>PID Project</th>
<th>LOC</th>
<th>#Classes</th>
<th>#Tests</th>
<th>COV</th>
<th>#Mutants</th>
<th>#Total Covered</th>
<th>#Weakly Killed</th>
<th>#Strongly Killed</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 assertj</td>
<td>24978</td>
<td>830</td>
<td>8545</td>
<td>0.90</td>
<td>59955</td>
<td>21677</td>
<td>19533</td>
<td>9178</td>
</tr>
<tr>
<td>2 checkstyle</td>
<td>31441</td>
<td>524</td>
<td>631</td>
<td>0.74</td>
<td>79464</td>
<td>18777</td>
<td>17738</td>
<td>9448</td>
</tr>
<tr>
<td>3 commons-lang</td>
<td>26578</td>
<td>264</td>
<td>2936</td>
<td>0.93</td>
<td>45630</td>
<td>43597</td>
<td>40453</td>
<td>33158</td>
</tr>
<tr>
<td>4 crawler4j</td>
<td>3745</td>
<td>47</td>
<td>11</td>
<td>0.27</td>
<td>3046</td>
<td>1017</td>
<td>853</td>
<td>505</td>
</tr>
<tr>
<td>5 dex-translator</td>
<td>4981</td>
<td>32</td>
<td>3</td>
<td>0.61</td>
<td>5812</td>
<td>1015</td>
<td>882</td>
<td>493</td>
</tr>
<tr>
<td>6 distributedlog</td>
<td>27976</td>
<td>697</td>
<td>339</td>
<td>0.43</td>
<td>21520</td>
<td>593</td>
<td>535</td>
<td>395</td>
</tr>
<tr>
<td>7 dynjs</td>
<td>34579</td>
<td>672</td>
<td>887</td>
<td>0.51</td>
<td>29148</td>
<td>14688</td>
<td>12960</td>
<td>8307</td>
</tr>
<tr>
<td>8 geotools</td>
<td>75236</td>
<td>991</td>
<td>670</td>
<td>0.38</td>
<td>62963</td>
<td>19852</td>
<td>17024</td>
<td>9135</td>
</tr>
<tr>
<td>9 graphhopper</td>
<td>26175</td>
<td>384</td>
<td>874</td>
<td>0.74</td>
<td>50319</td>
<td>11176</td>
<td>10168</td>
<td>7299</td>
</tr>
<tr>
<td>10 apns</td>
<td>1618</td>
<td>39</td>
<td>85</td>
<td>0.66</td>
<td>905</td>
<td>537</td>
<td>487</td>
<td>366</td>
</tr>
<tr>
<td>11 jtools</td>
<td>6262</td>
<td>133</td>
<td>43</td>
<td>0.82</td>
<td>7058</td>
<td>425</td>
<td>401</td>
<td>302</td>
</tr>
<tr>
<td>12 jfreechert</td>
<td>98334</td>
<td>657</td>
<td>2256</td>
<td>0.54</td>
<td>129417</td>
<td>14776</td>
<td>13057</td>
<td>5669</td>
</tr>
<tr>
<td>13 jpacman</td>
<td>1890</td>
<td>61</td>
<td>41</td>
<td>0.82</td>
<td>1606</td>
<td>1355</td>
<td>1159</td>
<td>580</td>
</tr>
<tr>
<td>14 junit-quickcheck</td>
<td>3038</td>
<td>67</td>
<td>354</td>
<td>0.98</td>
<td>1000</td>
<td>995</td>
<td>893</td>
<td>786</td>
</tr>
<tr>
<td>15 pac4j</td>
<td>5281</td>
<td>146</td>
<td>424</td>
<td>0.63</td>
<td>2703</td>
<td>1934</td>
<td>1689</td>
<td>929</td>
</tr>
<tr>
<td>16 pf4j</td>
<td>3021</td>
<td>67</td>
<td>24</td>
<td>0.28</td>
<td>1176</td>
<td>380</td>
<td>294</td>
<td>205</td>
</tr>
<tr>
<td>17 stream-lib</td>
<td>4767</td>
<td>77</td>
<td>121</td>
<td>0.83</td>
<td>11907</td>
<td>9920</td>
<td>9445</td>
<td>6924</td>
</tr>
<tr>
<td>18 telegrambots</td>
<td>1480</td>
<td>21</td>
<td>31</td>
<td>0.20</td>
<td>772</td>
<td>221</td>
<td>196</td>
<td>52</td>
</tr>
<tr>
<td>19 vraptor</td>
<td>12021</td>
<td>407</td>
<td>385</td>
<td>0.83</td>
<td>3490</td>
<td>2057</td>
<td>1652</td>
<td>1072</td>
</tr>
<tr>
<td>20 zt-zip</td>
<td>4255</td>
<td>84</td>
<td>3</td>
<td>0.71</td>
<td>2440</td>
<td>1049</td>
<td>906</td>
<td>422</td>
</tr>
</tbody>
</table>

**Overall**: 397656 6210 2470 0.64 520331 166041 150325 95225

**Note:** Column “LOC” standing for the line of code is measured by sloccount\[363\]. Column “#Tests” is the total number of passed test cases under our ComMT tool. We marked the value with underline when the total number of passed test cases is less than the entire test suite size. The failures of the test cases in our tool is because the dependencies of these test cases need to be configured by Maven plugin; this cannot be solved in the current version of ComMT. The fifth column “COV” means the line coverage of the test suite which is measured by IntelliJ IDEA coverage runner.

---

For **RQ3.2** we consider the speed-up metric. When establishing the speed-up, we should first consider the overhead induced by an approach. For random sampling, we consider the overhead to be zero, as mutation sampling does not require any prerequisite knowledge. For weak mutation, the overhead consists of one single execution of the test suite against an instrumented version of the original program. For the compression strategies, the overhead is composed of the overhead incurred by both weak mutation that are not strongly killed by \( T \) and that are correctly identified by \( M \) (true negatives); **total** denotes the total number of mutants for the class \( C \). To ease the comparison, we use the mean and standard deviation of absolute error and accuracy scores obtained for all classes in a given Java project.
and the compression procedure (mutant clustering and mutant selection):

\[ \text{overhead} = \text{exec\_time(weak\_mutation + compression)} \]  \hfill (3.3)

The speed-up metric itself is computed using strong mutation with coverage-based optimisation as the baseline. We explicitly chose this optimisation as it is already integrated into several existing mutation testing tools (e.g., JAVALANCHE [313], Major [204] and PIT/PiTest [3]). The results of random sampling and compression strategies are the average values over 100 runs; for weak mutation, the execution time is zero. Then, the speed-up is defined as follows:

\[ \text{speed-up} = \frac{\text{exec\_time(strong\_mutation)}}{\text{exec\_time(M)}} \]  \hfill (3.4)

where the denominator is the execution time of a method \( M \) computed as the sum of its overhead and the execution time needed to run the tests against the selected mutants.

For RQ3.3, we first provide a graphical comparison among the different mutation strategies by using the speedup-error graphs. In such a graph, the X-axis denotes the speed-up scores and the Y-axis shows the mean absolute error achieved by each strategy and for each project in our study; an “ideal” score would have a high X-value and a low Y-value. We also use the speedup-accuracy graphs, which plot the speed-up (mean) on the X-axis and the corresponding accuracy (mean) on the Y-axis; an “ideal” score would have a high X-value and a high Y-value. Although we may see some trends via graphical analysis, we would like to know which strategy achieves the best speed-up when accepting a given absolute error rate. Therefore, we consider the following absolute error thresholds: \( \sigma_{e_1} = 5\% \), \( \sigma_{e_2} = 10\% \), and \( \sigma_{e_3} = 15\% \). Then, for each threshold \( \sigma_{e_i} \) and for each mutation strategy \( M \), we count the number of projects for which \( M \) achieves the highest speed-up compared to the other strategies while yielding an absolute error score lower than \( \sigma_{e_i} \). Similarly, we also consider three accuracy thresholds, i.e., \( \sigma_{a_1} = 95\% \), \( \sigma_{a_2} = 90\% \), and \( \sigma_{a_3} = 85\% \). Different from the absolute error, we count the number of projects in which \( M \) achieves an accuracy higher than the threshold \( \sigma_{a_i} \).

Statistical Analysis. To assess whether the differences among the various mutation strategies are statistically significant or not, we adopt Friedman’s test [304] with \( \alpha = 0.05 \). It is a non-parametric test for comparing multiple treatments (mutation strategies) in the context of a multiple-problem analysis (i.e., multiple projects) [304]; it does not require data to be normally distributed and it is widely applied to compare randomised algorithms [154, 286] (e.g., random sampling). While Friedman’s test reveals whether data distributions differ statistically, tests for pairwise comparison are needed to determine which treatment outperforms the others. For this, we use Conover’s post-hoc procedure [104] and we further adjusted the obtained \( p \)-values using Holm-Bonferroni [181].

3.5. RESULTS

3.5.1. RQ3.1: ACCURACY
Table 3.3 reports the mean accuracy and absolute error scores for each project in our study as well as the corresponding standard deviation scores.

Absolute error. Focusing on the absolute error we observe that weak mutation performs worst with an error rate of 23% and a standard deviation of 22% on average. This
result is due to this strategy using all mutants that are weakly covered to approximate strong mutation coverage, yet, not all infected states propagate to changes observable in assertions.

Moreover, overlap+mloc produces the lowest mean absolute error in 19 out of 20 projects, followed by fca+mloc and overlap+mop. Overall, the strategies using overlapped grouping perform slightly better than FCA-based maximal groupings. To ease the comparison between the compression techniques and random sampling, in Table 3.3 we underline the mean and std values of a compression technique if they are smaller (better) than the values of random sampling in the same project. We can see that the six compression strategies outperform random sampling in terms of absolute error scores for most projects. The best (lowest) scores are obtained using the overlap+mop, overlap+mloc, fca+mop and fca+mloc approaches.

Looking at the six compression strategies, we can see that the mean absolute error and standard deviation scores are reduced when incorporating knowledge of mutation operators (mop) and location (mloc). For example, overlap achieves an error rate of 15% for the jpacman project, while when adding mutation operator and location knowledge it achieves an error rate of 10% and 7%, respectively. In general, we find that mutant location is more important than mutation operator, as the absolute error decreases by 4% on average, with a minimum improvement of 1% for assert j and a maximum improvement of 13% for zt−zip. This is an important novel contribution distinct from most related work, which consider mutation operators as a key element to detect redundant mutants or subsuming mutants (e.g. [46, 202, 219]). Hence, we found that mutation location trumps mutation operator information when selecting mutants to evaluate for strong mutation.

According to results of Friedman's test, the different mutation strategies achieve significantly different absolute error values (p-value = 10⁻¹⁶). To better understand which strategies perform best, Table 3.4 reports the final ranking produced by Friedman's test as
Table 3.4: Ranking produced by Friedman’s (larger rank indicates smaller error) and Statistical Significance by Conover’s post-hoc procedure

<table>
<thead>
<tr>
<th>ID</th>
<th>Algorithms</th>
<th>Rank</th>
<th>Significantly better than (PID)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(1)</td>
<td>overlap + Mloc</td>
<td>8.00</td>
<td>(2), (3), (4), (5), (6), (7), (8)</td>
</tr>
<tr>
<td>(2)</td>
<td>FCA + Mloc</td>
<td>6.55</td>
<td>(4), (5), (6), (7), (8)</td>
</tr>
<tr>
<td>(3)</td>
<td>overlap + Mop</td>
<td>6.30</td>
<td>(4), (5), (6), (7), (8)</td>
</tr>
<tr>
<td>(4)</td>
<td>FCA + Mop</td>
<td>4.55</td>
<td>(6), (7), (8)</td>
</tr>
<tr>
<td>(5)</td>
<td>Overlap</td>
<td>4.40</td>
<td>(6), (7), (8)</td>
</tr>
<tr>
<td>(6)</td>
<td>Random Sampling</td>
<td>2.70</td>
<td>(8)</td>
</tr>
<tr>
<td>(7)</td>
<td>FCA</td>
<td>2.50</td>
<td>(8)</td>
</tr>
<tr>
<td>(8)</td>
<td>Weak Mutation</td>
<td>1.10</td>
<td>-</td>
</tr>
</tbody>
</table>

well as the results of the pairwise comparison from Conover’s procedure. As we can observe, overlap with mutant location knowledge (mloc) is ranked first and performs significantly better than all other strategies in the comparison. FCA based on maximal groupings with mutant location knowledge is ranked second and statistically outperforms all other strategies with lower ranks. Finally, random sampling is statistically worse than all overlap strategies and FCA enhanced with mloc and mop. Instead, the original FCA approach proposed by our preliminary study [391] is statistically equivalent to random sampling in terms of absolute error.

Accuracy. The results for the accuracy are also reported in Table 3.3. Since random sampling selects 10% mutants to evaluate in strong mutation, it cannot be used to estimate whether the other non-selected mutants are killable or not. Conversely, the six compression strategies can estimate whether each mutant is killable even if only a few mutants are actually evaluated for strong mutation. This is possible thanks to the two-way clusters generated by FCA: if a mutant is strongly killed, then we assume that all other mutants within its own cluster are killable as well. In weak mutation, we consider as strongly killable all mutants that lead to a state infection (i.e., the weakly killed ones).

Similar to results of the absolute error, the top three strategies are overlap+mloc, fca+mloc and overlap+mop in terms of accuracy. Again, weak mutation produces the worst accuracy in terms of both mean and standard deviation values. The three compression methods based on the overlapped grouping are slightly better than those in FCA. These differences are due to the fact that FCA considers only the maximal groupings as clusters from which selecting tests and mutants to run. However, as explained in Section 3.3, maximal groupings can miss some mutants, which therefore are not assigned to any cluster. Hence, we cannot accurately estimate whether the missed mutants are likely to be strongly killed or not based on the results of other selected mutants. We also notice that compression with additional mutant information can enhance the prediction accuracy. Finally, the finding that mutation location trumps mutation operator information still holds: the improvements range between 1% (for commons-lang) and 13% (for junit-quickcheck) in terms of accuracy.

Overlap with mutation location knowledge outperforms all other mutation strategies in terms of both absolute error and prediction accuracy. Random sampling is statistically worse than all mutant compression techniques.
Table 3.5: Summary of results for RQ3.2

<table>
<thead>
<tr>
<th>Speed-up summary (selected mutant% / speed-up)</th>
<th>Random Sampling</th>
<th>Weak Mutation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Simple w/ Mop w/ Mloc</td>
<td>Simple w/ Mop w/ Mloc</td>
<td>Simple w/ Mop w/ Mloc</td>
</tr>
<tr>
<td>1</td>
<td>1.64/0.06</td>
<td>1.18/0.06</td>
</tr>
<tr>
<td>2</td>
<td>0.28/0.08</td>
<td>0.30/0.08</td>
</tr>
<tr>
<td>3</td>
<td>2.53/0.27</td>
<td>3.10/0.27</td>
</tr>
<tr>
<td>4</td>
<td>0.16/0.10</td>
<td>0.10/0.30</td>
</tr>
<tr>
<td>5</td>
<td>0.01/10.10</td>
<td>0.02/10.10</td>
</tr>
<tr>
<td>6</td>
<td>0.02/10.02</td>
<td>0.01/10.02</td>
</tr>
<tr>
<td>7</td>
<td>0.03/0.03</td>
<td>0.04/0.03</td>
</tr>
<tr>
<td>8</td>
<td>1.56/0.23</td>
<td>2.09/0.23</td>
</tr>
<tr>
<td>9</td>
<td>0.13/0.18</td>
<td>0.13/0.18</td>
</tr>
<tr>
<td>10</td>
<td>0.03/0.08</td>
<td>0.02/0.08</td>
</tr>
<tr>
<td>11</td>
<td>0.03/0.03</td>
<td>0.06/0.03</td>
</tr>
<tr>
<td>12</td>
<td>3.85/0.21</td>
<td>4.42/0.21</td>
</tr>
<tr>
<td>13</td>
<td>0.10/15.10</td>
<td>0.02/15.10</td>
</tr>
<tr>
<td>14</td>
<td>0.01/0.01</td>
<td>0.07/0.01</td>
</tr>
<tr>
<td>15</td>
<td>0.13/29.12</td>
<td>0.26/29.12</td>
</tr>
<tr>
<td>16</td>
<td>0.00/3.11</td>
<td>0.01/3.11</td>
</tr>
<tr>
<td>17</td>
<td>0.00/0.00</td>
<td>0.01/0.00</td>
</tr>
<tr>
<td>18</td>
<td>0.00/0.00</td>
<td>0.01/0.00</td>
</tr>
<tr>
<td>19</td>
<td>2.55/48</td>
<td>0.57/48</td>
</tr>
<tr>
<td>20</td>
<td>0.00/0.00</td>
<td>0.00/0.00</td>
</tr>
</tbody>
</table>

Mean: 0.15/12.54

Note: The second, third and fourth columns (i.e., Column “Simple”, “w/ Mop” and “w/ Mloc”) under Column “Overlap” correspond to method overlap, overlap+mop and overlap+mloc in Table 3.1. A similar rule applies to the fifth, sixth and seventh columns under Column “FCA”. To be clear, we highlight the highest values in the overhead ratios and two strategies achieving the best speed-up scores in **bold**. Also, we underline the compression strategies that achieve better speed-up scores than random sampling in each project.

### 3.5.2. RQ3.2: SPEED-UP

**Speed-up performance.** Table 3.5 summarises the overall speed-up for the eight approaches in our comparison. For each project, we highlight the two strategies achieving the best speed-up scores in **bold**. Notice that speed-up measures the overall execution time of strong mutation divided by the overall execution time of a mutation strategy. Hence, higher values denote a larger improvement in execution time.

We observe that weak mutation shows the highest speed-up scores since it only requires one suite execution against the original program. Except for weak mutation, FCA achieves the highest speed-up scores in 19 out of 20 cases. **FCA is also faster than random sampling**, which selects 10% mutants for strong mutation. Indeed, the former is 6.6 times faster than the latter on average, with a minimum speed-up of 2.6X (in vraprotor and in reachability condition) of 15.4X (in stream-lir). This is because FCA suggests on average less than 10% of mutants (with a minimum of 0.4% of mutants) to evaluate in strong mutation analysis. Instead, the sampling strategy constantly (and randomly) selects 10% of mutants to execute.

The only exception to the previous finding is represented by distributedlog for which **random sampling** is faster than FCA. In this case, the total percentage of mutants that are injected into statements covered by the test suite (reachability condition) is fairly low, being 2.8%. Thus, random sampling can achieve a considerable speed-up if we leverage the coverage-based optimisation, i.e., if we skip uncovered mutants (i.e., mutants of uncovered statements). Instead, FCA selects almost twice as many mutants for these projects.

To further ease the comparison, in Table 3.5 we underline the compression strategies that achieve better speed-up scores than random sampling in each project. We observe that overlap, FCA+mop and overlap+mop outperform random sampling in terms of speed-up for 19 projects out of 20. On average, they are respectively 3.7X, 3.0X, and 2.1X.
faster than random sampling. It is worth noticing that the number of selected mutants does not directly determine the overall speed-up. For example, for the project pac4j, overlap selected 21.0% of mutants, which is larger than the percentage of mutants selected by mutation sampling (i.e., 10%). However, overlap achieves a larger speed-up of 4.8X against 3.1X of mutation sampling. The reason is that compression strategies use weak mutation information to further filter out the unnecessary test executions, while mutation sampling does not.

From the comparison of the six compression strategies, we observe that including mutant location leads to selecting more mutants for strong mutation, thus, reducing the overall speed-up. For example, overlap+mloc achieves lower speed-up scores than overlap in all 20 projects. Moreover, by comparing the two strategies based on mutation location knowledge (i.e., overlap+mloc and fca+mloc) with random sampling, we observe that the differences in terms of speed-up are small. Indeed, the average speed-up scores of overlap+mloc, fca+mloc and random sampling are 5.13, 5.44 and 5.42, respectively. Instead, selecting mutants according to mutation operator generates a lower number of mutants to evaluate in strong mutation compared to mutation location.

Our findings are confirmed by Friedman’s test (shown in Table 3.6): the mutation strategies are statistically different in terms of speed-up scores (p-value = 10^{-16}). According to Conover’s procedure, weak mutation and FCA statistically outperform all other mutation strategies. Moreover, random sampling is ranked sixth and is statistically more efficient than overlap+mloc only, although the difference is marginal as suggested by the average scores reported in Table 3.5. Instead, FCA, overlap, FCA+mop and overlap+mop are statistically superior to random sampling.

**Overhead.** In the previous paragraphs, we observed that most of mutation compression strategies are more efficient than random sampling. Here, we investigate the overhead that is due to the different steps that such strategies implement. In the following, we consider as compression overhead the execution time needed to compute the maximal and/or overlapped groupings; while the overall overhead is the sum of the compression overhead, the time for running all tests once for weak mutation, and the time to select the mutants.

Table 3.5 reports the compression overhead and overall overhead as a percentage (ratio) of the full execution time of each strategy, which also includes the time needed to run the selected tests and mutants for strong mutation. The highest values for each project are highlighted in bold face. From Table 3.5, we can observe that the compression over-
head takes up less than 0.001% of the total execution time; thus, it is negligible with respect to the execution time of evaluating the selected mutants for strong mutation. The overall overhead accounts for up to 9.30% of the total execution time and weak mutation represents the larger portion of this overhead. Among the 20 projects, the overall overhead of the strategy FCA is likely higher than the other compression strategies. However, the differences among them are lower than 0.1%.

Weak mutation scores best among the eight techniques in terms of speed-up. Without considering weak mutation, four mutant compression strategies are statistically more efficient (have better speed-up scores) then random sampling.

3.5.3. RQ3.3: TRADE-OFFS
From the results of RQ3.1 and RQ3.2, it is clear that the mutation strategies that perform best in terms of accuracy are also the more expensive to perform. Weak mutation and FCA grouping strategies perform best in terms of speed-up, while the overlapped grouping strategies, and overlap+mloc in particular, better approximate the strong mutation score. Therefore, in this section, we analyse the trade-offs between speed-up, absolute error and accuracy.

From Figure 3.3, we observe that weak mutation achieves the best speed-up, while its absolute error and accuracy typically score worst when compared to other techniques. FCA comes second in terms of the overall speed-up, but its absolute error as well as accuracy are better than weak mutation for most of the projects. We notice that overlap is slightly slower than FCA, but shows a small improvement in both absolute error and accuracy when compared to FCA. FCA+mop and overlap+mop have quite similar trade-offs considering speed-up and absolute error as their data points are very close to each other. However, in terms of speed-up and accuracy, fca+mop is slightly faster than overlap+mop, while overlap+mop is more accurate than fca+mop. Moreover, overlap+mloc, fca+mloc and random sampling have the same speed-up score; however, the absolute error of random sampling is higher than for the other two strategies. Overlap+mloc and fca+mloc are the most accurate strategies in terms of both absolute error and accuracy, but their speed-up performance is the least good.

Table 3.7 shows the number of projects for which each strategy $M$ provide the best speed-up score at different thresholds of absolute error ($\sigma_e$) or accuracy ($\sigma_a$). As we can observe, overlap+mloc has the highest speed-up score when considering an absolute error $\leq 5\%$ for 10 projects out of 20. This indicates that using mutation location leads to more accurate estimations of the actual strong mutation. When considering a 10% error rate threshold, FCA+mop and FCA show the largest speed-up for the majority of projects. Instead, when the goal is to reach an absolute error $\leq 15\%$, FCA has the best speed-up scores for 11 out of 20 projects. Moreover, we notice that random sampling performs worst as it has speed-up scores that are always lower then the other mutation strategies at the same (or higher) level of absolute error.

Similar results can be observed when considering different thresholds for accuracy. As reported in Table 3.7, overlap+mloc and fca+mloc show the best speed-up for accuracy $\geq 95\%$ for the relative majority of the projects. When considering an accuracy $\geq 90\%$, overlap and fca+mloc show the best speed-up for 5 out of 20 projects each. Instead, if
3. AN INVESTIGATION OF COMPRESSION TECHNIQUES TO SPEED UP MT

Table 3.7: Number of projects for which each strategy $M_j$ provides the best speed-up score at different thresholds

(a) Error Rate

<table>
<thead>
<tr>
<th>Absolute Error</th>
<th>Overlap Simple</th>
<th>FCA Simple w/ Mop</th>
<th>Random Sampling</th>
<th>Weak Mut.</th>
</tr>
</thead>
<tbody>
<tr>
<td>≤5%</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>≤10%</td>
<td>4</td>
<td>1</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>≤15%</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td><strong>overall</strong></td>
<td>7</td>
<td>5</td>
<td>12</td>
<td>0</td>
</tr>
</tbody>
</table>

(b) Accuracy

<table>
<thead>
<tr>
<th>Accuracy</th>
<th>Overlap Simple</th>
<th>FCA Simple w/ Mop</th>
<th>Random Sampling</th>
<th>Weak Mut.</th>
</tr>
</thead>
<tbody>
<tr>
<td>≥95%</td>
<td>2</td>
<td>0</td>
<td>7</td>
<td>0</td>
</tr>
<tr>
<td>≥90%</td>
<td>5</td>
<td>3</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>≥85%</td>
<td>4</td>
<td>8</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td><strong>overall</strong></td>
<td>11</td>
<td>8</td>
<td>12</td>
<td>3</td>
</tr>
</tbody>
</table>

Note: The second, third and fourth columns (i.e., Column “Simple”, “w/ Mop” and “w/ Mloc”) under Column “Overlap” correspond to method overlap, overlap+mop and overlap+mloc in Table 3.1. A similar rule applies to the fifth, sixth and seventh columns under Column “FCA”. The last column “Weak Mut.” stands for the strategy of weak mutation.

we focus on 85% of accuracy, we observe that FCA is the best approach to choose as it shows a speed-up ranging from 6.3X up to 94.3X compared to strong mutation. Finally, if we focus on 85% accuracy, we observe that FCA is the best approach to choose.

**Overlap+mloc** provides the best speed-up scores when the goal is to achieve an accuracy >95% or an absolute error <0.05. Other mutation compression strategies provide larger speed-up, but with a corresponding decrease in accuracy. Random sampling is less accurate and/or slower than all compression strategies.

3.5.4. DISCUSSION

Looking at all the results, we can observe that random sampling with 10% sampling ratio is able to speed up (strong) mutation testing from 2.0 to 22.7X with an absolute error within 15% for 80% of the projects. Mutation sampling is also easy to apply in mutation tools as it does not require any prerequisite knowledge of the program context and mutation operators. However, mutation strategies based on compression techniques achieve better speed-up (i.e., are more efficient) and lower absolute error than random sampling. For example, overlap+mloc yields an absolute error which is always lower than 9% with a speed-up ranging between 2.0 to 53X. This represents an important finding if we consider the recent study by Gopinath et al. [160], which showed that other mutation reduction techniques (including e-selective) provide small or negligible improvements in effectiveness and are more expensive compared to random sampling.

Another disadvantage of random sampling is that it can estimate the overall muta-
3.6. Threats to Validity

Threats to external validity: Our results are based on mutants generated by the operators implemented in EvoSuite; these results might be different when using other mutation tools [220]. With regard to the subject selection, we chose 18 out of the 20 projects from GitHub’s top starred 3000 repositories; the selected projects differ in size, number of test cases and application domain.

Threats to internal validity: The main threat for our study is the implementation of the compression strategies. For FCA, we use its implementation available in MATLAB [245], which is a well-known scientific software. For the instrumentation and the mutation operators, we relied on their implementation available in EvoSuite [147]. Moreover, we carefully reviewed and tested all code for our study to eliminate potential faults in our implementation.

Threats to construct validity: The main threat is the measurement we used to evaluate our methods. We minimise this risk by adopting evaluation metrics that are widely used in research, as well as proper statistical analysis to assess the significance.

3.7. Conclusions

In this chapter, we have conducted a detailed investigation of different compression techniques to speed up mutation testing based on the work by our preliminary work [391]. We have enhanced our original FCA-based compression strategy in two distinct ways: (1) by proposing a novel mutant clustering algorithm, overlapped grouping, in addition to FCA; (2) by incorporating mutation location and mutation operator information in the compression procedure. Thereby, we have introduced and investigated six compression strategies based on two clustering algorithms and three mutant selection strategies.

The results of an empirical study with 20 open-source projects show that mutant compression techniques can effectively speed up strong mutation testing up to 94.3 times with an accuracy > 90%. FCA is the fastest strategy while overlap+mloc is the most accurate. In comparison, weak mutation attains a higher absolute error (23%) and lower accuracy (75%). Random sampling with 10% as sampling percentage is statistically less accurate than all mutant compression strategies, and worse in terms of speed-up than four compression strategies (excluding the two with knowledge of mutation locations).

Another important finding is that mutation location trumps mutation operator in-
formation when selecting mutants to evaluate for strong mutation. Hence, researchers should take into account the mutation location in addition to the mutation operators when detecting redundant or subsuming mutants (e.g. [46, 202, 219]). This is a clear invitation for future work.

Since our results are encouraging, we envision the following future work: (i) combining mutant location and mutation operator information; (ii) investigating other compression methods, such as Principal Component Analysis [366]; (iii) applying compression techniques in mutation-based test case generation [148, 285].
3.7. Conclusions

Figure 3.3: Graphical comparison of eight mutation strategies in terms of speed-up, absolute error and accuracy
Mutation testing is well-known for its efficacy to assess test quality, and it is starting to be applied in the industry as well. However, what should a developer do when confronted with a low mutation score? Should the test suite be plainly reinforced (i.e., writing additional tests) to increase the mutation score, or should the production code be improved as well, to make the creation of better tests possible (i.e., improving the production code and then writing additional tests)? In this chapter, we aim to provide a new perspective to developers that enables them to understand and reason about the mutation score in the light of testability and observability. First, we investigate whether testability and observability metrics are correlated with the mutation score on six open-source Java projects. We observe a correlation between observability metrics and the mutation score, e.g., test directness, which measures the extent to which the production code is tested directly, seems to be an essential factor. Based on our insights from the correlation study, we propose a number of “mutation score anti-patterns”, which enable software engineers to refactor their existing code or adding tests to be able to improve the mutation score. In doing so, we observe that relatively simple refactoring operations enable an improvement or increase in the mutation score. Moreover, taking Object-Oriented (OO) design principles into consideration, our study can guide developers in making choices between (1) adding new tests, (2) refactoring the production code, or (3) ignoring the surviving mutants when confronting the low mutation score.

This chapter has been submitted to the Journal of Systems and Software.
4.1. INTRODUCTION

Mutation testing has been a very active research field since the 1970s as a technique to evaluate test suite quality in terms of the fault-revealing capability [197]. Recent advances have made it possible for mutation testing to be used in industry [298]. For example, PIT/PITest [99] has been adopted by several companies, such as The Ladders and British Sky Broadcasting [102]. Furthermore, Google [297] has integrated mutation testing with the code review process for around 6000 software engineers.

As mutation testing gains traction in the industry, a better understanding of the mutation score (one outcome of mutation testing) becomes essential. The existing works have mainly linked the mutation score with test quality [189, 228] (i.e., how good is the test suite at detecting faults in the software?) and mutant utility [203, 373] (i.e., how useful is the mutant?). However, in Chapter 5, we have observed that certain mutants could be killed only after refactoring the production code to increase the observability of state changes. In such cases, test deficiency is not the only reason for the survival mutants, but some issues in the production code, such as code observability, result in difficulties to kill the mutants. Different from the previous works (e.g., [189, 203, 228, 373]), our goal is to bring a new perspective to developers that enable them to understand and reason about the mutation score in the light of testability and observability. Thereby, developers can make a choice when confronting low mutation scores: (1) adding new tests, (2) refactoring the production code to be able to write better tests, or (3) ignoring the surviving mutants.

To this aim, our study consists of two parts: firstly, we investigate the relationship between testability/observability and mutation testing in order to find the most correlated metrics; secondly, based on what we observe from the correlations, we define anti-patterns or indicators that software engineers can apply to their code to kill the surviving mutants. More specifically, we start with the investigations of the relationship between testability/observability metrics and the mutation score inspired by the work of Bruntink and van Deursen [89]. Testability is defined as the “attributes of software that bear on the effort needed to validate the software product” [89, 191]. Given our context, an important part of testability is observability, which is a measure of how well internal states of a system can be inferred, usually through the values of its external outputs [328]. Whalen et al. [362] formally defined observability as follows: An expression in a program is observable in a test case if the value of an expression is changed, leaving the rest of the program intact, and the output of the system is changed correspondingly. If there is no such value, the expression is not observable for that test. Compared to testability which covers various aspects of a project (e.g., inheritance and cohesion), observability is more specifically addressing the extent to which the value change of expression is observable in a test case.

Our first three research questions steer our investigation in the first part of our study:

RQ4.1 What is the relation between testability metrics and the mutation score?

RQ4.2 What is the relation between observability metrics and the mutation score?

RQ4.3 What is the relation between the combination of testability and observability metrics and the mutation score?
After investigating the relationship between testability/observability and mutation testing, we still lack insight into how these relationships can help developers to take actions when facing survival mutants. That is why, based on the observations from RQ4.1-RQ4.3, we define anti-patterns or indicators that software engineers can apply to their code/tests to ensure that mutants can be killed. This leads us to the next research question:

RQ4.4 To what extent does the removal of anti-patterns based on testability and observability help in improving the mutation score?

In terms of the methodology that we follow in our study, for RQ4.1-RQ4.3, we use statistical analysis on open-source Java projects to investigate the relationship between testability, observability, and the mutation score. For RQ4.4, we perform a case study with 16 code fragments to investigate whether the removal of anti-patterns increases the mutation score.

4.2. BACKGROUND

In this section, we briefly introduce the basic concepts of and related works on mutation testing, testability metrics, and our proposed metrics for quantifying code observability.

4.2.1. MUTATION TESTING

Mutation testing is defined by Jia and Harman [197] as a fault-based testing technique which provides a testing criterion called the mutation adequacy score. This score can be used to measure the effectiveness of a test suite regarding its ability to detect faults [197]. The principle of mutation testing is to introduce syntactic changes into the original program to generate faulty versions (called mutants) according to well-defined rules (mutation operators) [279]. The benefits of mutation testing have been extensively investigated and can be summarised in Chapter 2 as: 1) having better fault exposing capability compared to other test coverage criteria [144, 228, 244], 2) being a valid substitute to real faults and providing a good indication of the fault detection ability of a test suite [50, 201].

Researchers have actively investigated mutation testing for decades (as evidenced by the extensive survey [197, 241, 279, 393]). Recently, it has started to attract attention from industry [298]. In part, this is due to the growing awareness of the importance of testing in software development [48]. Code coverage, the most common metric to measure test suite effectiveness, has seen its limitations being reported in numerous studies (e.g., [144, 189, 228, 244]). Using structural coverage metrics alone might be misleading because in many cases, statements might be covered, but their consequences might not be asserted [189]. Another factor is that a number of well-developed open-source mutation testing tools (e.g., PIT/PITest [99] and Mull [12]) have contributed to mutation testing being applied in the industrial environments [102, 297, 298].

However, questions still exist about mutation testing, especially regarding the usefulness of a mutant [203]. The majority of the mutants generated by existing mutation operators are equivalent, trivial and redundant [88, 198, 203, 219, 295], which reduces the efficacy of the mutation score. If a class has a high mutation score while most mutants generated are trivial and redundant, the high mutation score does not promise high test effectiveness. A better understanding of mutation score and mutants is thus important.
To address this knowledge gap, numerous studies have investigated how useful mutants are. Example studies include mutant subsumption [219], stubborn mutants [373], and real-fault coupling [201, 295]. These studies paid attention to the context and types of mutants as well as the impact of the test suite, while the impact of production code quality has rarely been investigated. We have seen how code quality can influence how hard it is to test [89] (called software testability [151]), and since mutation testing can generally be considered as “testing the tests,” production code quality could also impact mutation testing, just like production code quality has been shown to be correlated with the presence of test smells [325]. Due to the lack of insights into how code quality affects the efforts needed for mutation testing, especially in how to engineer tests that kill all the mutants, we conduct this exploratory study. Our study can help researchers and practitioners deepen their understanding of the mutation score, which is generally related to test suite quality and mutant usefulness.

4.2.2. Existing Object-Oriented Metrics for Testability

The notion of software testability dates back to 1991 when Freedman [151] formally defined observability and controllability in the software domain. Voas [354] proposed a dynamic technique coined propagation, infection and execution (PIE) analysis for statistically estimating the program’s fault sensitivity. More recently, researchers have aimed to increase our understanding of testability by using statistical methods to predict testability based on various code metrics. Influential works include that of Bruntink and van Deursen [89], in which they explored the relationship between nine object-oriented metrics and testability. To explore the relation between testability and mutation score (RQ4.1), we first need to collect a number of existing object-oriented metrics which have been proposed in the literature. In total, we collect 64 code quality metrics, including both class-level and method-level metrics that have been the most widely used. We select those 64 metrics because they measure various aspects of a project, including basic characteristics (e.g., NLOC and NOMT), inheritance (e.g., DIT), coupling (e.g., CBO and FIN), and cohesion (LCOM). A large number of those metrics, such as LCOM and HLTH have been widely used to explore software testability [89, 153] and fault prediction [57, 167].

We present a brief summary of the 64 metrics in Table 4.1 (method-level) and Tables 4.2–4.3 (class-level). These metrics have been computed using a static code analysis tool provided by JHawk [18].

4.2.3. Code Observability

To explore the relation between observability and mutation score (RQ4.2), we first need a set of metrics to quantify code observability. According to Whalen et al. [362]’s definition of observability (as mentioned in Section 4.1), we consider that code observability comprises two perspectives: that of production code and that of the test case. To better explain these two perspectives, let us consider the example in Listing 4.1 from project jfreechart-1.5.0 showing the method setSectionPaint and its corresponding test. This method is to set the section paint associated with the specified key for the PiePlot object, and sends a PlotChangeEvent to all registered listeners. There is one mutant in Line 3 that removes the call to org/jfree/chart/plot/PiePlot::fireChangeEvent.
This mutant is not killed by testEquals. Looking at the observability of this mutant from the production code perspective, we can see that the setSectionPaint method is void; thus, this mutant is hard to detect because there is no return value for the test case to assert. From the test case perspective, although testEquals invokes the method setSectionPaint in Line 14 and 17, no proper assertion statements are used to examine the changes of fireChangeEvent() (which is used to send an event to listeners).

Starting with two angles of code observability, we come up with a set of the code observability metrics. Since our study is a starting point to design metrics to measure the code observability, we start with the simple and practical metrics, which are easy for practitioners to understand and apply.

First of all, we consider the return type of the method. As discussed in Listing 4.1, in a void method it is hard to observe the changing states inside the method because there is no return value for test cases to assert. Accordingly, we design two metrics, is_void and non_void_percent (shown in 1st and 2nd rows in Table 4.5). The metric is_void is to examine whether the return value of the method is void or not. The metric non_void_percent addresses the return type at class level which measures the percent of non-void methods in the class. Besides these two, a void method might change the

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Full name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>COMP</td>
<td>Cyclomatic Complexity</td>
<td>McCabe’s cyclomatic Complexity for the method</td>
</tr>
<tr>
<td>NOA</td>
<td>Number of Arguments</td>
<td>The number of Arguments</td>
</tr>
<tr>
<td>NOCL</td>
<td>Number of Comments</td>
<td>The number of Comments associated with the method</td>
</tr>
<tr>
<td>Nocl</td>
<td>Number of Comment Lines</td>
<td>The number of Comment Lines associated with the method</td>
</tr>
<tr>
<td>VDEC</td>
<td>Variable Declarations</td>
<td>The number of variables declared in the method</td>
</tr>
<tr>
<td>VREF</td>
<td>Variable References</td>
<td>The number of variables referenced in the method</td>
</tr>
<tr>
<td>NOS</td>
<td>Number of Java statements</td>
<td>The number of statements in the method</td>
</tr>
<tr>
<td>NEXP</td>
<td>Number of expressions</td>
<td>The number of expressions in the method</td>
</tr>
<tr>
<td>MDN</td>
<td>Max depth of nesting</td>
<td>The maximum depth of nesting in the method</td>
</tr>
<tr>
<td>HLTH</td>
<td>Halstead length</td>
<td>The Halstead length of the metric (one of the Halstead Metrics)</td>
</tr>
<tr>
<td>HVOC</td>
<td>Halstead vocabulary</td>
<td>The Halstead vocabulary of the method (one of the Halstead Metrics)</td>
</tr>
<tr>
<td>HVOL</td>
<td>Halstead volume</td>
<td>The Halstead volume of the method (one of the Halstead Metrics)</td>
</tr>
<tr>
<td>HDIF</td>
<td>Halstead difficulty</td>
<td>The Halstead difficulty of the method (one of the Halstead Metrics)</td>
</tr>
<tr>
<td>HEFF</td>
<td>Halstead effort</td>
<td>The Halstead effort of the method (one of the Halstead Metrics)</td>
</tr>
<tr>
<td>HBUG</td>
<td>Halstead bugs</td>
<td>The Halstead prediction of the number of bugs in the method (one of the Halstead Metrics)</td>
</tr>
<tr>
<td>TDN</td>
<td>Total depth of nesting</td>
<td>The total depth of nesting in the method</td>
</tr>
<tr>
<td>CAST</td>
<td>Number of casts</td>
<td>The number of class casts in the method</td>
</tr>
<tr>
<td>LOOP</td>
<td>Number of loops</td>
<td>The number of loops (for, while) in the method</td>
</tr>
<tr>
<td>NOPR</td>
<td>Number of operators</td>
<td>The total number of operators in the method</td>
</tr>
<tr>
<td>NAND</td>
<td>Number of operands</td>
<td>The total number of operands in the method</td>
</tr>
<tr>
<td>CREF</td>
<td>Number of classes referenced</td>
<td>The classes referenced in the method</td>
</tr>
<tr>
<td>XMET</td>
<td>Number of external methods</td>
<td>The external methods called by the method</td>
</tr>
<tr>
<td>LMET</td>
<td>Number of local methods</td>
<td>The number of methods local to this class called by this method</td>
</tr>
<tr>
<td>EXCR</td>
<td>Number of exceptions referenced</td>
<td>The number of exceptions referenced by the method</td>
</tr>
<tr>
<td>EXCT</td>
<td>Number of exceptions thrown</td>
<td>The number of exceptions thrown by the method</td>
</tr>
<tr>
<td>MOD</td>
<td>Number of modifiers</td>
<td>The number of modifiers (public, protected, etc.) in method declaration</td>
</tr>
<tr>
<td>NLOC</td>
<td>Lines of Code</td>
<td>The number of lines of code in the method</td>
</tr>
</tbody>
</table>
Table 4.2: Summary of class-level code quality metrics (1)

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Full name</th>
<th>Description</th>
</tr>
</thead>
</table>
| NOMT         | Number of methods                | The number of methods in the class (WMC - one of the Chi-
field(s) of the class it belongs to. A workaround to test a void method is to invoke getters. So getter_percentage (shown in 3rd row in Table 4.5) is proposed to complement is_void.

Secondly, we come up with the access control modifiers. Let us consider the example in Listing 4.2 from project commons-lang-LANG_3_7. The method getMantissa in class NumberUtils returns the mantissa of the given number. This method has only one mutant: the return value is replaced with “return if (getMantissa(str, str.length()) != null) null else throw new RuntimeException”. This mutant should be easy to detect given an input of either a legal String object (the return value is not null) or a null string (throw an exception). The reason this “trivial” mutant is not detected is because the method getMantissa is private. The access control modifier private makes it impossible to directly test the method getMantissa, for this method is only visible to methods from class NumberUtils. To test this method, the test case must first invoke a

1This mutant is generated by Return Values Mutator in PIT [103]. In Listing 4.2, getMantissa(str, str.length()) returns a String object. When the return value of a method is an object, the mutator replaces non-null return values with null and throw a java.lang.RuntimeException if the un-mutated method would return null.
4.2. **Background**

Table 4.3: Summary of class-level code quality metrics (2)

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Full name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PACK</td>
<td>Number of Packages imported</td>
<td>The number of packages imported by the class. (One of the Chidamber and Kemerer metrics)</td>
</tr>
<tr>
<td>RFC</td>
<td>Response for Class</td>
<td>The value of the Response For Class metric for the class.</td>
</tr>
<tr>
<td>MPC</td>
<td>Message passing</td>
<td>The value of the Message passing metric for the class. (One of the Chidamber and Kemerer metrics)</td>
</tr>
<tr>
<td>CBO</td>
<td>Coupling between objects</td>
<td>The value of the Coupling Between Objects metric for the class. (One of the Chidamber and Kemerer metrics)</td>
</tr>
<tr>
<td>FIN</td>
<td>Fan In</td>
<td>The value of the Fan In (Afferent coupling (Ca)) metric for the class.</td>
</tr>
<tr>
<td>FOOUT</td>
<td>Fan Out</td>
<td>The value of the Fan Out (Efferent coupling (Ce)) metric for the class.</td>
</tr>
<tr>
<td>R-R</td>
<td>Reuse Ratio</td>
<td>The value of the Reuse Ratio for the class.</td>
</tr>
<tr>
<td>S-R</td>
<td>Specialization Ratio</td>
<td>The value of the Specialization Ratio for the class.</td>
</tr>
<tr>
<td>NSUP</td>
<td>Number of Superclasses</td>
<td>The number of superclasses (excluding Object) in the hierarchy of the class. (NOC - one of the Chidamber and Kemerer metrics)</td>
</tr>
<tr>
<td>NSUB</td>
<td>Number of Subclasses</td>
<td>The number of subclasses below the class in the hierarchy.</td>
</tr>
<tr>
<td>MI</td>
<td>Maintainability Index (including comments)</td>
<td>The Maintainability Index for the class, including the adjustment for comments.</td>
</tr>
<tr>
<td>MINC</td>
<td>Maintainability Index (not including comments)</td>
<td>The Maintainability Index for the class without any adjustment for comments.</td>
</tr>
<tr>
<td>COH</td>
<td>Cohesion</td>
<td>The value of the Cohesion metric for the class.</td>
</tr>
<tr>
<td>DIT</td>
<td>Depth of Inheritance Tree</td>
<td>The value of the Depth of Inheritance Tree metric for the class. (One of the Chidamber and Kemerer metrics)</td>
</tr>
<tr>
<td>LCOM2</td>
<td>Lack of Cohesion of Methods (variant 2)</td>
<td>The value of the Lack of Cohesion of Methods (2) metric for the class. This uses the LCOM2 calculation. (One of the Chidamber and Kemerer metrics)</td>
</tr>
<tr>
<td>CCOM</td>
<td>Number of Comments</td>
<td>The number of Comments associated with the class.</td>
</tr>
<tr>
<td>CCML</td>
<td>Number of Comment Lines</td>
<td>The number of Comment Lines associated with the class.</td>
</tr>
<tr>
<td>cNLOC</td>
<td>Lines of Code</td>
<td>The number of lines of code in the class and its methods.</td>
</tr>
</tbody>
</table>

The next aspect we consider is test directness. Before we dig into test directness, we method that calls method `getMantissa`. From this case, we observe that access control modifiers influence the *visibility* of the method, so as to play a significant role in code observability. Thereby, we take access control modifiers into account to quantify code observability, where we design `is_public` and `is_static` (shown in 4th and 5th rows in Table 4.5).

The third point we raise concerns fault masking. We have observed that mutants generated in *certain locations* are more likely to be *masked* [162], i.e., the state change cannot propagate to the output of the method. The first observation is that mutants that reside in a nested class. The reasoning is similar to mutants that reside in nested sections of code, namely that a change in intermediate results does not propagate to a point where a test can pick it up. Thus, we come up with `is_nested` (in 6th row in Table 4.5). Another group of mutants is generated inside nested conditions and loops. These can be problematic because the results of the mutations cannot propagate to the output, and the tests have no way of checking the intermediate results within the method. Accordingly, we define `nested_depth` (shown in 7th row in Table 4.5) and a set of metrics to quantify the conditions and loops (shown in 8th through 13th rows in Table 4.5). The last observation is related to mutants that are inside a long method (the reason is similar to the mutants inside nested conditions and loops), thus we design `method_length` (shown in 14th row in Table 4.5).
**Listing 4.1: Example of Method `setSectionPaint` in Class `PiePlot` and its test**

```java
public void setSectionPaint(Comparable key, Paint paint) {
    this.sectionPaintMap.put(key, paint);
    fireChangeEvent(); // mutant: remove this method
}

@Test
public void testEquals() {
    PiePlot plot1 = new PiePlot();
    PiePlot plot2 = new PiePlot();
    assertTrue(plot1.equals(plot2));
    assertTrue(plot2.equals(plot1));
    // sectionPaintMap
    plot1.setSectionPaint("A", new GradientPaint(1.0f, 2.0f, Color.BLUE, 3.0f, 4.0f, Color.WHITE));
    assertFalse(plot1.equals(plot2));
    plot2.setSectionPaint("A", new GradientPaint(1.0f, 2.0f, Color.BLUE, 3.0f, 4.0f, Color.WHITE));
    assertTrue(plot1.equals(plot2));
    ...
}
```

**Listing 4.2: Example of Method `getMantissa` in Class `NumberUtils`**

```java
private static String getMantissa(final String str) {
    return getMantissa(str, str.length());
}
```

take Listing 4.3 as an instance. Listing 4.3 shows the class `Triple` from project `commons-lang-LANG_3_7`, which is an abstract implementation defining the basic functions of the object and that consists of three elements. It refers to the elements as “left”, “middle” and “right”. The method `hashCode` returns the hash code of the object. Six mutants are generated for the method `hashCode` in class `Triple`. Table 4.4 summarises all the mutants from Listing 4.3. Of those six mutants, only Mutant 1 is killed, and the other mutants are not equivalent. Through further investigation of method `hashCode` and its test class, we found that although this method has 100% coverage by the test suite, there is no direct test for this method. A direct test would mean that the test method directly invoking the method (production code) [59]. The direct test is useful because it allows to control the input data directly and to assert the output of a method directly. This example shows that test directness can influence the outcome of mutation testing, which denotes the test case angle of code observability. Previous works such as Huo and Clause [187] also addressed the significance of test directness in mutation testing. Therefore, we design two metrics, `direct_test_no.` and `test_distance` (shown in 15th and 16th row in Table 4.5), to quantify test directness. Those two metrics represent the test case perspective of code observability.

Last but not least, we take assertions into considerations. As discussed in Listing 4.1, we have observed that mutants without appropriate assertions in place (throwing exceptions is also under consideration) cannot be killed, as a prerequisite to killing a mutant is to have the tests fail in the mutated program. Schuler and Zeller [315] and Zhang and
4.3. Experimental Setup

To examine our conjectures, we conduct an experiment using six open-source projects. We recall the research questions we have proposed in Section 4.1:

- **RQ4.1:** What is the relation between testability metrics and the mutation score?
- **RQ4.2:** What is the relation between observability metrics and the mutation score?
- **RQ4.3:** What is the relation between the combination of testability and observability metrics and the mutation score?
- **RQ4.4:** To what extent does removal of anti-patterns based on testability and observability help in improving the mutation score?

Mesbah [384] also drew similar conclusion to ours. Accordingly, we come up with three metrics to quantify assertions in the method, assertion_no., assertion-McCabe_Ratio and assertion_density (shown in 17th - 19th rows in Table 4.5). The assertion-McCabe_Ratio metric [59] is originally proposed to measure test completeness by indicating the ratio between the number of the actual points of testing in the test code and the number of decision points in the production code (i.e., how many decision points are tested). For example, a method has a McCabe complexity of 4, then in the ideal case, we would expect 4 different assertions to test those linear independent paths (in this case this ratio would be 1), but if the ratio is lower than 1, it could be an indication that either not all paths are tested, or that not all paths are tested in a direct way. The assertion_density metric [217] aims at measuring the ability of the test code to detect defects in the parts of the production code that it covers. We include those two metrics here as a way to measure the quality of assertions. These three metrics are proposed based on the test case perspective of code observability.

To sum up, Table 4.5 presents all the code observability metrics we propose, where we display the name, the definition of each metric, and the category.
Table 4.5: Summary of code observability metrics

<table>
<thead>
<tr>
<th>#</th>
<th>Name</th>
<th>Definition</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>is_void</td>
<td>whether the return value of the method is void or not</td>
<td>return type</td>
</tr>
<tr>
<td>2</td>
<td>non_void_percent</td>
<td>the percent of non-void methods in the class</td>
<td>(class-level)</td>
</tr>
<tr>
<td>3</td>
<td>getter_percentage</td>
<td>the percentage of getter methods in the class</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>is_public</td>
<td>whether the method is public or not</td>
<td>access control modifiers</td>
</tr>
<tr>
<td>5</td>
<td>is_static</td>
<td>whether the method is static or not</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>nested_depth</td>
<td>the maximum number of nested depth (MDN from Section 4.2.2)</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>(cond)</td>
<td>the number of conditions (if, if-else and switch) in the method</td>
<td>fault masking</td>
</tr>
<tr>
<td>8</td>
<td>(cond(cond))</td>
<td>the number of nested conditions (e.g., if{if{f}}) in the method</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>(cond(loop))</td>
<td>the number of nested condition-loops (e.g., if{for{f}}) in the method</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>(loop)</td>
<td>the number of loops (for, while and do-while) in the method (LOOP from Section 4.2.2)</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>(loop(cond))</td>
<td>the number of nested loop-conditions (e.g., for{if{f}}) in the method</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>(loop(loop))</td>
<td>the number of nested loop-conditions (e.g., for{for{f}}) in the method</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>method_length</td>
<td>the number of lines of code in the method (NLOC from Section 4.2.2)</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>direct_test_no.</td>
<td>the number of test methods directly invoking the method under test (production code)</td>
<td>test directness</td>
</tr>
<tr>
<td>15</td>
<td>test_distance</td>
<td>the shortest method call sequence required to invoke the method (production code) by test methods</td>
<td>test directness</td>
</tr>
<tr>
<td>16</td>
<td>assertion_no.</td>
<td>the number of assertions in direct tests</td>
<td>assertion</td>
</tr>
<tr>
<td>17</td>
<td>assertion-McCabe_Ratio</td>
<td>the ratio between the total number of assertions in direct tests and the McCabe Cyclomatic complexity</td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>assertion_density</td>
<td>the ratio between the total number of assertions in direct tests and the lines of code in direct tests</td>
<td></td>
</tr>
</tbody>
</table>

1 A getter method must follow three patterns [49]: (1) must be public; (2) has no arguments and its return type must be something other than void. (3) have naming conventions: the name of a getter method begins with “get” followed by an uppercase letter.
2 If the method is not directly tested, then its direct_test_no. is 0.
3 If the method is directly tested, then its test_distance is 0. The maximum test_distance is set Integer.MAX_VALUE in Java which means there is no method call sequence that can reach the method from test methods.

4.3.1. Mutation Testing

We adopt PIT (Version 1.4.0) [99] to apply mutation testing in our experiments. The mutation operators we adopt are the default mutation operators provided by PIT [103]: Conditionals Boundary Mutator, Increments Mutator, Invert Negatives Mutator, Math Mutator, Negate Conditionals Mutator, Return Values Mutator and Void Method Calls Mutator. We did not adopt the extended set of mutation operators provided PIT, as the operators in the default version are largely designed to be stable (i.e., not be too easy to detect) and minimise the number of equivalent mutations that they
Table 4.6: Subject systems

<table>
<thead>
<tr>
<th>PID</th>
<th>Project</th>
<th>LOC</th>
<th>#Tests</th>
<th>#Methods</th>
<th>#Mutants</th>
<th>#Total</th>
<th>#Selected</th>
<th>#Total</th>
<th>#Killed</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Bukkit-1.7.9-R0.2</td>
<td>32373</td>
<td>432</td>
<td>7325</td>
<td>2385</td>
<td>7325</td>
<td>947</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>commons-lang-LANG_3_7</td>
<td>77224</td>
<td>4068</td>
<td>13052</td>
<td>2740</td>
<td>13052</td>
<td>11284</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>commons-math-MATH_3_6_1</td>
<td>208959</td>
<td>6523</td>
<td>48524</td>
<td>6663</td>
<td>48524</td>
<td>38016</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>java-apns-apns-0.2.3</td>
<td>3418</td>
<td>91</td>
<td>429</td>
<td>150</td>
<td>429</td>
<td>247</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>jfreechart-1.5.0</td>
<td>13417</td>
<td>2175</td>
<td>34488</td>
<td>7133</td>
<td>34488</td>
<td>11527</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>pysonar2-2.1</td>
<td>10926</td>
<td>269</td>
<td>3070</td>
<td>719</td>
<td>3074</td>
<td>836</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Overall</td>
<td>467017</td>
<td>13558</td>
<td>106888</td>
<td>19790</td>
<td>106892</td>
<td>62857</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Note: Column “LOC” standing for the line of code is measured by sloccount [363]. In our experiment, we remove the methods with no generated mutant by PIT, thus resulting in the number of selected methods (#Selected).

4.3.2. SUBJECT SYSTEMS

We use six systems publicly available on GitHub in this experiment. Table 4.6 summarises the main characteristics of the selected projects, which include the lines of code (LOC), the number of tests (#Test), the total number of methods (#Total Methods), the number of selected methods used in our experiment (#Selected), the total number of mutants (#Total Mutants), and the killed mutants (#Killed). In our experiment, we remove the methods with no generated mutant by PIT, thus resulting in the number of selected methods (#Selected). These systems are selected because they have been widely used in the research domain (e.g., [187, 315, 378, 384, 392]). All systems are written in Java, and tested by means of JUnit. The granularity of our analysis is at method-level.

The results of the mutants that are killable for all of the subjects are shown in Columns 7-8 of Table 4.6. Figure 4.1a shows the distribution of mutation score among selected methods. The majority of the mutation scores are either 0 or 1. Together with Figure 4.1b, we can see that the massive number of 0s and 1s are due to the low mutant number per method. Most methods show less than 10 mutants, which is mainly due to most methods being short methods (NOS < 2 as shown in Figure 4.2). Writing short methods is a preferred strategy in practice, for a long method is a well-known code smells [70]. Besides, PIT adopts several optimisation mechanisms [101] to reduce the number of mutants. Thus, the number of mutants (#Total Mutants) shown in Table 4.6 is fewer than the actual number of generated mutants. The large number of the methods with low mutant number is an unavoidable bias in our experiment.

4.3.3. TOOL IMPLEMENTATION

To evaluate the code observability metrics that we have proposed, we implement a prototype tool (coined MUTATION OBSERVER) to capture all the necessary information from both the program under test and the mutation testing process. This tool is openly available on GitHub [390].

Our tool extracts information from three parts of the system under test (in Java): source code, bytecode, and tests. Firstly, Antlr [1] parses the source code to obtain the basic code features, e.g., is public, is static and (cond). Secondly, we adopt Apache Com-
mons BCEL [2] to parse the bytecode. Then, java-callgraph [17] generates the pairs of method calls between the source code and tests, which we later use to calculate direct
4.3. **Experimental Setup**

![Figure 4.2: Distribution of Number of Java Statements (NOS) per method](image)

Figure 4.2: Distribution of Number of Java Statements (NOS) per method

![Figure 4.3: Overview of Mutation Observer architecture](image)

Figure 4.3: Overview of Mutation Observer architecture

test no. and other test call related metrics. The last part is related to the mutation testing process, for which we adopt PIT (Version 1.4.0) [99] to obtain the killable mutant results. An overview of the architecture of Mutation Observer can be seen in Figure 6.4.
4.3.4. Design of Experiment

RQ4.1-RQ4.3

Our investigation of the relationships between testability/observability metrics and the mutation score (RQ4.1-RQ4.3) is two-fold: in the first part, we adopt Spearman's rank-order correlation to measure the pairwise correlations statistically between each metric (both testability and observability metrics) and the mutation score; in the second part, we turn the correlation problem into a binary classification problem (where we adopt Random Forest as the classification algorithm) to investigate how those metrics interact with one another.

Pairwise correlations To answer RQ4.1, RQ4.2, and RQ4.3, we first adopt Spearman’s rank-order correlation to statistically measure the correlation between each metric (both testability and observability metrics) and the mutation score of the corresponding methods or classes. Spearman’s correlation test checks whether there exists a monotonic relationship (linear or not) between two data samples. It is a non-parametric test and, therefore, it does not make any assumption about the distribution of the data being tested. The resulting coefficient $\rho$ takes values in the interval $[-1;+1]$; the higher the correlation in either direction (positive or negative), the stronger the monotonic relationship between the two data samples under analysis. The strength of the correlation can be established by classifying into “negligible” ($|\rho| < 0.1$), “small” ($0.1 \leq |\rho| < 0.3$), “medium” ($0.3 \leq |\rho| < 0.5$), and “large” ($|\rho| \geq 0.5$) [178]. Positive $\rho$ values indicate that one distribution increases when the other increases as well; negative $\rho$ values indicate that one distribution decreases when the other increases.

The mutation score is calculated by Equation 4.1 (method-level).

\[
\text{mutation score}(A) = \frac{\#\text{killed mutants in method } A}{\#\text{total mutants in method } A}
\] (4.1)

We adopt Matlab [246] to calculate the Spearman’s rank-order correlation coefficient between each metric and the mutation score. In particular, we used the statistical analysis (corr function with the option of “Spearman” in Matlab’s default package).

Interactions Except for the pairwise correlations between each metric and the mutation score, we are also interested in how those metrics interact with one another. To do so, we first turn the correlation problem into a binary classification problem. We use 0.5 as the cutoff between HIGH and LOW mutation core because 0.5 is widely used as a cutoff in classification problems whose independent variable ranges in $[0,1]$ (e.g., defect prediction [340, 377]). We consider all the metrics to predicate whether the method belongs to classes with HIGH or LOW mutation score. One thing to notice here is that building a perfect prediction model is not our primary goal. Our interest is to see which metrics and/or which combinations of the metrics contributing to the LOW mutation score by

\[2\] In the original equation for mutation score, the divisor is the number of non-equivalent. In our study, our main focus is the relation between testability/observability metrics and mutation score, rather than mutation score itself. In our previous literature review (Chapter 2), we have found that treating all mutants as non-equivalent is a common method when the mutation score is used as a relative comparison. Therefore, we do not manually analyse the equivalent mutants, and treated all mutants as non-equivalent.

\[3\] https://www.mathworks.com/help/stats/corr.html
building the prediction models. Therefore, deciding different thresholds values is outside the scope of this chapter.

For prediction, we adopt Random Forest \cite{breiman2001random} as the classification algorithm, where we use \texttt{WEKA} \cite{weka} to build the prediction model. Random Forest is an ensemble method based on a collection of decision tree classifiers, where the individual decision trees are generated using a random selection of attributes at each node to determine the split \cite{ho1995random}. Besides, Random Forest is more accurate than one decision tree, and it is not affected by the overfitting problem \cite{ho1995random}. The reasons why we adopted Random Forest rather than linear regression here are as follows: (1) Random Forest is a more advanced method, and it can usually achieve high accuracy and avoid overfitting when considering many attributes. (2) We did build the linear regression in the first place. As the linear regression model enables to predict a certain value (i.e., the mutation score), it incurs far higher cross-validation errors than Random Forest.

As our investigation includes testability and observability metrics, for each project, we compare three types of classification models: (1) a model based on merely existing testability metrics, (2) a model based on merely code observability metrics, and (3) a model based on the combination of existing and our observability metrics (overlapping metrics, e.g., \texttt{method\_length} to \texttt{NLOC}, are only considered once). In particular, we include the model based on the combination of the two aspects for further comparison: to see whether the combination of the two aspects can work better than each aspect itself. To examine the effectiveness of Random Forest in our dataset, we also consider \texttt{ZeroR}, which classifies all the instances to the majority and ignores all predictors, as the baseline. It might be that our data is not balanced, as in that one project has over 90% methods with a \texttt{HIGH} mutation score. This could entail that the classification model achieving 90% accuracy is not necessarily an effective model. In this situation, \texttt{ZeroR} could also achieve over 90% accuracy in that scenario. Our Random Forest model must thus perform better than \texttt{ZeroR}; otherwise, the Random Forest model is not suitable for our dataset.

In total, we consider four classification models: 1) \texttt{ZeroR} (i.e., the constant classifier), 2) Random Forest based on existing metrics, 3) Random Forest based on code observability metrics, and 4) Random Forest based on the combination of existing metrics and code observability metrics. To build Random Forest, \texttt{WEKA} \cite{weka} adopts bagging in tandem with random attribute selection. We use \texttt{WEKA}'s default parameters to train the Random Forest model, i.e., "-P \text{100} -I \text{100} -\text{num-slots} \text{1} -\text{K 0 -M 1.0 -V 0.001 -S 1}". To evaluate the performance of the classifier model (e.g., precision and recall), we use 10-fold cross validation \cite{bhatia2020inter}. In terms of feature importance, we apply \texttt{scikit-learn} \cite{scikit-learn} to conduct the analysis. To determine the feature importance, \texttt{scikit-learn} \cite{scikit-learn} implements “Gini Importance” or “Mean Decrease Impurity” \cite{breiman1984classification}. The importance of each feature is computed by the probability of reaching that node (which is approximated by the proportion of samples reaching that node) averaged over total tree ensembles \cite{breiman1984classification}. We use the method of \texttt{feature\_importances\_} in \texttt{sklearn.ensemble.RandomForestRegressor} \cite{scikit-learn} package to analyse the feature importance.

RQ4.4
To answer RQ4.4, we first need to establish the anti-patterns (or smells) based on these metrics. An example of an anti-pattern rule generated from the metrics is `method_length > 20` and `test_distance > 2`. In this case, it is highly likely that the method has low mutation score. To obtain the anti-pattern rules, we adopt J48 to build a decision tree [143, 301]. We consider J48 because of its advantage in interpretation over Random Forest. After building the decision tree, we rank all leaves (or paths) according to instances falling into each leaf and accuracy. We select the leaves with the highest instances and accuracy ≥ 0.8 for further manual analysis, to understand to what extent refactoring of the anti-patterns can help in improving the mutation score.

4.3.5. Evaluation Metrics
For RQ4.1, RQ4.2, and RQ4.3, to ease the comparisons of the four classification models, we consider four metrics which have been widely used in classification problems: precision, recall, AUC, and the mean absolute error. To that end, we first introduce four key notations: TP, FP, FN, and TN, which denotes true positive, false positive, false negative, and true negative, respectively.

In our case, we cannot decide which class is positive or not, or in other words, we cannot say HIGH mutation score is what we expect. The goal to use a prediction model is to investigate the interactions between those metrics or how they interact with each other. So we adopt weighted precision and recall, which also take the number of instances in each class into consideration.

**Weighted precision.** The precision is the fraction of true positive instances in the instances that are predicted to be positive: TP/(TP+FP). The higher the precision, the fewer false positives. The weighted precision is computed as follows, where \( p_{c1} \) and \( p_{c2} \) are the precisions for class 1 and class 2, and \( |c1| \) and \( |c2| \) are the number of instances in class 1 and class 2, respectively:

\[
\text{weighted precision} = \frac{p_{c1} \times |c1| + p_{c2} \times |c2|}{|c1| + |c2|} \tag{4.2}
\]

**Weighted recall.** The recall is the fraction of true positive instances in the instances that are actual positives: TP/(TP+FN). The higher the recall, the fewer false negative errors there are. The weighted recall is computed as follows, where \( r_{c1} \) and \( r_{c2} \) are the recalls for class 1 and class 2, and \( |c1| \) and \( |c2| \) are the number of instances in class 1 and class 2:

\[
\text{weighted recall} = \frac{r_{c1} \times |c1| + r_{c2} \times |c2|}{|c1| + |c2|} \tag{4.3}
\]

**AUC.** The area under ROC curve, which measures the overall discrimination ability of a classifier. An area of 1 represents a perfect test; an area of 0.5 represents a worthless test.

**Mean absolute error.** The mean of overall differences between the predicted values and actual values.
### Table 4.7: Spearman results of existing code metrics for testability

<table>
<thead>
<tr>
<th>metric</th>
<th>rho</th>
<th>p-value</th>
<th>metric</th>
<th>rho</th>
<th>p-value</th>
<th>metric</th>
<th>rho</th>
<th>p-value</th>
</tr>
</thead>
<tbody>
<tr>
<td>COMP</td>
<td>0.0398</td>
<td>2.16E-08</td>
<td>NOC</td>
<td>0.1908</td>
<td>2.154E-161</td>
<td>R-R(class)</td>
<td>-0.2524</td>
<td>3.721E-285</td>
</tr>
<tr>
<td>NOCL</td>
<td>0.1047</td>
<td>2.723E-09</td>
<td>NOA</td>
<td>0.0423</td>
<td>0.0048</td>
<td>NSUB(class)</td>
<td>-0.2634</td>
<td>0</td>
</tr>
<tr>
<td>NOS</td>
<td>-0.0139</td>
<td>0.02302</td>
<td>CAST</td>
<td>-0.1334</td>
<td>2.691E-79</td>
<td>NCO(class)</td>
<td>-0.0751</td>
<td>3.602E-26</td>
</tr>
<tr>
<td>HLTH</td>
<td>0.0518</td>
<td>5.135E-05</td>
<td>NEXP</td>
<td>0.0288</td>
<td>0.0107</td>
<td>FOUT(class)</td>
<td>-0.1037</td>
<td>9.482E-52</td>
</tr>
<tr>
<td>HVEF</td>
<td>0.0856</td>
<td>1.564E-43</td>
<td>DIT(class)</td>
<td>-0.2524</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HBUG</td>
<td>0.0518</td>
<td>2.125E-15</td>
<td>LCOM(class)</td>
<td>-0.0751</td>
<td>0.001</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CREF</td>
<td>0.0193</td>
<td>1.206E-08</td>
<td>AVCC(class)</td>
<td>0.0014</td>
<td>0.9852</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>XMET</td>
<td>0.0465</td>
<td>5.416E-29</td>
<td>S-R(class)</td>
<td>0.0016</td>
<td>0.8184</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LMET</td>
<td>-0.0221</td>
<td>0.003191</td>
<td>HBUG(class)</td>
<td>0.01982</td>
<td>3.141E-19</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NLOC</td>
<td>-0.0004</td>
<td>9.95</td>
<td>HEFF(class)</td>
<td>0.0982</td>
<td>3.141E-19</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VDEC</td>
<td>0.0281</td>
<td>7.37E-05</td>
<td>UWCS(class)</td>
<td>0.0929</td>
<td>7.37E-05</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TDN</td>
<td>0.0408</td>
<td>9.634E-09</td>
<td>INST(class)</td>
<td>0.0045</td>
<td>0.9238</td>
<td>MPC(class)</td>
<td>-0.0636</td>
<td>3.314E-19</td>
</tr>
<tr>
<td>NAND</td>
<td>0.0357</td>
<td>5.956E-48</td>
<td>PACK(class)</td>
<td>-0.1029</td>
<td>0.0001</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LOOP</td>
<td>0.0685</td>
<td>6.38E-41</td>
<td>RFC(class)</td>
<td>0.0955</td>
<td>6.38E-41</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MOD</td>
<td>0.0103</td>
<td>0.1482</td>
<td>CBO(class)</td>
<td>-0.0157</td>
<td>0.0274</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NOPR</td>
<td>0.067</td>
<td>3.01E-21</td>
<td>MI(class)</td>
<td>0.0482</td>
<td>1.141E-11</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EXCT</td>
<td>0.1125</td>
<td>9.72E-57</td>
<td>CCM(class)</td>
<td>0.1559</td>
<td>6.998E-108</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MDN</td>
<td>0.053</td>
<td>8.3E-14</td>
<td>NLOCS(class)</td>
<td>0.1056</td>
<td>1.692E-26</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EXCR</td>
<td>-0.0067</td>
<td>3.498E-06</td>
<td>F-IN(class)</td>
<td>0.0875</td>
<td>6.031E-35</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HVOL</td>
<td>0.0512</td>
<td>5.719E-13</td>
<td>LCOM2(class)</td>
<td>-0.0486</td>
<td>3.738E-13</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VREF</td>
<td>0.0446</td>
<td>3.42E-10</td>
<td>MAXCC(class)</td>
<td>-0.0178</td>
<td>3.012E-48</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Note: Column "rho" represents the pairwise correlation coefficient between each code metric and the mutation score. Column "p-value" denotes the strength of evidence for testing the hypothesis of no correlation against the alternative hypothesis of a non-zero correlation using Spearman's rank-order. For p-values, we use 0.05 as the cutoff for significance. For convenience, we highlighted the p-values higher than 0.05 by underlining; those correlation results are not statistically significant. Also, we highlight the top 4 metrics in bold face in terms of absolute value of rho.

### 4.4. **RQ4.1 - RQ4.3** TESTABILITY VERSUS OBSERVABILITY VERSUS COMBINATION

We opt to discuss the three research questions, RQ4.1, RQ4.2, and RQ4.3, together, because it gives us the opportunity to compare testability, observability, and their combination in detail.

#### 4.4.1. **SPEARMAN’S RANK ORDER CORRELATION**

**Testability**

**Findings**

Table 4.7 presents the overall results of Spearman's rank-order correlation analysis for existing code metrics. The columns of "rho" represent the pairwise correlation coefficient between each code metric and the mutation score. The p-values columns denote the strength of evidence for testing the hypothesis of no correlation against the alternative hypothesis of a non-zero correlation using Spearman's rank-order. Here we used 0.05 as the cutoff for significance. From Table 4.7, we can see that except for NOS, NLOC, MOD, EXCR, INST(class), NSUB(class), COH(class) and S-R(class) (which, for convenience, we highlighted by underlining the value), the correlation results for the metrics are all statistically significant. Overall, the pairwise correlation between each source code metric and the mutation
score is not strong ($|\rho| < 0.27$). We speculate the reason behind the weak correlations to be collinearity of these code metrics. More specifically, Spearman’s rank-order correlation analysis only evaluates the correlation between individual code metric and mutation score. Some code metrics could interact with one another. For example, a long method does not necessarily have a low mutation score. Alternatively, another example: if there are more than four loops in a long method, then the method is very likely to have low mutation score. That is also an example of the collinearity, i.e., the number of loops and the method length are highly correlated.

From Table 4.7, we can see that the highest $\rho^5$ is -0.2634 for both NSUP (class) standing for Number of Superclasses, and DIT(class), or Depth of Inheritance Tree. Followed by R–R(class), for Reuse Ratio, and HIER(class), for Hierarchy method calls. At first glance, the top 4 metrics are all class-level metrics. However, we cannot infer that class-level metrics are more impactful on the mutation score than method-level ones. In particular, it can be related to the fact that we have considered more class-level metrics than method-level ones in the experiment.

Additionally, we expected that the metrics related to McCabe’s Cyclomatic Complexity, i.e., COMP, TCC, AVCC and MAXCC would show stronger correlation to the mutation score. In fact, McCabe’s Cyclomatic Complexity has been widely considered as a powerful measure to quantify the complexity of a software program, and it is used to provide a lower bound to the number of tests that should be written [140, 157, 369]. Based on our results without further investigation, we could only speculate that McCabe’s Cyclomatic Complexity might not directly influence the mutation score.

**Summary**  We found that the pair-wise correlations between the 64 existing source code metrics and the mutation score to be not so strong ($|\rho| < 0.27$). The top 4 metrics with the strongest correlation coefficients are NSUP(class), DIT(class), R–R(class) and HIER(class).

**Observability**

**Findings**  Table 4.8 shows the overall results of Spearman’s rank-order correlation analysis for code observability metrics. From Table 4.8, we can see that except for method_length and (cond(loop)), whose $p$-value is greater than 0.05, the results of the other observability metrics are statistically significant. The overall correlation between code observability metrics and mutation score is still not strong ($<0.5$), but significantly better than existing code metrics ($<0.27$). The top five metrics are test_distance, direct_test_no., assertion-density, assertion-McCabe and assertion_no. The metrics related to test directness, i.e., test_distance (-0.4923) and direct_test_no (0.4177) are ranked first in terms of $\rho$ among all metrics that we consider (including existing code metrics in Section 4.2.2). This observation corresponds to our hypothesis in Section 4.2.3 that the methods with no direct tests are more challenging to kill mutants. In terms of $\rho$ values, the assertion related metrics are ranked after test directness related metrics; this confirms both our conjectures in Section 4.2.3 and what has been reported in the related literature [315, 384] that the quality of assertions can influence the outcome of mutation testing.

---

5In terms of absolute value.
4.4. RQ4.1 - RQ4.3 TESTABILITY VERSUS OBSERVABILITY VERSUS COMBINATION

Table 4.8: Spearman results of code observability metrics

<table>
<thead>
<tr>
<th>metric</th>
<th>rho</th>
<th>p-value</th>
</tr>
</thead>
<tbody>
<tr>
<td>is_public</td>
<td>-0.0639</td>
<td>2.35E-19</td>
</tr>
<tr>
<td>is_static</td>
<td>0.1137</td>
<td>6.29E-58</td>
</tr>
<tr>
<td>is_void</td>
<td>-0.1427</td>
<td>1.42E-90</td>
</tr>
<tr>
<td>is_nested</td>
<td>0.0466</td>
<td>5.38E-11</td>
</tr>
<tr>
<td>method_length</td>
<td>-0.0004</td>
<td>0.95</td>
</tr>
<tr>
<td>nested_depth</td>
<td>0.053</td>
<td>8.3E-14</td>
</tr>
<tr>
<td>direct_test_no</td>
<td>0.4177</td>
<td>0</td>
</tr>
<tr>
<td>test_distance</td>
<td>-0.0921</td>
<td>0</td>
</tr>
<tr>
<td>assertion_no</td>
<td>0.2898</td>
<td>0</td>
</tr>
<tr>
<td>(cond)</td>
<td>0.023</td>
<td>0.00124</td>
</tr>
</tbody>
</table>

Note: Column "rho" represents the pairwise correlation coefficient between each code metric and the mutation score. Column "p-value" denotes the strength of evidence for testing the hypothesis of no correlation against the alternative hypothesis of a non-zero correlation using Spearman's rank-order. For p-values, we use 0.05 as the cutoff for significance. For convenience, we highlighted the p-values higher than 0.05 by underlining; those correlation results are not statistically significant. Also, we highlight the top 5 metrics in bold face in terms of absolute value of rho.

Table 4.9: Random forest results of code observability metrics vs. existing metrics

<table>
<thead>
<tr>
<th>pid</th>
<th>ZeroR</th>
<th>existing</th>
<th>code observability</th>
<th>combined</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>prec. recall</td>
<td>AUC</td>
<td>err.</td>
<td>prec. recall</td>
</tr>
<tr>
<td>1</td>
<td>0.856</td>
<td>0.497</td>
<td>0.2465</td>
<td>0.927</td>
</tr>
<tr>
<td>2</td>
<td>0.913</td>
<td>0.498</td>
<td>0.1595</td>
<td>0.947</td>
</tr>
<tr>
<td>3</td>
<td>0.815</td>
<td>0.499</td>
<td>0.3015</td>
<td>0.846</td>
</tr>
<tr>
<td>4</td>
<td>0.507</td>
<td>0.483</td>
<td>0.5001</td>
<td>0.607</td>
</tr>
<tr>
<td>5</td>
<td>0.62</td>
<td>0.4712</td>
<td>0.842</td>
<td>0.843</td>
</tr>
<tr>
<td>6</td>
<td>0.726</td>
<td>0.493</td>
<td>0.3982</td>
<td>0.73</td>
</tr>
</tbody>
</table>

Note: Column "prec." represents "precision" (as shown in Section 4.3.5). Column "err." stands for "Mean absolute error" (as shown in Section 4.3.5). To make clear which model performs better than the others, we highlight the values of the model achieving the best performance among the four in bold, that of second best in underline. The 7th row marked with "all" means that the results are based on the overall database (among all projects). The 8th row marked with "dir." means that the results are based on the methods with direct tests (among all projects). The 9th row marked with "non." means that the results are based on the methods with no direct tests (among all projects).

Summary  The correlations between code observability metrics and mutation score are not very strong (<0.5); however, they are significantly better than the correlations for existing code metrics. Test directness (test_distance and direct_test_no.) takes the first place of NSUP(class) in |rho| among all metrics (including existing ones in Section 4.2.2), followed by assertion-based metrics (assertion-density, assertion-McCabe and assertion_no).

4.4.2. RANDOM FOREST  Classification effectiveness  As discussed in Section 4.3.4, we compare the four models in terms of both our code observability metrics and the existing metrics, namely:

1. ZeroR: model using ZeroR approach
2. existing: Random Forest model based on existing code metrics

3. code observability: Random Forest model based on code observability metrics

4. combined: Random Forest model based on the combination of existing metrics and code observability metrics.

The comparison of the four models is shown in Table 4.9. To make clear which model performs better than the others, we highlighted the values of the model achieving the best performance among the four in **bold**, that of second best in *underline*. For preci-
4.4. RQ4.1 - RQ4.3 Testability versus observability versus combination

sion, recall, and AUC, the model with the best performance is the one with the highest value, while for the mean absolute error, the best scoring model exhibits the lowest value. For the ZeroR model, because this model classifies all the instances to the majority (i.e., one class), the precision of the minority is not valid due to 0/0. Thus, in Table 4.9, we mark the precisions by “-“.

From Table 4.9, we can see that the Random Forest models are better than the baseline ZeroR which only relies on the majority. This is the prerequisite for further comparison. Combined achieves the best performance (in 5 out of 6 projects) compared to the existing code metrics and code observability metrics in terms of AUC; this observation is as expected since combined considered both the existing and our metrics during training, which provides the classification model with more information. The only exception is java-apns-apns-0.2.3 (pid = 4). We conjecture that the number of instances (selected methods) in this project might be too small (only 150 methods) to develop a sound prediction model. In second place comes the model based on code observability metrics, edging out the model based on existing metrics.

For the overall dataset (the 7th row marked with “all” in Table 4.9), combined takes the first place in all evaluation metrics. In second place comes the code observability, slightly better than existing. Another angle which is interesting to investigate further is the test directness. If we only consider the methods that are directly tested (the second to last row in Table 4.9), combined again comes in first, followed by the existing code metrics model. The same observation holds for the methods that are not directly tested (the last row in Table 4.9). It is easy to understand that when the dataset only considers methods that are directly tested (or not), the test directness features in our model become irrelevant. However, we can see that the difference between existing metrics and ours are quite tiny (<3.4%).

Feature importance analysis Tables 4.10 and 4.11 show the top 15 features per project (and overall) in descending order. We can see that for five out of the six projects (including the overall dataset), test_distance ranks first. This again supports our previous findings that test directness plays a significant role in mutation testing. The remaining features in the top 14 vary per projects; this is not surprising, as the task and context of these projects vary greatly. For example, Apache Commons Lang (Column “2” in Table 4.10) is a utility library that provides a host of helper methods for the java.lang API. Therefore, most methods in Apache Commons Lang are public and static; thus, is_public and is_static are not among the top 15 features for Apache Commons Lang. A totally different context is provided by the JFreeChart project (Column “5” in Table 4.10). JFreeChart is a Java chart library, whose class encapsulation and inheritance hierarchy are well-designed, so is_public appears among the top 15 features.

Looking at the overall dataset (Column “all” in Table 4.11), there are eight metrics from our proposed code observability metrics among the top 15 features. The importance of test_distance is much higher than the other features (>4.83X). In second place comes PACK(class), or the number of packages imported. This observation is easy to understand since PACK(class) denotes the complexity of dependency, and dependency could influence the difficulty of testing, especially when making use of mocking objects. Thereby, dependency affects the mutation score. Clearly, more investiga-
Table 4.12: Spearman results of test directness vs. assertions in terms of \( \rho \)

<table>
<thead>
<tr>
<th>direct_test_no</th>
<th>assertion_no</th>
<th>assertion-McCabe</th>
<th>assertion_distance</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.9604</td>
<td>0.9472</td>
<td>0.9334</td>
<td></td>
</tr>
<tr>
<td>-0.8707</td>
<td>-0.8707</td>
<td>-0.8707</td>
<td></td>
</tr>
</tbody>
</table>

Note: \( \rho \) represents the pairwise correlation coefficient between each metric in test directness category and that in assertion category (as shown in Table 4.5).

As for the methods with direct tests (Column “dir.” in Table 4.11), \texttt{is\_void} takes the first position, which indicates that it is more difficult to achieve a high mutation score for void methods. Considering the methods without direct tests (Column “non-dir.” in Table 4.11), \texttt{test\_distance} again ranks first.

Another observation stems from the comparison of the performance of assertion related metrics in the feature importance analysis and the Spearman rank order correlation results (in Section 4.4.1). For Spearman’s rank order correlation, we can see that assertion related metrics are the second significant category right after test directness (in Table 4.8 in Section 4.4.1). While in the feature importance analysis, assertion related metrics mostly rank after the top 5 (shown in Table 4.10 and Table 4.11). To further investigate the reason behind the dramatic changes of ranks for assertion related metrics, we analyse the correlations between test directness (i.e., \texttt{direct\_test\_no} and \texttt{test\_distance}) and assertion related metrics (i.e., \texttt{assertion\_no}, \texttt{assertion-McCabe} and \texttt{assertion\_distance}). Looking at the correlation results between test directness and assertion related metrics in Table 4.12, the major reason is that test directness and assertion related metrics are almost collinear in the prediction model (where \(|\rho| > 0.87\)). To put simply, there are almost no tests without assertions for the six subjects. If the method has a direct test, then the corresponding assertion no. is always greater than 1. Therefore, the ranks of assertion related metrics are not as high as we had initially expected in the feature importance analysis.

Moreover, we would like to put our observations into perspective by comparing our results with the work of Zhang et al. [378], where they have constructed a similar Random Forest model to predict killable mutant result based on a series of features related to mutants and tests. The metrics that are common to their model and ours are Cyclomatic Complexity (COMP), Depth of Inheritance Tree (DIT), \texttt{nested\_depth}, Number of Subclasses (NSUB), and \texttt{method\_length}. Only two metrics in their study, i.e., \texttt{method\_length} (in 6th place) and \texttt{nested\_depth} (in 10th place) appear in our top 15 (Column “all” in Table 4.11). Especially COMP which ranks nine in their results is not in our top 15. There are multiple reasons for the difference in results: (i) we do consider a much larger range of metrics, which provide a better explanatory power (statistically speaking) than the one in their paper; (ii) our goal is to determine patterns in production and test code that may prevent killing some mutants while Zhang et al. [378] predict if
4.5. **RQ4.4 Code Refactoring**

Our goal is to investigate whether we can refactor away the observability issue that we expect to hinder tests from killing mutants and thus to affect the mutation score. In an in-depth case study, we manually analyse 16 code fragments to understand better the interaction between testability/observability metrics that we have been investigating, and the possibilities for refactoring.

Our analysis starts from the combined model, which as Table 4.9 shows, takes the leading position among the models. We then apply Principal Component Analysis (PCA) \([366]\) to perform feature selection, which, as Table 4.13 shows, leaves us with 36 features (or metrics). Then, as discussed in Section 4.3, we build a decision tree based on those 36 metrics using J48 (shown in Figure 4.4), and select the top 6 leaves (also called end nodes) in the decision tree for further manual analysis as potential refactoring guidelines. We present the top six anti-patterns in Table 4.14.

Here, we take a partial decision tree to demonstrate how we generate rules (shown in Figure 4.5). In Figure 4.5, we can see that there are three attributes (marked as an ellipse) and four end nodes or leaves (marked as a rectangle) in the decision tree. Since we would like to investigate how code refactoring increases mutation score (RQ4.4), we only consider the end nodes labeled with “LOW” denoting mutation score<0.5. By combining the conditions along the paths of the decision tree, we obtain the two rules for “LOW” end nodes (as shown in the first column of the table in Figure 4.5). For every end node, there are two values attached to the class: the first is the number of instances that correctly fall into the node, the other is the instances that incorrectly fall into the node. The accuracy in the table is computed by the number of correct instances divided by that of total instances. As mentioned earlier, we select the top 6 end nodes from the
Figure 4.4: Overview of J48 decision tree
### 4.5. RQ4.4 Code Refactoring

#### Table 4.14: Top six anti-patterns from J48 decision tree 4.4

<table>
<thead>
<tr>
<th>Rule No.</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>test_distance &gt; 5 &amp;&amp; (loop(loop)) ≤ 0 &amp;&amp; is_nested = 0 &amp;&amp; is_public = 0 &amp;&amp; XMET &gt; 4 &amp;&amp; NOCL ≤ 9 &amp;&amp; non-void_percent ≤ 0.42</td>
</tr>
<tr>
<td>2</td>
<td>test_distance &gt; 5 &amp;&amp; (loop(loop)) ≤ 0 &amp;&amp; is_nested = 0 &amp;&amp; is_public = 0 &amp;&amp; XMET &gt; 4 &amp;&amp; NOCL &gt; 9</td>
</tr>
<tr>
<td>3</td>
<td>test_distance &gt; 5 &amp;&amp; (loop(loop)) ≤ 0 &amp;&amp; is_nested = 0 &amp;&amp; is_public = 1 &amp;&amp; NOCL ≤ 4 &amp;&amp; NOCL &gt; 0 &amp;&amp; is_static = 0 &amp;&amp; getter_percent ≤ 0.01 &amp;&amp; HBUG ≤ 0.02 &amp;&amp; method_length &gt; 3</td>
</tr>
<tr>
<td>4</td>
<td>test_distance &gt; 5 &amp;&amp; (loop(loop)) ≤ 0 &amp;&amp; is_nested = 0 &amp;&amp; is_public = 1 &amp;&amp; NOCL &gt; 4 &amp;&amp; (cond) ≤ 0 &amp;&amp; isStatic = 0 &amp;&amp; LMET ≤ 1 &amp;&amp; NOCL &gt; 8 &amp;&amp; NOPR &gt; 5 &amp;&amp; isVoid = 1</td>
</tr>
<tr>
<td>5</td>
<td>test_distance ≤ 5 &amp;&amp; is_void = 1 &amp;&amp; nested_depth ≤ 0 &amp;&amp; NOS ≤ 2 &amp;&amp; assertion-density ≤ 0.14 &amp;&amp; MOD &gt; 1</td>
</tr>
<tr>
<td>6</td>
<td>test_distance ≤ 5 &amp;&amp; is_void = 1 &amp;&amp; nested_depth ≤ 0 &amp;&amp; NOS &gt; 2 &amp;&amp; assertion-density ≤ 0.22 &amp;&amp; CREF &gt; 1 &amp;&amp; XMET &gt; 0</td>
</tr>
</tbody>
</table>

![Decision Tree Diagram](image)

**Figure 4.5: Demo of rule generation**

The decision tree, where the end nodes are ranked by the number of correct instances under the condition accuracy ≥ 0.8.

After selecting the rules, the first author of this chapter has conducted the main task of the manual analysis. If there were any questions during the manual analysis, the attempts of refactoring or adding tests are discussed among all the authors to reach an agreement. In our actual case study, we manually analyse 16 cases in total. Due to space limitations, we only highlight six cases in this chapter (all details are available on GitHub [390]). We will discuss our findings in code refactoring case by case.
4.1. **Case 1: `plot.MeterPlot::drawValueLabel` from JFreeChart**

This case (shown in Listing 4.4) is under anti-pattern Rule 1: `test_distance > 5 && (loop(loop)) ≤ 0 && is_nested = 0 && is_public = 0 && XMET > 4 && (loop) ≤ 0 && NOCL ≤ 9 && non-void_percent ≤ 0.42`. In total, there are 5 mutants generated from this method (shown in Table 4.15). All 5 mutants survive the test suite.

**Code changes** We start with `test_distance > 5` which means there is no direct test for this method. Accordingly, we add one direct test (shown in Listing 4.5).

However, Mutant 4 and 5 cannot be killed by adding the above direct test. Upon inspection, we found that Mutant 4 and 5 cannot be killed because the `DrawValueLabel(...)` method is void. In particular, this means that the changes in the state caused by the `TextUtils.drawTextAlignedString()` method (line 1158) cannot be assessed. This is indicated by `non-void_percent ≤ 0.42` in Rule 1. We then refactor the method to have it return `Rectangle2D` (shown in Listing 4.6). Also, we improve the direct test for this method in Listing 4.5 by adding a new test method (shown in Listing 4.7) to avoid the assertion roulette test smell [254, 284]. By refactoring the method to non-void and adding a direct test, all previously surviving mutants are now successfully killed.

---

**Table 4.15: Summary of mutants from Listing 4.4 (Case 1)**

<table>
<thead>
<tr>
<th>ID</th>
<th>Line No.</th>
<th>Mutator</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1146</td>
<td>removed call to java/awt/Graphics2D::setFont</td>
<td>SURVIVED</td>
</tr>
<tr>
<td>2</td>
<td>1147</td>
<td>removed call to java/awt/Graphics2D::setPaint</td>
<td>SURVIVED</td>
</tr>
<tr>
<td>3</td>
<td>1149</td>
<td>negated conditional</td>
<td>SURVIVED</td>
</tr>
<tr>
<td>4</td>
<td>1151</td>
<td>negated conditional</td>
<td>SURVIVED</td>
</tr>
<tr>
<td>5</td>
<td>1157</td>
<td>Replaced float addition with subtraction</td>
<td>SURVIVED</td>
</tr>
</tbody>
</table>

Listing 4.4: `plot.MeterPlot::drawValueLabel` (Case 1)
Listing 4.5: Direct test for Listing 4.4 (Case 1)

protected Rectangle2D drawValueLabel(Graphics2D g2, Rectangle2D area) {
    g2.setFont(this.valueFont);
    g2.setPaint(this.valuePaint);

    String valueStr = "No value";
    if (this.dataset != null) {
        Number n = this.dataset.getValue();
        if (n != null) {
            valueStr = this.tickLabelFormat.format(n.doubleValue()) + " "+ this.units;
        }
    }

    float x = (float) area.getCenterX();
    float y = (float) area.getCenterY() + DEFAULT_CIRCLE_SIZE;
    returnTextUtils.drawAlignedString(valueStr, g2, x, y, TextAnchor.TOP_CENTER);
}

Listing 4.6: Refactoring of Listing 4.4 (Case 1)

Note: we highlight the refactored parts in yellow colour.

<table>
<thead>
<tr>
<th>ID</th>
<th>Line No.</th>
<th>Mutator</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>165</td>
<td>mutated return of Object value for org/jfree/chart/util/PaintAlpha::darker to (if (x != null) null else throw new RuntimeException)</td>
<td>NO_COVERAGE</td>
</tr>
<tr>
<td>2</td>
<td>166</td>
<td>Replaced double multiplication with division</td>
<td>NO_COVERAGE</td>
</tr>
<tr>
<td>3</td>
<td>167</td>
<td>Replaced double multiplication with division</td>
<td>NO_COVERAGE</td>
</tr>
<tr>
<td>4</td>
<td>168</td>
<td>Replaced double multiplication with division</td>
<td>NO_COVERAGE</td>
</tr>
</tbody>
</table>

4.5.2. CASE 2: AXIS_SYMBOLAXIS::DRAWGRIDBANDS FROM JFreeChart

This case (shown in Listing 4.8) is under Rule 2: test_distance > 5 && (loop(loop)) ≤ 0 && is_nested = 0 && is_public = 0 && XMET > 4 && (loop) ≤ 0 && NOCL > 9. In total, 4 mutants are generated from this method (see Table 4.16). None of the mutants are killed.

Code changes It is clear that this method is private, thus, it is impossible to call this method from outside the class directly. We first refactor this method from private to public. This is revealed by is_public = 0 in Rule 2.

Then, guided by test_distance > 5 from Rule 2, we add a direct test for this method to kill all mutants (see Listing 4.10).
4. An Exploratory Study on the Impact of Code Observability on MT

```java
@Test
public void testDrawValueLabelArea() {
    MeterPlot p1 = new MeterPlot(new DefaultValueDataset(1.23));
    BufferedImage image = new BufferedImage(3, 4, BufferedImage.TYPE_INT_ARGB);
    Graphics2D g2 = image.createGraphics();
    Rectangle2D area = new Rectangle(0, 0, 1, 1);
    Rectangle2D drawArea = p1.drawValueLabel(g2, area);
    assertEquals(0.5, drawArea.getCenterX(), 0.01);
    assertEquals(18.8671875, drawArea.getCenterY(), 0.01);
    assertEquals(15.0, drawArea.getHeight(), 0.01);
    assertEquals(64.0, drawArea.getWidth(), 0.01);
}
```

Listing 4.7: Improved direct test for Listing 4.4 (Case 1)

Note: we highlight the improved parts in yellow colour.

```java
/**
 * Similar to {@link Color#darker()}.<p>
 * The essential difference is that this method maintains the alpha-channel unchanged.<br>
 * @param paint a {code Color}
 * @return a darker version of the {code Color}
 */
private static Color darker(Color paint) {
    return new Color((int)(paint.getRed() * FACTOR),
                     (int)(paint.getGreen() * FACTOR),
                     (int)(paint.getBlue() * FACTOR), paint.getAlpha());
}
```

Listing 4.8: `axis.SymbolAxis::drawGridBands` (Case 2)

4.5.3. **Case 3: builder.IDKey::hashCode FROM Apache Commons Lang**

This case (shown in Listing 4.11) is under Rule 3: test_distance > 5 && (loop(loop)) ≤ 0 && is_nested = 0 && is_public = 1 && NOCL ≤ 4 && NOCL > 0 && is_static = 0 && getter_percent ≤ 0.01 && HBUG ≤ 0.02 && method_length > 3. Only one mutant is generated for this method: a mutant that replaces the return value with (x == 0 ? 1 : 0). This mutant survives.

**Code changes** Starting with test_distance > 5, we add a direct test for this method (shown in Listing 4.12), which works perfectly to kill the mutant.

4.5.4. **Case 4: AbstractCategoryItemRenderer::drawOutline FROM JFreeChart**

This case (shown in Listing 4.13) is under Rule 4: test_distance > 5 && (loop(loop)) ≤ 0 && is_nested = 0 && is_public = 1 && NOCL > 4 && (cond) ≤ 0 && is_static
public static Color darker(Color paint) {
    return new Color((int)(paint.getRed() * FACTOR),
                     (int)(paint.getGreen() * FACTOR),
                     (int)(paint.getBlue() * FACTOR), paint.getAlpha());
}

Listing 4.9: Refactoring of Listing 4.8 (Case 2)
Note: we highlight the refactored parts in yellow colour.

```java
@Test
case(Darker) {
    paint = new Color(10, 20, 30);
    darker = PaintAlpha.darker(paint);
    assertEquals(7, darker.getRed());
    assertEquals(14, darker.getGreen());
    assertEquals(21, darker.getBlue());
}
```

Listing 4.10: Direct test for Listing 4.8 (Case 2)

= 0 && LMET ≤ 1 && NOCL > 8 && NOPR > 5 && is_void = 1. Also in this case, only 1 mutant is generated for this method. The particular change applied is the removal of the call to AbstractCategoryPlot::drawOutline. The original test suite did not kill the mutant.

**Code changes** Based on test_distance > 5, we add one direct test (as shown in Listing 4.14) for this method to kill the surviving mutant.

### 4.5.5. CASE 5: builder.ToStringStyle::setUseShortClassName FROM Apache Commons Lang

This case (shown in Listing 4.15) is under Rule 5: test_distance ≤ 5 && is_void = 1 && nested_depth ≤ 0 && NOS ≤ 2 && assertion-density ≤ 0.14 && MOD > 1. In this case, a single (surviving) mutant is generated that removes the call to builder.ToStringStyle::setUseShortClassName.

**Code changes** We can see that Rule 5 is different from the previous rule in that test_distance is less than 5, while in Rule 4 test_distance > 5. A more in-depth analysis reveals that

```java
@Override
public int hashCode() {
    return id;
}

Listing 4.11: builder.IDKey::hashCode (Case 3)
the method in Listing 4.15 is already directly invoked by the original test suite. The surviving mutant is due to the fact that there are no assertions that examine the changes after the `setUseShortClassName` method call. This situation is reflected by `assertion-density ∑ 0.14` in Rule 5. Therefore, we add assertions to assess the changes (seen in Listing 4.16), which leads to the mutant being killed.

4.5.6. **CASE 6: exception.TooManyEvaluationsException::<init> FROM Apache Commons Math**

This case (shown in Listing 4.17) is under Rule 6: `test_distance ≤ 5 && is_void = 1 && nested_depth ≤ 0 && NOS > 2 && assertion-density ≤ 0.22 && CREF > 1 && XMET > 0 && VDEC ≤ 0 && NOCL ≤ 12`. A single mutant is generated: a removal of the call to `exception.util.ExceptionContext::addMessage`. This mutant is surviving the test suite.
4.5. **RQ4.4 Code Refactoring**

Listing 4.15: `builder.ToStringStyle::setUseShortClassName` (Case 5)

```java
/**
 * <p>Sets whether to output short or long class names.</p>
 */

@Override
public void setUseShortClassName(final boolean useShortClassName) {
    // NOPMD as this is implementing the abstract class
    super.setUseShortClassName(useShortClassName);
}
```

Listing 4.16: Additional assertions for Listing 4.15 (Case 5)

```java
@Test
public void testSetUseShortClassName()
{
    assertTrue(STYLE.isUseShortClassName());
    STYLE.setUseShortClassName(false);
    assertFalse(STYLE.isUseShortClassName());
    STYLE.setUseShortClassName(true);
    assertTrue(STYLE.isUseShortClassName());
}
```

**Code changes** We found that the mutant in Line 37 cannot be killed because the function `addMessage` changes the field `List<Localizable> msgPatterns`. This field is private in the class `ExceptionContext` and there is no other way to access it. As such, our first step is to add a getter for `msgPatterns` (shown in Listing 4.18). In Rule 6, we can see that `is_void = 1` is the underlying cause since void methods could be difficult to test if no getters for private fields exist.

To kill the surviving mutant, we add one extra assertion (in a new test method) to examine the changes in `msgPatterns` (in Listing 4.19). This action is also partly evidenced by `assertion-density ≤ 0.22` in Rule 6. As assertion-density denotes the ratio between the total number of assertions in direct tests and the lines of code in direct tests, low assertion-density is a sign of insufficient assertions in the direct tests to detect the mutant.

Listing 4.17: `exception.TooManyEvaluationsException::<init>` (Case 6)

```java
/**
 * Construct the exception.
 */

public TooManyEvaluationsException(Number max) {
    super(max);
    getContext().addMessage(LocalizedFormats.EVALUATIONS);
}
```
4.5.7. RQ4.4 Summary

Based on all 16 cases that we analysed (available in our GitHub repository [390]), we found that our code observability metrics can lead to simple refactorings that enable to kill mutants that were previously not being killed. Ultimately, this leads to an increase of the mutation score:

- most cases can be easily fixed by adding direct tests if test_distance>5.
- most cases can be easily fixed by adding assertions if test_distance≤5.
- private methods must be refactored to protected/public for testing (indicated by is_public=0).
- three void methods had to be refactored to be non-void (indicated by is_void=1 and non-void_percent≤0.42).
- one void method needed an additional getter because a private field was changed (indicated by is_void=1).

4.5.8. Discussion

From the findings of RQ4.4, we can see that some code refactorings break OO design principles [81]. For instance, we suggest to change the access modifier from private to protected/public to kill the mutants; this violates the idea of Encapsulation, the ability to protect some components of the object from external entities [81]. This observation brings us to a discussion about the dilemma between OO design principles and testing and hence software testability [335]. The main concepts of OO design are centred around the features of Data abstraction, Encapsulation, Inheritance, Polymorphism, and Dynamic binding. However, some factors such as Encapsulation and Inheritance could
increase the complexity of OO systems and hence hinder testing and testability [335]. Existent literature [257, 263, 323, 385] has already addressed this dilemma. Mouchawrab et al. [257] pointed out that increasing the size of the inheritance hierarchy could increase the cost of testing due to dynamic dependencies. Singh and Saha’s work [323] has shown that Inheritance and Polymorphism increase testing effort and lower software testability. All the works above indicate that there is a trade-off between OO design features and software testability. Currently, it is up to practitioners to balance the two perspectives themselves depending on the requirements of software and their preferences.

In the context of mutation testing, a similar trade-off between OO design features and the ease of killing mutants exists. In this study, we relate the ease of killing mutants to the testability and observability. In Section 4.5.7, we found that a simple strategy to kill all the mutants is to write additional direct tests and/or assertions. However, some OO design features related to Encapsulation, such as the private access modifier (see Listing 4.8), increase the difficulty to add a direct test. Also, the void return type prevents killing the mutants generated from the immediate states that cannot propagate to the output (see Listing 4.4). As such, a very important note here is that our refactoring recommendations listed in Section 4.5.7 are centred around the anti-patterns based on the testability and observability; they do not take OO design principles into consideration. The recommendations attempt to help developers in understanding the cause of the low mutation score considering testability and observability, but not all surviving mutants are due to test quality.

Take Listing 4.8 for instance. The developer found the mutation score of this method is low, and our tool shows the low mutation score is mainly due to private access control modifier. Then, the developer can decide to ignore the surviving mutants if he cannot break Encapsulation based on the requirement. Or if this method is critical and must be well-tested according to the document, he may alter the access control modifier from private to protected/public to kill the mutants. Whether the developers make use of these testability and observability recommendations depends on their choices with regard to either (1) adding test cases [71–73] (2) refactoring the production code to kill the mutants, or (3) ignoring the surviving mutants.

4.6. Threats to Validity

External validity Our results are based on mutants generated by the operators implemented in PIT. While PIT is a frequently used mutation testing tool, our results might be different when using other mutation tools [220]. Concerning the subject systems selection, we choose six open-source projects from GitHub; the selected projects differ in size, the number of test cases and application domain. Besides, as mentioned in Section 4.3, the large number of the methods with low mutant number is an unavoidable bias in our experiment. The reason is partly due to the optimisation mechanism of PIT [101] and partly due to a large number of short methods in those projects. Nevertheless, we do acknowledge that a broad replication of our study would mitigate any generalisability concerns even further.
**Internal validity** The main threat to internal validity for our study is the implementation of the Mutation Observer tool for the experiment. To reduce internal threats to a large extent, we rely on existing tools that have been widely used, e.g., WEKA, MATLAB, and PIT. Moreover, we carefully reviewed and tested all code for our study to eliminate potential faults in our implementation. Another threat to internal validity is the disregard of equivalent mutants in our experiment. However, this threat is unavoidable and shared by other studies on mutation testing that attempt to detect equivalent mutants or not [165, 252]. Moreover, we consider equivalent mutants as a potential weakness in the software (reported by Coles [100, slide 44-52]); thereby, we did not manually detect equivalent mutants in this chapter.

**Construct validity** The main threat to construct validity is the measurement we used to evaluate our methods. We minimise this risk by adopting evaluation metrics that are widely used in research (such as recall, precision, and AUC), as well as a sound statistical analysis to assess the significance (Spearman’s rank-order correlation).

### 4.7. Related Work

The notion of *software testability* dates back to 1991 when Freedman [151] formally defined *observability* and *controllability* in the domain of software. Voas [354] proposed a dynamic technique coined propagation, infection, and execution (PIE) analysis for statistically estimating the program’s fault sensitivity. More recently, researchers have aimed to increase our collective understanding of testability by using statistical methods to predict testability based on various code metrics. A prime example is the work of Bruntink and van Deursen [89], who have explored the relationship between nine class-level object-oriented metrics and testability. To the best of our knowledge, no study uses statistical or machine learning methods to investigate the relationship between testability/observability metrics and the mutation score.

Mutation testing was initially introduced as a fault-based testing method which was regarded as significantly better at detecting errors than the covering measure approach [92]. Since then, mutation testing has been actively investigated and studied, thereby resulting in remarkable advances in its concepts, theory, technology, and empirical evidence. For more literature on mutation testing, we refer to the existing surveys of DeMillo [115], Offutt and Untch [277], Jia and Harman [197], Offutt [279] and our literature review (Chapter 2). Here we mainly address the studies that concern mutant utility [203], the efficacy of mutation testing. Yao et al. [373] have reported on the causes and prevalence of equivalent mutants and their relationship to stubborn mutants based on a manual analysis of 1230 mutants. Visser [351] has conducted an exhaustive analysis of all possible test inputs to determine how hard it is to kill a mutant considering three common mutation operators (i.e., relational, integer constants and arithmetic operators). His results show that mutant reachability, mutation operators and oracle sensitivity are the key contributions to determining how hard it is to kill a mutant. Just et al. [203] have shown a strong correlation between mutant utility and context information from the program in which the mutant is embedded. Brown et al. [88] have developed a method for creating potential faults that are more closely coupled with changes made by actual program-
4.8. **Conclusion & Future Work**

This chapter aims to bring a new perspective to software developers helping them to understand and reason about the mutation score in the light of testability and observability. This should enable developers to make decisions on the possible actions to take.
when confronted with low mutation scores. To achieve this goal, we firstly investigate the relationship between testability and observability metrics and the mutation score. More specifically, we have collected 64 existing source code quality metrics for testability, and have proposed a set of metrics that specifically target observability. The results from our empirical study involving 6 open-source projects show that the 64 existing code quality metrics are not strongly correlated with the mutation score ($|\rho| < 0.27$). In contrast, the 19 newly proposed code observability metrics, that are defined in terms of both production code and test cases, do show a stronger correlation with the mutation score ($|\rho| < 0.5$). In particular, test directness, test_distance, and direct_test_no stand out.

To better understand the causality of our insights, we continue our investigation with a manual analysis of 16 methods that scored particularly bad in terms of mutation score, i.e., a number of mutants were not killed by the existing tests. In particular, we have refactored these methods and/or added tests according to the anti-patterns that we established in terms of the code observability metrics. Our aim here is to establish whether the removal of the observability anti-patterns would lead to an increase in the mutation score. We found that these anti-patterns can indeed provide insights in order to kill the mutants by indicating whether the production code or the test suite needs improvements. For instance, we found that private methods (expressed as is_public=0 in our schema) are prime candidates to potentially refactor to increase their observability, e.g., by making them public or protected for testing purpose.

However, some refactoring recommendations could violate OO design principles. For example, by changing private to protected/public we increase observability, but we also break the idea of encapsulation. Therefore, we suggest developers make a choice between—(1) adding test cases, (2) refactoring the production code to kill the mutants, or (3) ignoring the surviving mutants—by considering the trade-off between OO design features and testability/observability.

To sum up, our chapter makes the following contributions:

1. 19 newly proposed code observability metrics
2. A detailed investigation of the relationship between testability/observability metrics and the mutation score (RQ4.1-RQ4.3)
3. A case study with 16 code fragments to investigate whether removal of the anti-patterns increases the mutation score (RQ4.4)
4. A guideline for developers to make choices when confronting low mutation scores
5. A prototype tool coined Mutation Observer (openly available on GitHub [390]) that automatically calculates code observability metrics

Future work With our tool, and since the results are encouraging, we envision the following future work: 1) conduct additional empirical studies on more subject systems; 2) evaluate the usability of our code observability metrics by involving practitioners; 3) investigate the relations between more code metrics (e.g., code readability) and mutation score.
Mutation Testing for Physical Computing

Physical computing, which builds interactive systems between the physical world and computers, has been widely used in a wide variety of domains and applications, e.g., the Internet of Things (IoT). Although physical computing has witnessed enormous realisations, testing these physical computing systems still face many challenges, such as potential circuit related bugs which are not part of the software problems, the timing issue which decreasing the testability, etc.; therefore, we proposed a mutation testing approach for physical computing systems to enable engineers to judge the quality of their tests in a more accurate way. The main focus is the communication between the software and peripherals. More particular, we first defined a set of mutation operators based on the common communication errors between the software and peripherals that could happen in the software. We conducted a preliminary experiment on nine physical computing projects based on the Raspberry Pi and Arduino platforms. The results show that our mutation testing method can assess the test suite quality effectively in terms of weakness and inadequacy.

This chapter has been published in the 18th IEEE International Conference on Software Quality, Reliability, and Security (QRS) [394].
5.1. **INTRODUCTION**

Physical computing creates a conversation between the physical world and the virtual world of the computer [282]. The recent confluence of embedded and real-time systems with wireless, sensor, and networking technologies is creating a nascent infrastructure for an educational, technical, economic, and social revolution. Fuelled by the recent adoption of a variety of enabling wireless technologies such as RFID tags, embedded sensor and actuator nodes, the Internet of Things (IoT) has stepped out of its infancy and is rapidly advancing in terms of technology, functionality, and size, with more real-time applications [166]. A good example of the IoT is wearable devices like fitness trackers that are ever getting more popular.

Modern embedded platforms, like those centred around the 8051 and Freescale microcontroller series, have seen a dramatic rise in speed and functionality. The Raspberry Pi and Arduino platforms, which were originally meant for education, are two of the most popular modern embedded platforms. They are both open-source electronics platforms based on easy-to-use hardware and software.

An equally important trend is *softwarization of hardware*. In the early days, hardware engineers had to build circuits by physically connecting electronic components using wire and soldering. More recently, *reconfigurable computing* tools provide the opportunity to compile programs written in high-level languages such as C and Java into a hardware architecture. A Raspberry Pi supports several programming languages including Python to control the General Purpose Input/output (GPIO) pins to communicate with the external devices. This means that developing a physical computing system has been simplified to the point where the hardware peripherals can easily be controlled via software without even knowing the hardware part. This trend also provides a great opportunity for applying methodologies of software engineering in physical computing, especially testing techniques.

As physical computing is maturing, testing these sensor-based applications, especially the processing programs, becomes essential. Essential, because compared to conventional software projects, the costs associated with failing physical computing systems are often even bigger, as bugs can result in real-life accidents. For example, a robotic arm might accidentally hurt the human if the programmer does not set up the initial state properly. Therefore, to develop a rigorous and sound physical computing system, a high-quality test suite becomes crucial. This brings us to *mutation testing*, a fault-based testing technique that assesses the test suite quality by systematically introducing small artificial faults [197]. It has been shown to perform well in exposing faults [144, 228, 244].

In this chapter, we propose a novel mutation testing approach for physical computing systems enabling engineers to judge the quality of their tests in an accurate way. Specifically, we define a set of mutation operators based on *common mistakes* that we observed when developing physical computing systems. We present an initial evaluation of our approach on the Raspberry Pi and Arduino platforms.

5.2. **BACKGROUND AND MOTIVATION**

We introduce basic concepts related to *physical computing* and *mutation testing*. We then motivate why mutation testing should be applied to physical computing systems.
5.2. BACKGROUND AND MOTIVATION

5.2.1. PHYSICAL COMPUTING

Most physical computing systems (and most computer applications in general) can be broken down into the following same three stages: input, processing, and output [282]. The input is about how computers sense the physical world via sensors and signals, such as buttons and speakers. While the output is where computers make changes to the world under people’s desire through various actuators, like servos, motors and LEDs. The processing procedure requires a computer (usually an embedded platform) to read the inputs and turn them into outputs.

The General Purpose Input/output (GPIO) is the primary interface that micro-controllers including Raspberry Pi use to communicate with external devices. The pins available on a processor can be programmed to be used to either accept input or provide output to external devices depending on user desires and application requirements. These pins support a variety of data handling methods, such as Analog-to-Digital conversion and interrupt handling. GPIO is also the main focus of our methodology.

Among different embedded system platforms, the Raspberry Pi is a popular one-chip computer which includes an ARM-compatible CPU, a GPU and a Secure Digital (SD) card module. Its recommended operating system for normal use is Raspbian, a free, Debian-based operating system optimised for the platform. Python is the recommended programming language and the RPi.GPIO library is used to configure GPIO pins.

Another popular micro-controller is Arduino which is also open-source and easy-to-use. Arduino boards support GPIO pins as well. The Arduino Software (IDE) runs on the Windows, MacOS, and Linux operating systems. Its programming language can be expanded through C++ libraries, and users wanting to understand the technical details can make the leap from Arduino to the AVR C programming language on which it is based. Similarly, users can also add AVR-C code directly into Arduino programs.

5.2.2. MUTATION TESTING

Mutation testing is defined by Jia and Harman [197] as a fault-based testing technique which provides a testing criterion called the mutation adequacy score. This score can be used to measure the effectiveness of a test set regarding its ability to detect faults [197]. The principle of mutation testing is to introduce syntactic changes into the original program to generate faulty versions (called mutants) according to well-defined rules (mutation operators) [279]. The benefits of mutation testing have been extensively investigated and can be summarised as (mentioned in Chapter 2): 1) having better fault exposing capability compared to other test coverage criteria [144, 228, 244], 2) being an excellent alternative to real faults and providing a good indication of the fault detection ability of a test suite [50].

5.2.3. CHARACTERISTICS OF PHYSICAL COMPUTING

Physical computing allows to build interactive physical systems through a combination of hardware and software. The following six major characteristics describe the uniqueness of physical computing [329]:

(1) Safety and security issue: physical computing systems are much more safety-critical than traditional software where small defects could have a tremendous impact on the reliability of systems upon which people’s lives and living depend. Moreover, sen-
sor networks interact closely with their physical environment and with people, posing additional security problems.

(2) Fault-tolerance: fault-tolerance is a crucial requirement for physical computing systems that manage to handle exceptions properly once a certain part does not work. E.g., sensors may fail due to surrounding physical conditions or when their energy runs out. It may be difficult to replace existing sensors; the network must be fault-tolerant such that non-catastrophic failures are hidden from the application [339].

(3) Lack of knowledge: physical computing is a multi-disciplinary domain which requires developers to create high-level software system as well as low-level embedded systems solutions. However, most embedded systems developers have an electrical engineering background, therefore, might lack basic knowledge of software engineering, especially testing techniques; which could lead to error-prone code and low-quality tests.

(4) Circuit related bugs: this type of errors is mostly due to hardware configuration, such as shorts circuits, errors in sensors, undefined states (not pulling up resistors for the input processing); these bugs could be prevented or localised by testing each component at the unit level.

(5) Timing issue: in most cases, peripherals are activated or deactivated at a particular time, e.g., systems embedded with sonic sensors only start working when the distance meets a specific condition. The timing issue decreases testability of physical computing systems as it is hard to set up the real scenarios for testing.

(6) Slow execution speed: although there is a dramatic improvement in the power and functionality of modern embedded platforms, the execution speed of these embedded platforms is still not as comparable as PCs and servers. Thereby, the processing program must be carefully designed to avoid computationally-consuming algorithms.

Motivation. We can see that physical computing systems require extremely error-free and reliable code considering the safety and security issue and fault-tolerance. The slow execution speed of embedded platforms also demands a well-designed and cost-effective processing program to be deployed ubiquitously. Moreover, the testing procedure is of utmost importance to implement high-quality and error-free programs, as well as detect circuit related bugs, and make up developers’ lack of knowledge of software engineering. Also, a weak test suite is not sufficient enough to detect the faults and cannot correctly handle the timing issue.

Taking all the characteristics of physical computing systems together, the primary challenge for physical computing systems here is: how to effectively and efficiently test these physical systems? To deal with this challenge, we are seeking to apply software engineering methodologies to the physical computing domain. In particular, mutation testing, which is well-known for its high fault-revealing effectiveness, is a viable way to help developers design better quality test suites in this highly safety critical domain. Also, mutation testing, as a fault injection technique, is an ideal method for testing the fault tolerance mechanisms with respect to a specific set of inputs the physical computing systems are meant to cope with [58].

5.3. Designing Mutation Operators

To integrate computing with the physical world via sensors and actuators, an essential component is an interface between the software (processing programs) and peripher-
als (sensors and actuators). The proliferation of sensor and actuator networks in (civilian) applications requires new approaches to handle real-time, multimedia and multi-threaded communications, such as wireless sensor network [339] and cloud computing [125]. This leads to a more complex and error-prone integration part. Therefore, when designing a mutation operator for physical computing, our main goal is to narrow down the scope of the mutation process to parts of the code that affect the communication between the software and peripherals (digital circuits\(^1\)), namely the GPIO interface. To derive the mutation operators that represents errors typically made by programmers during the implementation of the software, we first summarise common mistakes that could happen in the software based on our experience. Subsequently, we design a set of mutation operators for these common mistakes.

(1) **output value errors**: The output value is usually decided by a complex function which takes many elements such as feedback from the sensors and preferences of the user, into consideration. For example, an automatic watering system decides when to water the plants according to multiple environmental conditions, e.g., soil humidity and the amount of water configured by the user. Thus, the output could be wrong if there exists a bug in the function. More specifically, we only pay attention to the final output value generated by the function, i.e., whether the output value is high or low, regardless of the function details. For this type of the error, we derived the *OutputValueReplacement* (OVR) operator which replaces *HIGH* to *LOW* (and vice versa) in the output value.

(2) **output setting omissions**: Once a certain signal has been received/read by a peripheral, the output value should, in some cases, be reset to ensure that the peripheral can change states at a later stage. For example, a self-driving car should reduce engine output when detecting a wall, but the engine should engage again after clearing the wall. Accordingly, we designed the *OutputSettingRemoval* (OSR) operator which deletes the output setting function.

(3) **pin number errors**: The programmer may read information or send control signals using a wrong pin that she does not intend to operate. The problem typically arises during prototyping for two reasons: 1) the GPIO pins are usually on the PCB as a symmetric array without labels so that designers need to locate a pin by counting, and 2) the order of a pin on the PCB is typically different from its numerical ID in the software API, making the mapping error-prone. *PinNumberReplacement* (PNR) replaces the pin id with one of the surrounding pin ids.

(4) **input value errors**: There are usually two ways to obtain an input value. The simplest way is to check the input value at a point in time. This “polling” can potentially miss an input if the program reads the value at the wrong time. The other way of responding to a GPIO input is using edge detection. An edge is the name of a transition from *HIGH* to *LOW* (falling edge) or *LOW* to *HIGH* (rising edge). Quite often, we are more concerned by a change in state of an input than its value. One potential fault in the edge detection is to mix up the falling and rising edge. This problem is common due to the confusion brought by the variety of external devices, e.g., for the 7400 series logic chip, for instance, the 74LS107 JK flip-flop chip [338] triggers on a rising edge, while the 74HC74 D flip-flop chip [337] triggers on a falling edge. For input value mistakes, we defined the following

---
\(^1\)In this chapter, we focus on the digital circuits, where two possible states, i.e., *HIGH* and *LOW*, are considered. As this is the fundamental circuit type compared to analog.
Table 5.1: Summary of mutation operators

<table>
<thead>
<tr>
<th>Mutation operator</th>
<th>Full name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>OVR</td>
<td>Output Value Replacement</td>
<td>replace HIGH to LOW (and vice versa) in the output value</td>
</tr>
<tr>
<td>OSR</td>
<td>Output Setting Removal</td>
<td>delete the output setting function</td>
</tr>
<tr>
<td>PNR</td>
<td>Pin Number Replacement</td>
<td>replace the pin id with its surrounded pin ids</td>
</tr>
<tr>
<td>IVR</td>
<td>Input Value Replacement</td>
<td>replace HIGH to LOW (and vice versa) in the input value</td>
</tr>
<tr>
<td>EDR</td>
<td>Edge Detection Replacement</td>
<td>replace edge names among {FALLING, RISING, BOTH}</td>
</tr>
<tr>
<td>IOMR</td>
<td>I/O Mode Replacement</td>
<td>replace IN to OUT (and vice versa) in the mode setting</td>
</tr>
<tr>
<td>SIR</td>
<td>Setup Input Replacement</td>
<td>replace the input value from \textit{PUD	extunderscore UP} to \textit{PUD	extunderscore DOWN} (and vice versa) in setup function</td>
</tr>
<tr>
<td>SOR</td>
<td>Setup Output Replacement</td>
<td>replace the output value from HIGH to LOW (and vice versa) in setup function</td>
</tr>
<tr>
<td>SVR</td>
<td>Setup Value Removal</td>
<td>remove the initial value setting in setup function for both input and output modes</td>
</tr>
</tbody>
</table>

Two mutation operators:

- \textit{InputValueReplacement} (IVR): replaces HIGH to LOW (and vice versa) in the input value
- \textit{EdgeDetectionReplacement} (EDR): replaces FALLING to RISING (and vice versa) in the edge detection. However, sometimes, there is one more edge event called \textit{BOTH} which covers both the falling and rising edge. In this case, the replacement happens among the three edge events, e.g., replace FALLING to RISING and BOTH.

(5) I/O pin mode errors: A GPIO pin allows to define each individual pin on the chip as being in \textit{input} or \textit{output} mode. As a side-effect of pin number mistakes, the programmer might set the pin I/O mode by mistake. Thus we designed the \textit{I/O Mode Replacement (IOMR)} operator that changes \texttt{IN} to \texttt{OUT} (or vice versa).

(6) Initial setup value errors: If a pin is not “connected” to a peripheral, it will “float”. In other words, the value that is read in is undefined because it is not connected to anything. It could frequently change values as a result of receiving mains interference. To get around this, GPIO modules usually provide an option to use a pull-up (\texttt{PUD	extunderscore UP}) or pull-down (\texttt{PUD	extunderscore DOWN}) resistor to set the default value of the input. Two potential errors in this context are (1) the omission of setting up the input value or (2) initializing it with the opposite value by mistake. Similarly, for the output mode, pins can have different default output values in a single GPIO module. The initial output value affects the initial state of the peripheral that the pin is connected to, which could lead to a breakdown or unexpected activation. For instance, if the pin connected to a motor is initially set to \texttt{HIGH}, then once the module is activated, the motor is immediately activated which is supposed to be activated when the switch is on. The potential errors in output value setup are similar to the input value setup, i.e., the setup omission and the initial value mistakes. Accordingly, there are three mutation operators:

- \textit{SetupInputReplacement} (SIR): replace the input value from \texttt{PUD	extunderscore UP} to \texttt{PUD	extunderscore DOWN} (and vice versa) in setup function.
• *SetupOutputReplacement (SOR)*: replace the output value from *HIGH* to *LOW* (and vice versa) in setup function.

• *SetupValueRemoval (SVR)*: remove the initial value in setup function for both input and output modes.

**Summary**: We designed nine mutation operators (summarised in Table 5.1) to replicate common communication errors in physical computing systems.

### 5.4. **Tool Implementation**

Various modern embedded platforms contain the GPIO module, such as Arduino, BeagleBone, PSoC kits and Raspberry Pi. In this chapter, we chose Raspberry Pi and Arduino as the target platforms to implement the aforementioned mutation operators. One thing to note is that our approach should work with the other aforementioned platforms as well.

We have coined our mutation tool *MUTPHY* and implemented it in Python. The overall architecture of *MUTPHY* is shown in Figure 6.4. *MUTPHY* consists of two components, i.e., the mutation engine and the test executor. *MUTPHY* takes the program and its test suite as input. First, the mutation engine analyses the source code and marks all possible mutation points, and then the mutation generator produces all the mutants according to mutation operators. After that, the program and generated mutants together with the test suite go to the test executor where the mutation testing is performed: each mutant is executed against the test suite one by one. Finally, *MUTPHY* prints out the detailed mutant killable results. The main task of the code analyser is to analyse the test dependencies and parse the source code of the program for the mutation generator. The mutation generator contains all the mutation operators and the details of the mutants including the mutation location (line number) and the mutation operator type.

As Raspberry Pi and Arduino are the target platforms, we have created two variants of *MUTPHY*. The main differences between the two variants are inherent to the programming languages that are supported by two platforms. For Raspberry Pi, the code analyser of *MUTPHY* needs to parse Python, as Python is Raspberry Pi’s recommended programming language. As Arduino only supports C/C++, we created a C/C++ code analyser in *MUTPHY* for Arduino. Moreover, we considered *pytest* [27], a non-boilerplate alternative to Python’s standard *unittest* testing framework [40], as the test executor for both the Raspberry Pi and Arduino platforms, as it can also handle other popular Python testing libraries, e.g. *unittest* and *doctests* [7].

### 5.5. **Empirical Evaluation**

To assess the efficacy of our mutation testing approach, we conducted an experimental study using two embedded system platforms, i.e. Raspberry Pi and Arduino. We proposed the following research questions to steer our experimental study:

• **RQ5.1**: *How effective is MUTPHY in evaluating the existing test suite?* With this research question, we evaluate to what extent *MUTPHY* can effectively evaluate the quality of the existing test suite.
- **RQ5.2**: *How efficient is MutPhy in generating non-equivalent mutants?* As we designed the mutation operators based on common mistakes made by programmers, this might lead to potential *redundant* mutation operators which are subsumed by others. **RQ5.2** addresses the efficiency of MutPhy in generating non-equivalent mutants.

- **RQ5.3**: *Is it possible to kill all non-equivalent surviving mutants by adding extra test cases?* This research question focuses on non-equivalent surviving mutants and aims to assess whether our approach enables engineers to write a better test suite.

For **RQ5.1**, we determined the effectiveness of our approach based on the number of non-equivalent surviving mutants. Also, we compared our results to test coverage. To answer **RQ5.2**, we manually analysed the generated mutants to determine whether the mutant is equivalent to the original program. For **RQ5.3**, we analysed the non-equivalent surviving mutants in detail and tried to manually engineer new test cases to kill these mutants.

### 5.5.1. Case Studies with Raspberry Pi

In the first part of the experiment, we use five Raspberry Pi based projects for evaluating MutPhy. For these five projects, four are obtained from GitHub, and one is from industry (Guangzhou Kompline Electronics). The four open source projects have been manually selected from GitHub under the Raspberry Pi topic using the following process: we (1) sorted by stars (from high to low), (2) checked whether they contain “GPIO” as a keyword, (3) verified that they are implemented in Python, and (4) examined whether they can be successfully built, and (5) inspected whether they contain a test suite. Since our main focus is the GPIO interface, we only apply mutation operators on the files that use...
the GPIO library. Table 5.2 summarises the main characteristics of the selected projects.

When answering the RQs in the next sections, we will start with RQ5.2, as we need to answer non-equivalent mutants to calculate the mutation score which is part of RQ5.1.

RPLCD

The project RPLCD [66] is a Python 2/3 Raspberry Pi Character LCD library for the Hitachi HD44780 [16] controller. The main peripheral of this system is a LCD module.

Table 5.3: Mutants result of RPLCD

<table>
<thead>
<tr>
<th>MOP</th>
<th>#Generated</th>
<th>#Covered</th>
<th>#Alive</th>
<th>#Killed</th>
<th>#Equiv.</th>
<th>MS</th>
</tr>
</thead>
<tbody>
<tr>
<td>OVR</td>
<td>13</td>
<td>10</td>
<td>13</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>OSR</td>
<td>11</td>
<td>10</td>
<td>11</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>PNR</td>
<td>47</td>
<td>41</td>
<td>47</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>IVR</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>-</td>
</tr>
<tr>
<td>EDR</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>-</td>
</tr>
<tr>
<td>IOMR</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>SIR</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>-</td>
</tr>
<tr>
<td>SOR</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>-</td>
</tr>
<tr>
<td>SVR</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>-</td>
</tr>
<tr>
<td>Overall</td>
<td>72</td>
<td>62</td>
<td>72</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

Note: Column “MOP” means mutation operator. Column “#Equiv.” means the number of the equivalent mutants. Column “MS” means mutation score.

Using MUTPHY, we generated 72 mutants for the RPLCD project. This project mainly uses the GPIO.output method to write data to the LCD board, thus, only four types of mutation operators can be applied to the system: OVR, OSR, PNR and IOMR. The details of all generated mutants are presented in Table 5.3. We can see from Table 5.3 that only one equivalent mutant is generated by MUTPHY. This equivalent OSR mutant is located in a statement that, under the existing test configuration, cannot be reached.
for this LCD controlling system, the efficiency of MUTPhy in generating non-equivalent mutants is promising (RQ5.2).

While the statement coverage is 71%, the mutation score is zero. Furthermore, 86.1% of mutants are covered by the test suite, but none of the mutants is actually killed. Why then is the mutation score of this project so low? We found that the developers replaced the RPi.GPIO module of the system under test with mock objects; this allows the tests to be executed without a Raspberry Pi. As a side effect, the developers did not assess the communication between the software and peripherals for this system. The above findings indicate that compared to statement coverage, the mutation score can better represent how a test suite examines the behaviour of GPIO pins (RQ5.1).

To kill the mutants (RQ5.3), we first removed the mock objects for the RPi.GPIO module and executed the test suite on an actual Raspberry Pi. This modification led to 21 PNR and 1 IOMR mutants killed. Then, we analysed whether the remaining mutated statements are covered by the tests or not. As shown in Table 5.3, we found 83.2% non-equivalent mutants to be covered by the test suite. However, the existing test suite only calls the functions in gpio.py file, but does not check the behaviour of the GPIO pins. To address this drawback of the existing test suites, we added five test cases to examine all the pins once their states changed. To capture the state change sequence of GPIO pins, we introduced new mock objects. Different from the system developers’ mock objects, we used mock objects to increase the observability of the system under test. For instance, one method in gpio.py file called pulse_enable(), that sends a pulse signal to tell the LCD board to process the data. The method pulse_enable() calls GPIO.output three times in one pin generating a LOW-HIGH-LOW signal. Without a mock object of method GPIO.output, it is hard to tell what happens to this pin after this function call, as the starting and the ending states are both LOW. With the additional five test cases, all the non-equivalent mutants are killed.

**hcsr04sensor**

The hcsr04sensor project [60] is a Python module for measuring distance and depth with a Raspberry Pi and HC-SR04 Ultrasonic Module [16], which uses sonar to determine the distance to an object, just like bats or dolphins do. The sensor first emits ultrasound at 40,000 Hz, which travels through the air and if there is an object or obstacle on its path, the ultrasound will bounce back to the module. Considering the travel time and the speed of the sound, it calculates the distance. The HC-SR04 Ultrasonic Module has 4 pins: Ground, VCC, Trig and Echo.

Table 5.4 details the generated mutants for hcsr04sensor. In total, MUTPhy generated 41 mutants. For this system, the Raspberry Pi controls the HC-SR04 Ultrasonic Module by writing to the Trig pin and reading from Echo. As such, this control program mainly adopts GPIO.output and GPIO.input methods. This results in five types of mutants from OVR, OSR, PNR, IVR and IOMR operators. There are no equivalent mutants generated by our proposed mutation operators; this indicates MUTPhy has high efficiency in generating non-equivalent mutants (RQ5.2).

For RQ5.1, although 100% of the mutants are covered, 22% of the mutants are not detected by the test suite. Looking at the existing test suite, we found that the test suite checked all the initial settings of each GPIO pins, but lacks tests to (1) examine the pins’
Table 5.4: Mutants result of hcsr04sensor

<table>
<thead>
<tr>
<th>MOP</th>
<th>#Generated</th>
<th>#Covered</th>
<th>#Alive</th>
<th>#Killed</th>
<th>#Equiv.</th>
<th>MS</th>
</tr>
</thead>
<tbody>
<tr>
<td>OVR</td>
<td>3</td>
<td>3</td>
<td>1</td>
<td>2</td>
<td>0</td>
<td>0.67</td>
</tr>
<tr>
<td>OSR</td>
<td>3</td>
<td>3</td>
<td>1</td>
<td>2</td>
<td>0</td>
<td>0.67</td>
</tr>
<tr>
<td>PNR</td>
<td>31</td>
<td>31</td>
<td>7</td>
<td>24</td>
<td>0</td>
<td>0.77</td>
</tr>
<tr>
<td>IVR</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>EDR</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>-</td>
</tr>
<tr>
<td>IOMR</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>SIR</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>-</td>
</tr>
<tr>
<td>SOR</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>-</td>
</tr>
<tr>
<td>SVR</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>-</td>
</tr>
<tr>
<td>Overall</td>
<td>41</td>
<td>41</td>
<td>9</td>
<td>32</td>
<td>0</td>
<td>0.78</td>
</tr>
</tbody>
</table>

Note: Column “MOP” means mutation operator. Column “#Equiv.” means the number of the equivalent mutants. Column “MS” means mutation score.

5.5. Empirical Evaluation

state changes during the execution and (2) the final states after tearing down. For this project, it is important to clean up the Trig and Echo pins after use, because otherwise the distance cannot be accurately calculated by a new request to the ultrasonic sensor. This gives another indication that mutation score is a better metric of test suite quality than statement coverage, which only reveals insufficient tests for the system.

Regarding RQ5.3, we observe seven PNR mutants that are still alive; all originating from the GPIO.cleanup function. To kill these mutants, we need to add two additional assertions at the point just after the pins are torn down which means the pins are not used anymore. Once the pins are torn down, they cannot be read from or written to anymore, so the assertions expect exceptions when trying to read those pins.

The other two alive mutants, one of type OVR and one other of type OSR, are located on the same line, more precisely when calling the GPIO.output function. Similar to the pulse_enable() method in project RPLCD, this GPIO.output function is meant to send a LOW value, the first stage of the pulse signal. We follow a similar strategy in that we try to introduce mock objects to increase the observability, but this modification led to a syntax error: a local variable sonar_signal_on is referenced before assignment. Through further investigation, we found that this local variable is only assigned right after the Echo pin detects a HIGH signal via the GPIO.input function, while in the situation with mocks, the GPIO.input function is not actually invoked. This leaves us in the situation that if we do not introduce mock objects, the state change of this GPIO.output function cannot be observed, while if we do introduce mock objects, there is a syntax error.

The aforementioned observation is a case of a snarled method, a term coined by Feathers to describe a method dominated by a single large, indented section [138]. Feathers suggest to perform an extract method refactoring to move all the statements related to the pulse signal into a separate method [138]. In doing so, we create a function pulse_enable() and we separate responsibilities of this snarled method. As a result, we can easily test the state change caused by the target GPIO.output function without affecting the remaining part. For these two mutants, it is hard to derive new tests to kill them without refactoring the original production code. Through refactoring, the statement where the mutants are
located is moved from a long method to a short one, thus, improving the observability of the state change made by the statement. This raises an interesting speculation: the testability of the production code [254] could have an influence on the test suite’s mutation score. In Voas et al.’s work [355], they proposed that software testability could be defined for different types of testing, such as data-flow testing and mutation testing. Their work inspires us to explore the relationship of software testability and mutation testing in the future work.

*jean-pierre*

The project *jean-pierre* [94] is a little DIY robot based on the Raspberry Pi Zero W [29]. It uses a camera to scan food barcodes: it fetches information about the product from the OpenFoodFacts API [25] and adds it to a grocery list that the user can manage from a web interface. Once an object is successfully added to the grocery list, a buzzer makes two beeps. This system consists of three components: a Raspberry Pi Zero W, a Raspberry Pi Camera Module [28] and a buzzer. The main use of the GPIO pins in this project is to control the buzzer (*buzzer.py* file).

Table 5.5: Mutants result of *jean-pierre*

<table>
<thead>
<tr>
<th>MOP</th>
<th>#Generated</th>
<th>#Covered</th>
<th>#Alive</th>
<th>#Killed</th>
<th>#Equiv.</th>
<th>MS</th>
</tr>
</thead>
<tbody>
<tr>
<td>OVR</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>OSR</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>PNR</td>
<td>6</td>
<td>0</td>
<td>6</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>IVR</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>-</td>
</tr>
<tr>
<td>EDR</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>-</td>
</tr>
<tr>
<td>IOMR</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>SIR</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>-</td>
</tr>
<tr>
<td>SOR</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>-</td>
</tr>
<tr>
<td>SVR</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>-</td>
</tr>
<tr>
<td>Overall</td>
<td>11</td>
<td>0</td>
<td>11</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Note: Column “MOP” means mutation operator. Column “#Equiv.” means the number of the equivalent mutants. Column “MS” means mutation score.

As the buzzer only has one function, i.e., `beep()`, it mainly adopts the `GPIO.output` function. When running our tool, 11 mutants are generated (shown in Table 5.5). For RQ5.2, no equivalent mutant is generated, which shows MUTPHY’s high efficiency in generating non-equivalent mutants. For RQ5.1, we can see that the mutation score is 0 while the statement coverage is 41%. Although the statement coverage is 41%, none of the generated mutants is covered by the test suite. Closer inspection revealed that there are no tests in the existing test suite that are specifically designed to test the communication of the software and the buzzer. We can see that the mutation score enables to evaluate how the test suite examines the integration part of the software and peripherals in physical computing systems, while the test coverage cannot.

To kill the mutants (RQ5.3), we first added a test case to cover the mutants without assertions. Once the mutated statements are covered, i.e., the statement coverage reaches 100%, the six alive PNR and one alive IOMR mutants are killed. These seven mutants can easily be detected once the mutated GPIO pins are invoked, because the
RPi.GPIO module throws exceptions if these pins are either not initialised or initialised incorrectly. For instance, GPIO8 pin is called without initialisation, or GPIO9 pin is written to HIGH after being initialised to input mode. Then, to kill the remaining four surviving mutants, we again introduced mock objects to assess each state change made by the GPIO.output function. By designing effective test oracles to test the state change of the GPIO pins using mock objects, all the mutants are killed.

**gpizero**

The project gpizero [308] is a simple interface to GPIO devices with Raspberry Pi, which requires minimal boilerplate code to get started. This project is developed by the Raspberry Pi Foundation. This library provides many simple and obvious interfaces for the essential components, such as LED, Button, Buzzer, sensors, motors and even a few simple add-on boards.

Table 5.6: Mutants result of gpizero

<table>
<thead>
<tr>
<th>MOP</th>
<th>#Generated</th>
<th>#Covered</th>
<th>#Alive</th>
<th>#Killed</th>
<th>#Equiv.</th>
<th>MS</th>
</tr>
</thead>
<tbody>
<tr>
<td>OVR</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>OSR</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>PNR</td>
<td>68</td>
<td>68</td>
<td>0</td>
<td>68</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>IVR</td>
<td>6</td>
<td>6</td>
<td>0</td>
<td>6</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>EDR</td>
<td>19</td>
<td>19</td>
<td>0</td>
<td>19</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>IOMR</td>
<td>14</td>
<td>14</td>
<td>0</td>
<td>14</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>SIR</td>
<td>8</td>
<td>8</td>
<td>0</td>
<td>8</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>SOR</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>SVR</td>
<td>5</td>
<td>5</td>
<td>1</td>
<td>4</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Overall</td>
<td>125</td>
<td>125</td>
<td>1</td>
<td>124</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

Note: Column “MOP” means mutation operator. Column “#Equiv.” means the number of the equivalent mutants. Column “MS” means mutation score.

Table 5.6 shows the 125 mutants generated by MUTPHY. For RQ5.2, there is only one equivalent mutant generated by MUTPHY. This equivalent mutant of type SVR stems from the initial value being removed from the setup function, yet with the default output value being the same as the initial value, there is an equivalence. For RQ5.1, the mutation score of this project is 1, which shows the existing test suite is adequate to detect all the mutants. One necessary condition for such a high mutation score is high test coverage. We can see that the statement coverage of the existing test suite is 97% and all the mutated statements are covered by the test suite. Moreover, there are 302 test cases in the existing test suite. Looking at the tests in detail, we found that each test case not only examines the basic information of the pin under test, i.e., the pin number and the pin state, but also other possible settings of the pin, e.g., I/O pin mode and resistor state. As the mutation score of this project has already achieved 1, there is no need for us to add extra tests to enhance the test quality (RQ5.3). From project gpizero, we can conclude that the test suite can indeed achieve 100% mutation score when the GPIO pins are taken into consideration in tests and test oracles are carefully designed.
This subject is a four-wheel robot, which has been designed and developed for industrial use (as shown in Figure 5.2). The robot is capable of moving pie-shaped objects from one place to another. During the movement, the robot may optionally rotate the object by at most $2\pi$ rad, and the four wheels can move it in six directions (as presented in Figure 5.3). The robot includes one Raspberry Pi 2, five photoelectric sensors, two DC motors, four stepper motors and three servos. The photoelectric sensors are mainly used to align the robot in specific positions (e.g., the starting point and the destination) based on differently coloured regions. The four stepper motors are responsible for the movement of the four wheels. As for the two DC motors, one drives the vertical movement of the robotic arm; the other is for the rotation of the arm. The three servos are used to control the action of the claw to grab the pie-shaped objects. The control system of
the robot consists of two parts, the chassis (chassis.py) and the arm (arm.py). The chassis part has 13 functions, and the arm part consists of 13 functions. The entire system's footprint comprises 337 lines of code. To set up a safe environment for testing, there is one test track with black and white lines designed for the robots. All the test cases are based on this test track. The test suite for the four-wheel robot system consists of 15 test cases totalling 243 lines of code. The statement coverage of the test suite is 96.5%.

Using MUTPHY, we generated 371 mutants. The summarised result of all generated mutants is presented in Table 5.7. For RQ5.2, we found there are 10 equivalent mutants generated by MUTPHY. Similar to project gpiozero, all the equivalent mutants are of type SVR, where the initial value assignment in the setup function is removed. The cause of the equivalence is also similar: the initial default value is the same as the explicitly set initial value. Although these mutants are equivalent to the original program, explicitly setting the initial value in the setup function is still recommended because different embedded platforms have different default values and setting the initial value can avoid unexpected initial states. In conclusion, for the four-wheel robot system, the efficiency of MUTPHY in generating non-equivalent mutants is high (97.3%).

For RQ5.1, the overall mutation score is 0.83, which is lower than the statement coverage (96.5%). The three mutation operators with the highest mutation score are IOMR (1), PNR (0.91) and IVR (0.81). The first two mutation operators are easier to be killed than the others because these mutants can be detected once the mutated GPIO pins are
invoked: in most cases, these pins are not initialised or initialised correctly (e.g., replace the output mode to the input mode). The 20 alive mutants from PNR are because of insufficient assertions in the tests suite; these missing assertions are needed to check the mutated statements. For IVR, as the input pins of the robots are connected to photoelectric sensors that are used to align the robot, most IVR mutants are easily killed if the robot does not reach the specific position by reading the un-mutated photoelectric sensors’ states. For the four alive IVR mutants, one is due to uncovered statements; the other three are due to poor test design.

The three mutation operators with lowest mutation score are SIR (0), SVR (0.08) and SOR (0.46). The reason why none of the SIR mutants is killed is that the corresponding pins are connected to the peripherals (in particular, the photoelectric sensors) with very high resistors; this means the replacement of initial input value (PUD_UP or PUD_DOWN) cannot affect the overall potential. These alive mutants cannot be killed in this case, and even adding new tests would not make a difference. For SVR, the five alive non-equivalent mutants are due to insufficient assertions of the tests suite: the existing test suite does not examine all the initial states of the GPIO pins. The low mutation score of the SOR operator is due to inadequate tests that do not examine the initial states of the GPIO pins once the program starts.

The mutation score of mutants generated from OVR and OSR are 0.69 and 0.63, which is lower than we expected. The alive mutants of these two operators are due to meaningless feedback produced by the control program, and the test oracles are based on these feedback messages. For instance, the function \texttt{lift()} in \texttt{arm.py} lifts the arm for a given direction (up or down) and a period. Once the \texttt{lift()} call is finished, the function returns the input direction. This kind of feedback does not reflect the actual states of the GPIO pins. Thus, the corresponding tests can never fail. To kill these surviving mutants, we replaced \texttt{GPIO.output} functions with mock objects to assess intermediate states of the target pins. For the five mutants that are located in the method \texttt{lift()}, introducing mock objects enables to effectively detect these mutants. However, the 17 other mutants cannot be easily killed by making use of mock functions. These 17 mu-

---

**Table 5.7: Mutants result of four-wheel robot**

<table>
<thead>
<tr>
<th>MOP</th>
<th>#Generated</th>
<th>#Covered</th>
<th>#Alive</th>
<th>#Killed</th>
<th>#Equiv. MS</th>
</tr>
</thead>
<tbody>
<tr>
<td>OVR</td>
<td>32</td>
<td>32</td>
<td>10</td>
<td>22</td>
<td>0</td>
</tr>
<tr>
<td>OSR</td>
<td>32</td>
<td>32</td>
<td>12</td>
<td>20</td>
<td>0</td>
</tr>
<tr>
<td>PNR</td>
<td>235</td>
<td>235</td>
<td>20</td>
<td>215</td>
<td>0</td>
</tr>
<tr>
<td>IVR</td>
<td>21</td>
<td>20</td>
<td>4</td>
<td>17</td>
<td>0</td>
</tr>
<tr>
<td>EDR</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>IOMR</td>
<td>19</td>
<td>19</td>
<td>0</td>
<td>19</td>
<td>0</td>
</tr>
<tr>
<td>SIR</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>SOR</td>
<td>13</td>
<td>13</td>
<td>7</td>
<td>6</td>
<td>0</td>
</tr>
<tr>
<td>SVR</td>
<td>16</td>
<td>16</td>
<td>15</td>
<td>1</td>
<td>10</td>
</tr>
</tbody>
</table>

Overall 371 370 71 300 10 0.83

Note: Column “MOP” means mutation operator. Column “#Equiv.” means the number of the equivalent mutants. Column “MS” means mutation score.
tants reside in complicated methods with loops and input detections. Similar to project hcsr04sensor, the intermediate changes cannot be easily captured and observed by introducing mock objects, as the sequence of the method calls is uncertain (another case of a snarled method [138]). Thus, we need to refactor the original control program by moving the related GPIO.output function calls into new methods; this enabled us to design accurate test oracles to examine the state changes.

For RQ5.3, we managed to kill the 51 non-equivalent alive mutants by adding and improving test cases. The remaining 20 non-equivalent surviving mutants cannot be killed by simply adding tests. Among the 20 mutants, 17 mutants can be killed by refactoring the production code. This observation strengthens our earlier assumption that the mutation score could be influenced by the testability of the production code. The other three non-killable SIR mutants are caused by the peripherals. More precisely, for the affected circuits the overall potential cannot be changed by pulling up or down resistor, as the resistor of peripherals is too high to be changed by the Raspberry Pi’s function. This type of stubborn mutants is unique to physical computing systems when compared to conventional software; it also increases the difficulty of testing physical computing systems. We suggest to classify this type of stubborn mutants as equivalent mutants, as the peripherals are part of the system, and generally, this part is not likely to change once the system is built up.

5.5.2. Case Studies with Arduino

The second part of our experiment targets the Arduino platform. The Arduino based system is taken from a lab session of an Embedded Software course for second-year undergraduate students at Delft University of Technology. The system is a robot that uses a camera instead of light or IR sensors to follow a line. It is shown in Figure 5.4 and is composed of of three components, each with a different role:

1. Smartphone: the camera of the smartphone is mounted on the robot makes images of the floor in front of the robot where the line should be detected;

2. Laptop: the laptop runs the Robot Operating System (ROS) core [281] and performs line detection on the images of the smartphone;

3. Arduino-based robot: the robot has to follow the line on the ground. This part includes one LCHB-100 H-bridge [20], one Arduino Mega ADK [55], one HC-05 Bluetooth dongle and one HC-SR04 ultrasonic sensor.

The students are required to implement the control program for the Arduino board and the line detection program based on ROS in groups of two. We collected implementations from four groups (the average LOC is 122.5 measured by sloccount[363]), and then the teaching assistant was asked to design test suites for those implementations. The main purpose of the test suites are to examine the five behaviours of the robot, i.e., going straight, turning left, turning right, stopping when there is an obstacle in front and stopping when no image is received. However, since the implementations of different groups are different from each other, we have to adjust the details of the tests to make them pass for further mutation testing. The statement coverage of the test suite is 100%.
The testing system is expected to be as isolated as possible from the program under test. In particular, the testing system should monitor the GPIO signals while keeping the code untouched. However, since the requirements of the student codes do not include the testing part, most of them cannot be tested without altering the codes. The reasons are as follows: first of all, the Arduino platform does not support multi-process nor multi-threading and thus only allows one main loop during execution. For the line-follower robot, the Arduino control program needs to be running continuously to receive operation signals from the PC as a client. Secondly, the test execution should be independent of the control program as a second process. In order to not introduce another process, we have to alter the students’ code by adding test cases in the same program. This results in modifications and uncertainties in the control program. Therefore, we worked around the software limitation by adding a hardware monitor as shown in Figure 5.5. More specifically, we used another Arduino board (Arduino Uno [56]) to monitor the pin states of the control board of the line-follower robot.

The hardware monitor picks up two types of signals from the system under test.

- **Pulse Width Modulation (PWM) signals for the two DC motors for the wheels.** Each DC motor occupies a pair of PWM channels for the two rotational directions (controlled via LCHB-100 H-bridge). Therefore, the two DC motors take four PWM channels in total. We program the monitor hardware to sample the signals from the four channels at regular intervals. Thus, we can know whether the signal is high or low at each interval. We then approximate the duty cycle by calculating the ratio between the number of high signals and that of all signals. For instance, there are 100 high signals out of 500 detected in five seconds for one PWM channel. Thus, the approximated duty cycle is 20%.
5.5. **Empirical Evaluation**

![Layout of test setup of line-follower robot](image)

Figure 5.5: Layout of test setup of line-follower robot

- **Standard digital signals from the ultrasonic distance sensor.** The sensor (HC-SR04) has a trigger pin and an echo pin. The trigger pin is used to emit ultrasound at 40,000 Hz, and the ultrasound signal is received in the echo pin. A test may override the echo signal of the sensor to create a simulated situation in which the robot detects a wall or an obstacle. The trigger pin is programmed to send an ultrasound continuously in this robot, which is independent of the simulation, so we use a single channel to emulate the echo signal.

To fully automate the testing process, we removed the chassis part from the Arduino-based robot, which does not influence the states of the PWM channels but prevents the robot from moving physically. Because our test oracles are based on the PWM signals of the DC motors to examine the robot’s behaviour without the information of the physical location. For example, we designed the assertion for the robot turning left as `right_fwd_pwm > right_fwd_pwm`, where the forward PWM signal of the right motor is greater than that of the left motor. As a consequence, the whole mutation testing process is automated and requires no human observations.

**RESULT**

The overall mutation scores of the four implementations are quite similar, i.e., 0.34, 0.36, 0.39 and 0.40. The test suites examine the five movements of the robots; they are almost the same for the four student projects that we consider. Table 5.8 summarises the mutants for these four implementations. We observe that 416 mutants have been generated. We did not find equivalent mutants amongst the generated mutants (RQ5.2). This
Table 5.8: Mutants result of line-follower robot

<table>
<thead>
<tr>
<th>MOP</th>
<th>#Generated</th>
<th>#Covered</th>
<th>#Alive</th>
<th>#Killed</th>
<th>#Equiv. MS</th>
</tr>
</thead>
<tbody>
<tr>
<td>OVR</td>
<td>38</td>
<td>38</td>
<td>26</td>
<td>12</td>
<td>0</td>
</tr>
<tr>
<td>OSR</td>
<td>34</td>
<td>34</td>
<td>25</td>
<td>9</td>
<td>0</td>
</tr>
<tr>
<td>PNR</td>
<td>298</td>
<td>298</td>
<td>184</td>
<td>114</td>
<td>0</td>
</tr>
<tr>
<td>IVR</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>EDR</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>IOMR</td>
<td>36</td>
<td>36</td>
<td>19</td>
<td>17</td>
<td>0</td>
</tr>
<tr>
<td>SIR</td>
<td>4</td>
<td>4</td>
<td>2</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>SOR</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>SVR</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Overall</td>
<td>416</td>
<td>416</td>
<td>261</td>
<td>155</td>
<td>0</td>
</tr>
</tbody>
</table>

Note: Column “MOP” means mutation operator. Column “#Equiv.” means the number of the equivalent mutants. Column “MS” means mutation score.

is likely due to the control program of the Arduino being quite simple: it is mainly a signal receiver for the ROS core. The key program, the image processing program, on the other hand, is located on the PC side.

For RQ5.1 we note that while the statement coverage of the test suite is 100%, the overall mutation score is 0.37. Further investigation of the test suite leads us to the fact that the existing test suite lacks assertions to examine all the target pins. In fact, the test suite only checks the states of two pins which control the forward direction of the motors (i.e. the 1FWD and 2FWD ports in the LCHB-100 H-bridge). Ideally, the test suite should check the four pins connected to the other ports of the LCHB-100 H-bridge.

To kill the alive mutants (RQ5.3), we added four assertions in each test case to ensure the correct states of the pins connected to the LCHB-100 H-bridge that controls the movement of the motors. This improvement resulted in 201 mutants being killed. However, there are still 60 mutants surviving after the modification. These 60 mutants are hard to kill due to the limitations of our test environment setup. Among the 60 stubborn mutants, 20 mutants are related to a pin that the hardware monitor did not track. This pin is to control an LED which students mostly used for debugging purposes. These 20 mutants could be killed if we monitor the states of the LED pin and add specific assertions for it. The remaining 40 mutants are hard to kill because our test environment can only monitor the pin states of the robot. This means that we cannot further check the other settings of the pins, e.g., the pin mode and resistor state, as we can do in the Raspberry Pi platform. This type of stubborn mutants is different from the previously observed stubborn mutants in the hcsr04sensor and four-wheel robot projects, where the stubbornness was due to software testability issues. As mentioned in Section 5.5.2, limitations of the Arduino platform prevent us from touching the codebase of the control program directly. The adoption of the hardware monitor treats the system as a black box; this restricts the features that we can test in this system, such as the internal settings of the pins. For this line-following robot, 90.4% non-equivalent surviving mutants can be killed by adding extra test cases, while the rest mutants are not killable due to test setups.
Table 5.9: Mutants result of all subjects

<table>
<thead>
<tr>
<th>MOP</th>
<th>#Generated</th>
<th>#Covered</th>
<th>#Alive</th>
<th>#Killed</th>
<th>#Equiv.</th>
<th>MS</th>
</tr>
</thead>
<tbody>
<tr>
<td>OVR</td>
<td>90</td>
<td>85</td>
<td>52</td>
<td>38</td>
<td>0</td>
<td>0.42</td>
</tr>
<tr>
<td>OSR</td>
<td>83</td>
<td>80</td>
<td>51</td>
<td>32</td>
<td>1</td>
<td>0.39</td>
</tr>
<tr>
<td>PNR</td>
<td>685</td>
<td>673</td>
<td>264</td>
<td>421</td>
<td>0</td>
<td>0.61</td>
</tr>
<tr>
<td>IVR</td>
<td>29</td>
<td>28</td>
<td>4</td>
<td>25</td>
<td>0</td>
<td>0.86</td>
</tr>
<tr>
<td>EDR</td>
<td>19</td>
<td>19</td>
<td>0</td>
<td>19</td>
<td>0</td>
<td>1.00</td>
</tr>
<tr>
<td>IOMR</td>
<td>73</td>
<td>72</td>
<td>21</td>
<td>52</td>
<td>0</td>
<td>0.71</td>
</tr>
<tr>
<td>SIR</td>
<td>15</td>
<td>15</td>
<td>5</td>
<td>10</td>
<td>0</td>
<td>0.67</td>
</tr>
<tr>
<td>SOR</td>
<td>18</td>
<td>18</td>
<td>9</td>
<td>9</td>
<td>0</td>
<td>0.50</td>
</tr>
<tr>
<td>SVR</td>
<td>24</td>
<td>24</td>
<td>19</td>
<td>5</td>
<td>11</td>
<td>0.38</td>
</tr>
<tr>
<td>Overall</td>
<td>1036</td>
<td>1014</td>
<td>425</td>
<td>611</td>
<td>12</td>
<td>0.60</td>
</tr>
</tbody>
</table>

Note: Column “MOP” means mutation operator. Column “#Equiv.” means the number of the equivalent mutants. Column “MS” means mutation score.

5.5.3. SUMMARY

Based on the case studies on the Raspberry Pi and Arduino platforms, we evaluated our method in terms of the efficiency in generating non-equivalent mutants (RQ5.2) and the effectiveness in evaluating the test suite quality (RQ5.1). Moreover, we also manually analysed non-equivalent surviving mutants to explore whether the mutation score can be improved by implementing new or improved tests (RQ5.3). In this section, we summarise all results of all subjects involved in our experimental study (as shown in Table 5.9) and answer the three research questions in the light of our observations.

Table 5.9 indicates that there are 1036 mutants generated in total, with the PNR mutants comprising 66.1% of the total. The EDR mutants are easiest to kill, while the OSR and SVR mutants are most difficult to kill. For RQ5.2, the overall percentage of non-equivalent mutants is 98.8%, which is quite promising. The equivalent mutants mainly stem from SVR (one from project gpiozero and ten from project four-wheel robot). However, the equivalent versions without the initial value setup are not recommended since different embedded platforms have different default values. Explicitly setting the initial value in the setup function can avoid unexpected initial states. The other equivalent one arises from OSR, which is due to dead code (see project RPLCD in Section 5.5.1). Besides, three SIR mutants are non-killable which are caused by the circuit of the peripherals. We considered these mutants as equivalent mutants in the context of physical computing systems. Even taking the three SIR mutants into consideration, the non-equivalent mutants still comprise 97.5% of the total number of mutants, showing MUTPHY has high efficiency in generating non-equivalent mutants.

For RQ5.1, compared to the statement coverage, the mutation score generated by our method can be a better indicator of test suite quality. More specifically, the mutation score can evaluate how well the test suite examines the integration part of the software and peripherals in physical computing systems, something the statement coverage does not allow. Except for project gpiozero, all the non-equivalent alive mutants reveal the inadequate test cases in the existing test suite. This is especially true for project RPLCD, for which the mutation score is 0, while the statement coverage is 71%.
For RQ5.3, 94.2% of the mutants, in most cases, it is possible to kill all non-equivalent surviving mutants by adding extra test cases, which again supports RQ5.1 that mutation score can effectively evaluate the existing test suite. The exception being 59 mutants. The Raspberry Pi case studies account for 19 of these mutants: 2 mutants from project hcsr04sensor and 17 mutants from project four-wheel robot. Killing these mutants would require refactoring the production code to increase the observability of state changes. This implies that test quality is not the only factor to determine the mutation score, as the testability of the production code can also impact the mutation score. Moreover, introducing mock objects is a double-edged sword. If the mock objects are used properly, the behaviour of the GPIO pins cannot be examined, e.g., replacing the whole RPi.GPIO module to mock objects in project RPLCD. While proper use of mock objects can improve the observability of intermediate state changes to derive high-quality tests (see project hcsr04sensor and project four-wheel robot). For Arduino, 40 mutants remain not-killed as our test setups are unable to assess the internal settings of the system. A deeper analysis of these 40 mutants reveals that factors such as the testability of the software under test and the test setup influence the mutation score. We would like to explore these potential factors in the future work to further understand mutation testing and thus improve it.

5.6. Threats to Validity

External validity: First, our results are based on the Raspberry Pi and Arduino platforms; these results might be different when using other embedded platforms. Second, concerning the subject selection, we only chose nine physical computing systems in total to evaluate our approach. Unfortunately, few physical computing systems on the Raspberry Pi and Arduino platforms with up-to-date test suites are publicly available.

Internal validity: The main threat to internal validity for our study is the implementation of MUTPHY for the experiment. To reduce internal threats to a large extent, we carefully reviewed and tested all code for our study to eliminate potential faults in our implementation. Another threat to internal validity is the detection of equivalent mutants through manual analysis. However, this threat is unavoidable and shared by other studies that attempt to detect equivalent mutants.

Construct validity: The main threat to construct validity is the measurement we used to evaluate our methods. We used the percentage of non-equivalent mutants and the mutation score as key metrics in our experiment, both of which have been widely used in other studies on mutation testing.

5.7. Related Work

There has been a great deal of work on verification and validation of embedded systems (not limited to physical computing systems) in literature. The main methodologies are static analysis (e.g., [64, 357]), dynamic analysis (e.g., [309, 352]), formal verification (e.g., [209, 223]), black-box testing (e.g., [334, 341]), and white-box testing (e.g., [233, 383]).

Most related to our approach are software-implemented fault injection (SWIFI) techniques that inject faults pre-runtime at machine code level (e.g., by changing the con-
tent of memory/registers based on specified fault models) to emulate the consequences of hardware faults [152]. One of the earliest SWIFI techniques was presented by Segall et al. [316]. Their technique's initial results showed usefulness in reducing the fault injection complexity and validation of the system. Later, in 1995, Kanawati et al. [205] proposed a flexible software-based fault and error injection system, which is useful in evaluating the dependability properties of complex systems. More recently, Arlat et al. [58] compared physical and software-implemented fault injection techniques. As shown in their results, these two types of fault injection techniques are rather complementary, while SWIFI approaches are preferable mainly due to high controllability, repeatability and cost-effectiveness. All the above works focus on hardware testing, and more specifically, the kernel layer. None of them considers the communication between the software and peripherals in physical computing systems.

Concerning the application of mutation testing in embedded systems, Zhan et al. [376], He et al. [175] and Stephan et al. [330] have addressed the notion of Simulink model mutations. They proposed a set of mutation operators explicitly for Simulink that target the run-time properties of the model, such as signal addition operators. Moreover, Enoiu et al. [133] investigated mutation-based test generation for PLC embedded software using model checking. In their work, they designed six mutation operators for PLC embedded software relying on commonly occurring faults in IEC 61131-3 software [280, 321]. Different from our approach, all these works target mutation testing at the model level, and can only be applied to one specific type of software, e.g. Simulink. Our approach, on the other hand, is based on source code, and can thus potentially apply to all kinds of embedded system platforms.

5.8. **CONCLUSION & FUTURE WORK**

Physical computing systems come with their own set of challenges. This chapter focuses on the challenge of testing these physical computing systems, with a particular focus on assessing the quality of the tests that validate the interactions between the software and the physical components. We zoom in on common mistakes that occur in these interactions and propose a novel mutation testing approach with nine mutation operators targeting these common interaction mistakes.

Our results have shown encouraging results in uncovering weaknesses in existing tests. As such, our mutation testing approach enables to guide engineers to test systems more effectively and efficiently. More specifically, for our nine case study systems our mutation testing tool generated a total of 1036 mutants of which 41% were not killed by the original test suite (and 1.2% of the overall mutants being equivalent mutants). Adding tests or reinforcing existing tests made it possible to kill 94% of the non-equivalent surviving mutants.

This chapter makes the following contributions:

- a generic mutation testing approach for physical computing systems;
- a mutation testing tool named MUTPHY working on the Raspberry Pi and Arduino platforms;
- a preliminary experiment on nine physical computing systems²;
Future work. In the future, we aim to conduct additional case studies on more realistic physical computing systems. Also, we would like to explore the complementarity between traditional mutation operators and our newly designed, yet very specific mutation operators. Finally, we also aim to explore the relationship between testability and mutation score.

\(^2\)All the tools, scripts and metadata for this experimental study are available in our GitHub repository [388].
6

**Massively Parallel, Highly Efficient, but What About the Test Suite Quality? Applying Mutation Testing to GPU Programs**

Thanks to rapid advances in programmability and performance, GPUs have been widely applied in High-Performance Computing (HPC) and safety-critical domains. As such, quality assurance of GPU applications has gained increasing attention. This brings us to mutation testing, a fault-based testing technique that assesses the test suite quality by systematically introducing small artificial faults. It has been shown to perform well in exposing faults. In this chapter, we investigate whether GPU programming can benefit from mutation testing. In addition to conventional mutation operators, we propose nine GPU-specific mutation operators based on the core syntax differences between CPU and GPU programming. We conduct a preliminary study on six CUDA systems. The results show that mutation testing can effectively evaluate the test quality of GPU programs: conventional mutation operators can guide the engineers to write simple direct tests, while GPU-specific mutation operators can lead to more intricate test cases which are better at revealing GPU-specific weaknesses.

---

This chapter has been published in the IEEE International Conference on Software Testing, Verification and Validation (ICST) 2020 [395].
6. APPLYING MUTATION TESTING TO GPU PROGRAMS

6.1. INTRODUCTION
A graphics processing unit (GPU) is a single-chip processor originally used to boost the performance of video and graphics. The recent development of massive parallelism and energy efficiency and the ease of programming using the CUDA [267] and OpenCL [259] programming models have made GPUs attractive for High-Performance Computing (HPC), which requires compute-intensive, highly parallel computation [134, 336]. Moreover, GPUs are increasingly used in some safety-critical domains, such as medical science [332] and automotive [225]. In both HPC and safety-critical domains, quality assurance of GPU applications is an important issue [158, 303].

However, it is not easy to write a correct GPU program [226]. The essential elements of GPU programs are kernels, which are functions executed on GPU cores. To efficiently schedule instances of kernels on a GPU platform, a programmer needs to face the challenges in computation and memory access that do not appear in Central Processing Unit (CPU) programs.

Regarding computation, a programmer tends to spend less effort on thread management on the CPU platform than on the GPU platform [226]. To ensure high execution efficiency, a CPU usually supports far fewer threads running in parallel than a GPU of the same generation. Since the operating system needs to spend extra time on thread scheduling when the number of threads triggered by an application exceeds the total number of cores on the CPU. As a result, a CPU programmer may focus on the correctness and efficiency of a single thread, and leave the thread collaboration issues to libraries (e.g., OpenMP) and third-party tools. In contrast, managing threads on GPUs is challenging and rarely automated as a GPU often contains thousands of cores. Development toolkits as CUDA require programmers to manage the threads explicitly.

With regard to memory access, the hardware-level facilities for memory, such as the memory hierarchy, are typically transparent to programmers for the CPU. For instance, a CPU programmer may reorder entries in an array without knowing or controlling the movement of data in between the main memory and CPU cache. In contrast, a GPU platform has a separate memory space which is isolated from the main memory of the host computer. To ensure correctness and execution efficiency, GPU programmers have to explicitly manage different types of memory including shared memory, global memory and the memory of host computer [250].

Given the increasing demand for quality assurance of GPU applications as well as the challenges in GPU programming, it becomes essential to understand to which extent a GPU program can be analysed and tested. This brings us to mutation testing, a fault-based testing technique that measures the test effectiveness in terms of fault detection [197]. Mutation testing has been shown to perform well in exposing faults compared to other test coverage criteria [144, 228, 244]. Also, mutants can act as a valid substitute to real faults [50, 201].

In this chapter, we aim to enable mutation testing for GPU programming to investigate if mutation testing can help in GPU program testing. To achieve this goal, we develop a mutation testing tool named MUTGPU especially for GPU applications in the CUDA programming model. Considering the differences between CPU and GPU programming, we design nine new GPU-specific mutation operators in addition to conventional mutation operators. We perform an empirical study involving six GPU projects...
Figure 6.1: Comparison of CPU and GPU [267]

from the CUDA SDK [6]. To steer our experimental study, we propose the following research questions:

RQ6.1 How frequently can GPU-specific mutation operators be applied, and how good is the existing test suite at killing them?

RQ6.2 How effective are conventional mutation operators in evaluating the test suite of GPU programs?

RQ6.3 How effective are GPU-specific mutation operators in evaluating the test suite of GPU programs?

RQ6.4 How do GPU-specific mutation operators compare with conventional mutation operators in terms of the improvement?

6.2. BACKGROUND

6.2.1. GPU COMPUTING

A graphics processing unit (GPU) was originally dedicated to providing a high-performance, visually rich, interactive 3D experience [234]. With rapid advances of programmability and performance, a GPU becomes a compelling platform for computationally demanding tasks in various domains [283].

GPU computing, also known as general-purpose computing on the GPU (GPGPU), is to use a GPU as a co-processor to accelerate CPUs for general-purpose scientific and engineering computing [283]. Compared to the CPU, the GPU contains many more transistors devoted to data processing rather than data caching and flow control (as demonstrated in Figure 6.1) [267]. Thus, the GPU is especially well-suited for compute-intensive, highly parallel computation.

Another important characteristic of GPUs is that the programmable units (a GPU core) follow a “SPMD” programming model: single program, multiple data [283]. More specifically, the GPU processes many elements (vertices) in parallel using the same program, and each element is independent of the other elements.
So far, there are three major GPU programming models: OpenCL (Open Computing Language), from the Khronos Group [259]; CUDA, from NVIDIA [267]; and C++ AMP, from Microsoft [164]. CUDA, as a popular GPU platform and programming model, was introduced by NVIDIA in November 2006. CUDA comes with a software environment that enables developers to program in C/C++. Except for C/C++, CUDA also supports Fortran, DirectCompute, OpenACC and Python.

6.2.2. Example of GPU Programming

In this section, we are going to demonstrate the main concepts of GPU programming along with a simple program in CUDA C\(^1\). This program is to sum two vectors \((a \text{ and } b)\) into a third vector \((c)\). In standard C, we can easily compute within a for loop shown as Listing 6.1. In CUDA C, we can accomplish the same addition on a GPU by introducing a device function. Here, we refer to the CPU and the system memory as the host and the GPU and its memory as the device. As shown in Listing 6.2, we add _global_ to sum() (Line 1 in Listing 6.2) in order to notify the compiler that this function should be compiled to run on a device instead of the host. Moreover, we need to determine how many parallel copies of sum() function (named a kernel meaning a function that executes on the device) to launch. A kernel is executed by a collection of thread blocks (called a grid), and a thread block can be further split into threads (shown in Figure 6.2). The statement `sum<<<4096,256>>>()` (Line 13 in Listing 6.2) specifies to launch 1,048,576 parallel threads (4096 blocks \(\times 256\) threads per block) for function sum.

After we launch the kernel with 1M parallel threads, the CUDA runtime assign varying values to those threads by blockIdx.x*blockDim.x + threadIdx.x \(^2\) (Line 2 in Listing 6.2), the first taking 0 and the last taking \(n-1\). Thus, all the threads run the same instructions but with different indices in parallel. Figure 6.3 presents the actual code being executed in threads.

Last but not least, in order to call the kernel, we first need to load the values of the two vectors \((a \text{ and } b)\) to the device \((\text{dev}_a \text{ and } \text{dev}_b)\) by invoking cudaMemcpy (Line 10 and 11 in Listing 6.2). The function cudaMemcpy, similar to memcpy in standard C, controls the memory copy between the device and the host. After the execution of the device function in the GPU, we then copy the output from the device \((\text{dev}_c)\) to the host \((c)\) (Line 14 in Listing 6.2).

\(^1\)CUDA C is standard C with some ornamentation to allow developers to specify which code should run on the GPU and which should run on the CPU [311]

\(^2\)Those are built-in variables in CUDA runtime that contains the value of thread index for whichever thread is currently running the device code.
6.3. Motivation

From Section 6.2, we can see there are important differences in the programming models of the CPU and the GPU. This raises the question of whether conventional mutation operators for C/C++ are enough to represent bugs in GPU programming? We observe that a test suite mutated with conventional operators may be insufficient: the GPU code with certain issues can still easily pass the test suite.

The first example is the memory management in GPU. In GPU programming, we first need to specify the number of parallel processors to launch in the device. In Listing 6.2, we can see that 1,048,576 parallel threads are used for the kernel. In this example, the size of our testing data is $2^{20}$, the exact same size as the number of parallel threads; this means that every thread can process one index of the vectors. Thereby, this test can easily pass. What if the testing data exceeds $2^{20}$ (such as $2^{25}$ shown in Listing 6.3)? For this test case, the specific parallel threads are not enough to iterate and compute each index individually. Therefore, the test in Listing 6.3 fails. This exposes a bug in the sum function: we have to modify the CUDA C code to allow certain threads to compute more than one index of the vectors (see in Listing 6.4). For Listing 6.2, existing mutation operators for C cannot target the problem related to parallel processor allocation in GPUs.

Another instance we observe is the thread management in the GPU. Different from the CPU, GPU computing involves massive parallel operations via threads; the bugs in thread management are hard to represent with conventional mutation operators. For example, Listing 6.5 presents one example of indexing bugs that could occur in GPU programs.

We would also like to mention atomic operations in GPU programming. When devel-
6. APPLYING MUTATION TESTING TO GPU PROGRAMS

6.4. MUTATION OPERATORS FOR GPU PROGRAMMING

6.4.1. GPU-SPECIFIC MUTATION OPERATORS

Mutation operators are well-defined rules to specify the syntactic changes to generate faulty versions (called mutants) [279]. They are the key to mutation testing, where good mutation operators lead to effective test suites while poor mutation operators generate many trivial and redundant mutants.

To design mutation operators, we usually follow two methodologies [121]: the first is based on fault models, and the other is to analyse the syntax of the language being mutated. In our study, we mainly follow the later guideline: we have defined GPU-specific mutation operators based on the core syntax differences between CPU and GPU programming (as discussed in Section 6.3). Meanwhile, we also consider the syntactic changes in ways that programmers could make mistakes in GPU programming (the first
6.4. Mutation Operators for GPU Programming

```c
__global__ void sum(int n, float *a, float *b, float *c){
    int i = blockIdx.x*blockDim.x + threadIdx.x;
    if (i < n){
        c[i] = a[i] + b[i];}
}
```

Listing 6.2: sum function in CUDA C

Note: we highlight the different test data setting in yellow colour.

To verify that the mutation operators we have proposed represent the common mistakes in GPU programming, we have searched for them on StackOverflow with the keyword "cuda" + issue name. For example, the keyword for the shared memory issue is “cuda shared memory”. After searching for “cuda shared memory”, we have obtained 500 search results from StackOverflow sorted by relevance. We have analysed the first 150 items. Among those, 48% are referring to bug issues.

We categorise the GPU-specific mutation operators according to the key syntactic differences between CPU and GPU programming. In the following sections, we describe the GPU-specific mutation operators we proposed by category.

Memory Management

Execution configuration  As mentioned in Section 6.2.2, we need to specify the execution configuration for a kernel function. The execution configuration defines the dimension of the grid and blocks that will be used to execute the function on the device. To de-
Applying Mutation Testing to GPU Programs

1. **sum** function in CUDA C with indexing bugs
   
   ```c
   __global__ void sum(int n, float *a, float *b, float *c){
   int i = threadIdx.x*blockDim.x + blockIdx.x;
   while (i < n){
   c[i] = a[i] + b[i];
   i += blockDim.x * gridDim.x; }
   }
   
   Listing 6.5: sum function in CUDA C with indexing bugs
   Note: we highlight the faulty parts in yellow colour.
   ```

2. **histogram** in CUDA C with atomic operation omission
   
   ```c
   __global__ void histogram(unsigned char *buffer, long size, unsigned int *histo){
   int i = blockIdx.x*blockDim.x + threadIdx.x;
   while (i < n){
   histo[buffer[i]] += 1;
   i += blockDim.x * gridDim.x; }
   }
   
   Listing 6.6: histogram in CUDA C with atomic operation omission
   Note: we highlight the faulty parts in yellow colour.
   ```

3. **termine** the number of parallel processors allocated for the kernel, many factors should be taken into consideration, for instance, the maximum size of the data and the limitation of the GPU device. For the execution configuration is unique in GPU programming, we propose the following three mutation operators to cover this aspect:

   - **alloc_swap**: to replace the number of threads with the number of blocks in parallel processor allocations (and vice versa). The same bug was posted in SO29158775 [33].

   ```c
   add <<<4096,256>>>(N, a, b, c); // original
   -- add <<<256,4096>>>(N, a, b, c); // mutant
   
   Listing 6.7: Example of alloc_swap mutator
   ```

   - **alloc_increment**: to increase the number of parallel processors (in both threads and blocks) allocated by one

   ```c
   add <<<4096,256>>>(N, a, b, c); // original
   -- add <<<4096+1,256>>>(N, a, b, c); // mutant
   
   Listing 6.8: Example of alloc_increment mutator
   ```

   - **alloc_decrement**: to decrease the number of parallel processors (in both threads and blocks) allocated by one

   ```c
   add <<<4096,256>>>(N, a, b, c); // original
   -- add <<<4096-1,256>>>(N, a, b, c); // mutant
   
   Listing 6.9: Example of alloc_decrement mutator
   ```

4. **Shared memory** The shared memory in GPU programming provides a means by which threads within a block can communicate and collaborate on computations [267]. To declare the variable in shared memory, we use the __shared__ memory space specifier in CUDA C, for instance, __shared__ float share[64]: The shared memory management is the main cause of data races and bank conflicts. The mutation operator share_removal is introduced to represent such bugs in GPU programs. There are a great deal of questions
posted on StackOverflow addressing the confusion about the shared memory in GPU programming, e.g., SO25255699 [32] and SO9488590 [36].

- **share_removal**: to remove the shared memory space specifier in variable declarations

```c
__shared__ float cache[N]; // original
- float cache[N]; // mutant
```

Listing 6.10: Example of *share_removal* mutator

**THREAD MANAGEMENT**

**GPU indexing**  GPU programming introduces a new indexing mechanism to iterate the data and threads using built-in variables such as threadIdx.x and blockIdx.x (as mentioned in Section 6.3). While in conventional imperative programming, we use the loop statement (e.g., *for* and *while*) to iterate the data and threads. Since the indexing scheme is quite different from serial code, there are numerous questions posted on StackOverflow addressing the confusion about GPU indexing, such as SO9859456 [37], SO21677559 [31] and SO33159171 [35]. Therefore, we design three mutation operators address the indexing issue:

- **gpu_index_replacement**: to replace the thread indexing variable (*threadIdx*) with the block indexing variable (*blockIdx*) and vice versa

```c
int tid = blockIdx.x; // original
- int tid = threadIdx.x; // mutant
```

Listing 6.11: Example of *gpu_index_replacement* mutator

- **gpu_index_increment**: to increase the indexing variables (*threadIdx* and *blockIdx*) by one

```c
int tid = blockIdx.x; // original
- int tid = blockIdx.x+1; // mutant
```

Listing 6.12: Example of *gpu_index_increment* mutator

- **gpu_index_decrement**: to decrease the indexing variables (*threadIdx* and *blockIdx*) by one

```c
int tid = blockIdx.x; // original
- int tid = blockIdx.x-1; // mutant
```

Listing 6.13: Example of *gpu_index_decrement* mutator

**Synchronisation functions**  The synchronisation function, also called *barrier*, is used to coordinate communications between threads in a specific block (e.g., __syncthreads() function in CUDA C). Many *data races* and *deadlocks* are caused by the incorrect barrier placement. We propose *sync_removal* to mimic the mistakes of the incorrect barrier placement. The omission or misplacement of the synchronisation function are very common in GPU code, e.g., SO29233426 [34].
• **sync removal**: to remove the synchronisation function call (e.g. `{ sync_removal }

```c
int i = blockDim.x/2;
while (i != 0) {
    if (cIndex < i)
        cache[cIndex] += cache[cIndex + i];
    __syncthreads(); //original
    i /= 2;
}
```

Listing 6.14: Example of **sync removal** mutator

**Atomic operations**

Atomic operations are unavoidable in multithreaded applications in the sense that they are guaranteed to be performed without interference from other threads. In other words, no other thread can access this address until the operation is complete. However, if the programmer does not pay enough attention, he or she is very likely to omit the atomic operations in GPU programming, for example, SO14057678 [30].

• **atom removal**: to remove the atomic functions (e.g., `atomicAdd()` with non-atomic operations

```c
while (i < size) {
    atomicAdd(&(histo[buffer[i]]),1); //original
    histo[buffer[i]] += 1; //mutant
    i += stride;
}
```

Listing 6.15: Example of **atom removal** mutator

6.4.2. **Conventional Mutation Operators**

CUDA C is an extension of standard C [267], therefore, conventional mutation operators for C also apply to CUDA C. Since the existing C mutation tools, such as Mull [122], cannot fully parse the grammar of CUDA C, we have to define the grammar of CUDA C first. So far, we have implemented five mutation operators which are most widely adopted in mutation testing, i.e., *conditional boundary replacement*, *negate conditional replacement*, *math replacement*, *increment replacement* and *logical replacement*.  

6.4.3. **GPU-specific vs. Conventional Mutation Operators**

The design principle of CUDA C/C++ is based on the traditional C/C++ syntax, which makes it easy to learn and use for developers. Although our newly proposed GPU-specific mutation operators seem to be subsumed by the existing mutation operators in terms of syntax, they are semantically different. Take `gpu_index_replacement` from GPU-specific mutation operators and `array_reference` from conventional mutation operators for example. The operator `gpu_index_replacement` replaces the thread indexing variable (`threadIdx`) with the block indexing variable (`blockIdx`). The thread/block indexing variable on the GPU is not equivalent as the array variable on the CPU. The thread/block indexing variable is used to access the parallel processors on the GPU, while `array_reference` variable is used to access the memory blocks on the CPU. One thing to notice here is that the mutants generated by GPU-specific mutation operators are totally different from the
To sum up, we have designed nine mutation operators (summarised in Table 6.1) to replicate common errors in GPU programming. Meanwhile, we have also implemented five conventional mutation operators that can be applied to CUDA C programs (also included in Table 6.1).

### 6.5. TOOL IMPLEMENTATION

As mentioned earlier in Section 6.2, there are three major GPU programming models, i.e., OpenCL, CUDA and C++ AMP. In this chapter, we select CUDA as the target model to implement the aforementioned mutation operators.

To evaluate our approach, we have implemented a prototype tool (coined MUTGPU) in Python to apply mutation testing in GPU programs. Figure 6.4 presents an overview of the architecture of MUTGPU [389]. MUTGPU consists of two components, i.e., the mutation engine and the test executor. MUTGPU takes the program and its test suite as input. First, the mutation engine analyses the source code and marks all possible mutation points, and then the mutation generator produces all the mutants according to mutation operators. After that, the program and generated mutants together with the test suite go to the test executor, where the mutation testing is performed: each mutant is executed against the test suite one by one. Finally, MUTGPU prints out the detailed mutant killable results.

The main task of the code analyser is to analyse the test dependencies and parse the source code of the program for the mutation generator. We have adopted Pyparsing [248] as the code analyser to parse the CUDA C code. Pyparsing is a pure-Python class library that constructs recursive-descent parsers with ease. The mutation generator contains all the mutation operators and the details of the mutants including the mutation location (line number) and the mutation operator type.
6.6. **EMPIRICAL EVALUATION**

To assess the efficacy of our mutation testing approach, we conducted an experimental study based on the CUDA programming model. The main purpose of this study is to investigate whether GPU programming can benefit from mutation testing, so we proposed the following research questions to steer our experimental study:

- **RQ6.1:** How frequently can GPU-specific mutation operators be applied, and how good is the existing test suite at killing them?
- **RQ6.2:** How effective are conventional mutation operators in evaluating the test suite of GPU programs?
- **RQ6.3:** How effective are GPU-specific mutation operators in evaluating the test suite of GPU programs?
- **RQ6.4:** How do GPU-specific mutation operators compare with conventional mutation operators in terms of the improvement?

### 6.6.1. SUBJECT SYSTEMS

We select six GPU benchmark projects from the CUDA SDK [6]. All these benchmark projects are widely used in the research domain [78, 82, 227]. Table 6.2 summarises the main characteristics of the selected projects. All systems are written in CUDA C, and contain a set of test cases.

We perform the experiment on two different NVIDIA graphic cards (GeForce MX150 & GTX 960) with two releases of CUDA toolkit (9.0 & 9.1) to minimise the threat caused by errors residing in hardware and CUDA toolkits.

### 6.6.2. EXPERIMENTAL SETUP

To answer RQ6.1, we investigate the mutant results for each GPU-specific mutation operator we proposed in detail. More specifically, we evaluate the frequency of each muta-
Table 6.2: Subject systems

<table>
<thead>
<tr>
<th>Project</th>
<th>File</th>
<th>LOC</th>
<th>hCOV</th>
<th>#Mutants</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Source</td>
<td>Test</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MonteCarloMultiGPU</td>
<td>MonteCarlo_kernel.cu</td>
<td>231</td>
<td>359</td>
<td>71 59</td>
</tr>
<tr>
<td></td>
<td>MonteCarlo_reduction.cuh</td>
<td>71</td>
<td></td>
<td>14 2</td>
</tr>
<tr>
<td>convolutionFFT2D</td>
<td>convolutionFFT2D.cu</td>
<td>226</td>
<td>509</td>
<td>40 36</td>
</tr>
<tr>
<td></td>
<td>convolutionFFT2D.cuh</td>
<td>463</td>
<td></td>
<td>250 64</td>
</tr>
<tr>
<td>histogram</td>
<td>histogram64.cu</td>
<td>219</td>
<td>141</td>
<td>82 96</td>
</tr>
<tr>
<td></td>
<td>Histogram256.cu</td>
<td>165</td>
<td></td>
<td>48 81</td>
</tr>
<tr>
<td>mergeSort</td>
<td>mergeSort.cu</td>
<td>636</td>
<td>95</td>
<td>100 300</td>
</tr>
<tr>
<td>transpose</td>
<td>transpose.cu</td>
<td>349</td>
<td>174</td>
<td>100 319</td>
</tr>
<tr>
<td>scan</td>
<td>scan.cu</td>
<td>290</td>
<td>116</td>
<td>100 70</td>
</tr>
<tr>
<td></td>
<td>total</td>
<td>2650</td>
<td>1394</td>
<td>100 1039</td>
</tr>
</tbody>
</table>

Note: Column “LOC” standing for the line of code is measured by sloccount. Column “hCOV” indicates the statement coverage for the host code. For device code, coverage analysis is a wrong approach as already discussed by the Nvidia community [4].

For RQ6.2 and RQ6.3, we determine the effectiveness of the mutation operators in assessing test quality of GPU programs based on non-equivalent surviving mutants. Because non-equivalent surviving mutants are crucial to calculate the mutation score, and by investigating non-equivalent surviving mutants, we can see whether those mutants are due to inadequate test suites or not. We have implemented five conventional and nine GPU-specific mutation operators in our tool MUTGPU. We apply all the mutation operators to the six subject systems and manually analyse the non-equivalent surviving mutants. We identify the equivalent mutants by hand.

To compare the conventional mutation operators with GPU-specific ones (RQ6.4), we are interested in what kind of enhancements the GPU-specific mutation operators can bring to the conventional mutation operators. In other words, we would like to investigate whether there exists some bugs or issues that cannot be detected by the conventional mutation operators, but can be detected by GPU-specific mutation operators. Therefore, we first try to manually engineer new test cases to kill all the possible conventional mutants to obtain a C-sufficient test suite for each system. Then, we apply GPU-specific mutation operators to the C-sufficient test suites to see if there are non-equivalent GPU mutants survived. The last step is to manually analyse the remaining GPU mutants that cannot be detected by the C-sufficient test suites.

6.7. RESULTS

RQ6.1: FREQUENCY OF GPU-SPECIFIC MUTATION OPERATORS & MUTATION SCORES

We sum up the mutant results for each mutation operator in Table 6.3. From Table 6.3, we can observe that operator gpu_index_replacement generates the most mutants (411) for GPU programs, followed by operator gpu_index_decrement (210) and gpu_index_increment (210). This indicates that the GPU indexing operations are commonly used in GPU programming. Thus, designing specific mutation operators for GPU indexing seems nec-
Table 6.3: Mutant results for each mutation operator

<table>
<thead>
<tr>
<th>category operator</th>
<th>#covered</th>
<th>#killed</th>
<th>#equiv.</th>
<th>#survived</th>
<th>total MS</th>
</tr>
</thead>
<tbody>
<tr>
<td>C conditional_boundary_replacement</td>
<td>114</td>
<td>60</td>
<td>45</td>
<td>58</td>
<td>118</td>
</tr>
<tr>
<td>increment_replacement</td>
<td>12</td>
<td>9</td>
<td>0</td>
<td>3</td>
<td>12</td>
</tr>
<tr>
<td>logical_replacement</td>
<td>5</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td>math_replacement</td>
<td>372</td>
<td>154</td>
<td>136</td>
<td>172</td>
<td>744</td>
</tr>
<tr>
<td>negate_conditional_replacement</td>
<td>156</td>
<td>139</td>
<td>6</td>
<td>30</td>
<td>160</td>
</tr>
<tr>
<td>subtotal</td>
<td>1001</td>
<td>773</td>
<td>140</td>
<td>266</td>
<td>1039</td>
</tr>
<tr>
<td>GPU alloc_decrement</td>
<td>46</td>
<td>38</td>
<td>0</td>
<td>12</td>
<td>50</td>
</tr>
<tr>
<td>alloc_increment</td>
<td>46</td>
<td>21</td>
<td>0</td>
<td>29</td>
<td>50</td>
</tr>
<tr>
<td>alloc_swap</td>
<td>46</td>
<td>31</td>
<td>3</td>
<td>19</td>
<td>50</td>
</tr>
<tr>
<td>atom_removal</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>gpu_index_decrement</td>
<td>204</td>
<td>181</td>
<td>0</td>
<td>29</td>
<td>210</td>
</tr>
<tr>
<td>gpu_index_increment</td>
<td>204</td>
<td>173</td>
<td>0</td>
<td>37</td>
<td>210</td>
</tr>
<tr>
<td>gpu_index_replacement</td>
<td>403</td>
<td>340</td>
<td>0</td>
<td>71</td>
<td>411</td>
</tr>
<tr>
<td>share_removal</td>
<td>20</td>
<td>17</td>
<td>0</td>
<td>3</td>
<td>20</td>
</tr>
<tr>
<td>sync_removal</td>
<td>25</td>
<td>19</td>
<td>1</td>
<td>6</td>
<td>25</td>
</tr>
<tr>
<td>subtotal</td>
<td>995</td>
<td>821</td>
<td>4</td>
<td>206</td>
<td>1027</td>
</tr>
</tbody>
</table>

Note: Column “#equiv.” represents the number of the equivalent mutants. Column “MS” represents the mutation score which is calculated by the number of killed mutants divided by the number of non-equivalent mutants (the same in the following tables).

necessary. The operator atom_removal only produces one mutant. We assume the reason behind the low mutant number (=1) is because the selected subject systems we selected do not contain many atomic operations.

From the aspect of the mutation score, except operator atom_removal whose mutation score is 1, the rest ranges from 0.438 to 0.862. This means that not all the mutants generated by the GPU-specific mutation operators can be detected by the existing test suites. There is still space for improvement in the existing test suites. The high mutation score for operator atom_removal is due to its low mutant number. This observation indicates that all GPU specific mutation operators we designed are useful in GPU programming to guide the engineers to write better tests.

The GPU-specific mutation operators we propose can be frequently applied in GPU programming. Furthermore, the mutation score obtained from applying these mutation operators ranges from 0.438 to 1.0.

RQ6.2: CONVENTIONAL MUTATION OPERATORS

Table 6.4 summarises the mutant results from running both C and GPU mutants against existing test suites. Overall, there are 1039 C mutants generated in total (as shown in Table 6.4). 96.3% mutants are covered by the existing test suites (meaning the line from which the mutant is generated is covered by the test suite), while 74.4% mutants (86.0% non-equivalent mutants) are killed. We can see that the mutation score (0.860) is lower than the mutation coverage (0.963), which means some mutants that are covered by the tests can still survive. Looking at the existing test suites, we found that most tests from the six projects do not target the unit-level: the main design of the test suites is to invoke a series of functions in turn and examine the final results in the end. Therefore,
Table 6.4: Mutant results

<table>
<thead>
<tr>
<th>Project</th>
<th>File</th>
<th>C Mutants</th>
<th></th>
<th>GPU Mutants</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>#total</td>
<td>#covered</td>
<td>#killed</td>
<td>#equiv. MS</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MonteCarloMultiGPU</td>
<td>MonteCarlo_kernel.cu</td>
<td>71</td>
<td>65</td>
<td>44</td>
<td>7 0.688</td>
</tr>
<tr>
<td></td>
<td>MonteCarlo_reduction.cuh</td>
<td>14</td>
<td>14</td>
<td>13</td>
<td>1 1.000</td>
</tr>
<tr>
<td></td>
<td>convolutionFFT2D</td>
<td>40</td>
<td>40</td>
<td>40</td>
<td>0 1.000</td>
</tr>
<tr>
<td></td>
<td>convolutionFFT2D.cuh</td>
<td>250</td>
<td>249</td>
<td>213</td>
<td>34 0.986</td>
</tr>
<tr>
<td></td>
<td>histogram</td>
<td>82</td>
<td>77</td>
<td>70</td>
<td>6 0.921</td>
</tr>
<tr>
<td></td>
<td>histogram64.cu</td>
<td>48</td>
<td>48</td>
<td>41</td>
<td>5 0.953</td>
</tr>
<tr>
<td></td>
<td>mergeSort</td>
<td>264</td>
<td>244</td>
<td>180</td>
<td>33 0.779</td>
</tr>
<tr>
<td></td>
<td>mergeSort.cu</td>
<td>180</td>
<td>174</td>
<td>99</td>
<td>45 0.723</td>
</tr>
<tr>
<td></td>
<td>transpose</td>
<td>90</td>
<td>90</td>
<td>73</td>
<td>11 0.924</td>
</tr>
<tr>
<td></td>
<td>transpose.cu</td>
<td>1039</td>
<td>1001</td>
<td>773</td>
<td>140 0.860</td>
</tr>
<tr>
<td></td>
<td>total</td>
<td>1027</td>
<td>995</td>
<td>821</td>
<td>3 0.970</td>
</tr>
</tbody>
</table>

Note: Column "#equiv." represents the number of the equivalent mutants. Column "MS" represents the mutation score which is calculated by the number of killed mutants divided by the number of non-equivalent mutants (the same in the following tables).

1 for (int i=0; i<TILE_DIM; i+=BLOCK_ROWS){
2     if (xIndex < height && yIndex < width){
3         odata[index]=tile[threadIdx.y][threadIdx.x];}

Listing 6.16: Bug example of an equivalent mutant (in transpose.cu)

it is very likely that a small change in the program (a mutant) do not propagate to the outputs (fault masking [162]). Moreover, test directness, which measures the extent to which the production code is tested directly, plays an important role in mutation testing (as mentioned in Chapter 4). However, there are few direct tests in the existing test suite to assess the difference between the original and the mutated programs; this causes a small number of mutants to not be detected by the existing test suites. The comparison of coverage and mutation score indicates that the mutation score is a stronger indicator of test suite quality than test coverage.

Speaking of equivalent mutants, the conventional mutation operators generate 140 equivalent mutants (13.5%) out of 1039 mutants as displayed in Table 6.4. Furthermore, from Table 6.3 where we sum up the mutant results for each mutation operator, we can see that over 50% of mutants (61.4%) are generated by operator math_replacement, followed by operator conditional_boundary_replacement (32.1%). Most of the equivalent mutants produced by math_replacement are because one operand in the math operation is zero, such as threadIdx.x + 0, thus the replacement of the math operators, e.g., from + to −, does not influence the result. The equivalent mutants from conditional_boundary_replacement are owing to the fact that the boundary conditions (the equivalent condition, i.e., =) cannot be reached or satisfied. Also, there are a few equivalent mutants guiding us to detect the bugs in the systems. Listing 6.16 presents an example of a bug caught by the equivalent mutants. The mutant which replaces < to ≤ in Line 1 is equivalent to the original program since the variable i does not affect the result of the loop. This equivalency turns out to be a potential bug in the program as variable i is useless in the loop. The cause for the bug is that there is a similar loop in the previous function (shown in Listing 6.17). Thus, the bug shown in Listing 6.16 might be due to copy-pasting the previous statements but omitting the modification. This finding supports that GPU programming can benefit from mutation testing.
Moreover, to further understand the effectiveness of the mutation operators in assessing test quality, we need to manually analyse the 126 surviving non-equivalent mutants to see whether these surviving non-equivalent mutants are due to inadequate test suites. Compared to conventional CPU programs, testing GPU code is more challenging. Only a small number of mutants (34 out of 126) can simply be killed by improving and adding tests. To detect the remaining mutants, we first need to refactor the existing code, and then add tests. The reason for a number of the mutants that need to be refactored is because many functions cannot be directly accessed from the test suites.

According to the CUDA programming model (shown in Figure 6.2), there are two parts in the GPU programs: the host (the CPU and the system memory) and the device (the GPU and its memory). The tests are mainly located in the host which invokes a function in the device/host and examines the result. Therefore, if the function is executed on the device and callable from the device only, it is impossible to access the function directly from the host. This exception is the function specified by __device__. The workaround is to wrap __device__ functions with a __global__ function which can be callable from the host. Other function specifiers, e.g., static and inline, also prevent the tests to access those functions from a different file. Since the access to static and inline functions is restricted to the file where they are declared. To test static and inline functions, we have to remove the static and inline specifiers to allow the access from a separate test file.

By modifying the function accessibility for the tests and adding direct tests, we can kill another 58 mutants. However, some mutants generated are located in intermediate variables which do not propagate to the output. These are much harder to detect: they usually require to split the method into smaller portions, or refactor the method to non-void. This might considerably alter the structure of the systems, and also affect the mutation score. Therefore, in this study, we leave this type of "stubborn" mutants aside. Except for "stubborn" mutants, to kill a conventional mutant in a GPU program, adding one direct test without carefully choosing test input can work well which we can achieve it within 1 min. Finally, we can achieve 0.962 mutation score by improving the test quality, which indicates the conventional mutation operators can effectively evaluate the existing test quality in the context of GPU programming.

GPU programming can benefit from the conventional mutation operators which mainly guide the engineers to write direct tests for GPU programs. The average time to engineer a test case to kill a mutant is within 1 min.

**RQ6.3: GPU-SPECIFIC MUTATION OPERATORS**

From Table 6.4, we can see that there are 1027 mutants generated by GPU-specific mutation operators, slightly less than C mutants. Among all the GPU mutants, 96.9% mutants are covered by the existing test suites. The overall mutation score is 0.803. The same observation holds for GPU mutants as for CPU mutants: the mutation score is higher than...
the coverage. As we mentioned in Section 6.7, the majority of the tests only examine the final outputs after a series of function calls. Therefore, although a number of mutants are covered by the test suites, their changes do not propagate to the final outputs. This also shows the advantage of the mutation testing over test coverage in evaluating test quality.

In terms of equivalent mutants, GPU specific mutation operators only generate four equivalent mutants. Three are from operator `alloc_swap`, which are all located in the execution configuration for a kernel function call (__global__ function call). The mutants generated by `alloc_swap` are due to the number of threads being the same as the number of blocks in parallel processor allocations. The last equivalent mutant is generated by operator `sync_removal`. This mutant is similar to Listing 6.16 which indicates the presence of a potential bug (presented in Listing 6.18). The main task of Listing 6.18 is to produce a smaller array of the sum result by reduction. The code fragment in Listing 6.18 does not contain write operations to the shared array `sum` and `sum2`, thereby, there is no need for a synchronisation function (cg::sync(cta)) in the end to guarantee that all of those writes to the shared arrays complete before anyone tries to read from the buffers. The synchronisation function (cg::sync(cta)) in Listing 6.18 is not necessary. This also confirms that misuses of the synchronisation functions in GPU programming are quite common, and the operator `sync_removal` can well represent common errors in GPU programming. Looking into the surviving GPU mutants, a large number of mutants (131) can easily be detected by modifying the function accessibility (e.g., remove static specifier) and adding direct tests as mentioned in Section 6.7. To kill the remaining non-equivalent mutants is more challenging: in addition to examining the expected result after the function call, more factors should be taken into consideration, such as the execution sequence, the size of the test input and the times of test execution. For instance, to detect the mutants from operator `sync_removal`, it usually requires multiple test executions (> 10 times), as the execution order of the code in GPU cores is undetermined. Although, we assume that GPU cores run the parallel program at the same time, there exist some latencies in different GPU cores. For instance, Thread 1 is executed before Thread 2 in one execution, while Thread 2 is executed before Thread 1 in another execution. Thus, data races do not occur every time. Another example is to kill the mutant generated from a __global__ function. It is very likely to encounter illegal memory access if the test input size is inappropriate. To kill a GPU mutant, it usually requires us to understand the program context very well and choose more than one specific test input to kill a mutant; this could take up to hours to kill a GPU mutant. Thus, those tests designed to kill GPU mutants can better reveal GPU-specific weakness.

However, we found that not all the non-equivalent surviving mutants can be killed by adding test cases. There are 22 mutants not affecting the result of the kernel functions but the GPU performance. The GPU performance means the execution time by GPUs.
Table 6.5: Mutant results (C-sufficient test suites)

<table>
<thead>
<tr>
<th>Project</th>
<th>File</th>
<th>C Mutants</th>
<th>GPU Mutants</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>#total</td>
<td>#covered</td>
</tr>
<tr>
<td>MonteCarloMultiGPU</td>
<td>MonteCarlo_kernel.cu</td>
<td>71</td>
<td>71</td>
</tr>
<tr>
<td></td>
<td>MonteCarlo_reduction.cuh</td>
<td>14</td>
<td>14</td>
</tr>
<tr>
<td>convolutionFFT2D</td>
<td>convolutionFFT2D.cu</td>
<td>40</td>
<td>40</td>
</tr>
<tr>
<td></td>
<td>convolutionFFT2D.cuh</td>
<td>250</td>
<td>249</td>
</tr>
<tr>
<td>histogram</td>
<td>histogram64.cu</td>
<td>82</td>
<td>77</td>
</tr>
<tr>
<td></td>
<td>Histogram256.cu</td>
<td>48</td>
<td>48</td>
</tr>
<tr>
<td>mergeSort</td>
<td>mergeSort.cu</td>
<td>264</td>
<td>264</td>
</tr>
<tr>
<td>transpose</td>
<td>transpose.cu</td>
<td>180</td>
<td>180</td>
</tr>
<tr>
<td>scan</td>
<td>scan.cu</td>
<td>90</td>
<td>90</td>
</tr>
<tr>
<td>total</td>
<td></td>
<td>1039</td>
<td>1033</td>
</tr>
</tbody>
</table>

Note: Column "#equiv." represents the number of the equivalent mutants. Column "MS" represents the mutation score which is calculated by the number of killed mutants divided by the number of non-equivalent mutants (the same in the following tables).

For example, one mutant generated by `alloc_increment` modifies the number of threads in parallel processor allocations from 256 to (256-1). But the modifications do not influence the function output since the function already takes care of the boundary condition when the test input exceeds the number of parallel threads (just as in Listing 6.4). Also, the performance difference caused by the allocation decrement (-1) is too small to be sensed by any test. The performance difference is unique to GPU programming since the standard CPU programs do not use GPUs as co-processors. We suggest considering these mutants that only influence the performance at a small scale without output modification as equivalent mutants in the context of GPU programming. Another option to void such "equivalent" mutants generated from GPU programming could be using performance requirement to be part of the definition of a test case passing or failing.

GPU-specific mutation operators can effectively evaluate the test quality in the context of GPU programming. To kill the GPU mutants, many factors should be taken into consideration, such as test directness, the program context, the execution sequence and the test input size. It takes up to hours to kill a GPU mutant.

RQ6.4: CONVENTIONAL VS. GPU-SPECIFIC

In this section, we are going to shed light on the comparison of the conventional and GPU-specific mutation operators we proposed. As mentioned earlier, we are interested in what kind of improvements the GPU-specific mutation operators can bring to the conventional mutation operators. Thereby, we use C-sufficient test suites (100% mutation coverage for C mutants) as the base to apply mutation testing on the subject systems. Table 6.5 displays the mutant results based on the C-sufficient test suites. We can see that C-sufficient test suites have a high average mutation score using conventional mutation operators compared to GPU-specific ones; this is what we expect. Otherwise, GPU mutants are subsumed by C mutants, i.e., if the test suite achieve 100% mutation coverage on C mutants, it also achieves 100% mutation coverage on GPU mutants.

From Table 6.5, we can see that with an increase in mutation score with conventional mutation operators, the mutation score of GPU-specific mutation operators also
increases. This is mainly due to the design of the existing test suites, that do not target the unit testing level (mentioned in Section 6.7). We also observe a lack of direct tests for each function in the existing test suites. Thus, when we engineer new tests to kill the C mutants, we mainly concentrate on designing direct tests (as we discussed in Section 6.7). When we target a C mutant, the GPU mutant(s) located in the same line or the same function unit is also under investigation. Once the change(s) of the GPU mutant(s) in the same line or the same function unit can be observed by the direct test designed for the C mutant, the GPU mutant(s) can typically be killed at the same time.

Considering the remaining GPU mutants that are not detected by the C-sufficient test suites, the majority requires more delicate and complex test cases to observe the differences. Take a surviving GPU mutant in File convolutionFFT2D.cuh (shown in Listing 6.19) for example. The function `padKernel_kernel` aims to position the center of the convolution kernel at (0, 0) of the image which makes use of 2D GPU indexing.

All the mutants generated in Line 2 are detailed in Table 6.6. In order to kill the C mutant (MID = 0) in Line 2, we add a direct test (shown in Listing 6.20) for function `pad-`
Table 6.6: Mutant details for Listing 6.19 in Line 2

<table>
<thead>
<tr>
<th>MID</th>
<th>operator</th>
<th>details</th>
<th>category</th>
<th>existing</th>
<th>c-sufficient</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>math_rep./</td>
<td>c</td>
<td>survived</td>
<td>killed</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>gpu_index_rep. threadIdx.y</td>
<td>gpu</td>
<td>killed</td>
<td>killed</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>gpu_index_rep. blockIdx.x</td>
<td>gpu</td>
<td>survived</td>
<td>survived</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>gpu_index_inc. (blockIdx.y+1)</td>
<td>gpu</td>
<td>killed</td>
<td>killed</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>gpu_index_dec. (blockIdx.y-1)</td>
<td>gpu</td>
<td>killed</td>
<td>killed</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>math_rep. -</td>
<td>c</td>
<td>killed</td>
<td>killed</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>gpu_index_rep. blockIdx.y</td>
<td>gpu</td>
<td>killed</td>
<td>killed</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>gpu_index_rep. threadIdx.x</td>
<td>gpu</td>
<td>killed</td>
<td>killed</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>gpu_index_inc. (threadIdx.y+1)</td>
<td>gpu</td>
<td>killed</td>
<td>killed</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>gpu_index_dec. (threadIdx.y-1)</td>
<td>gpu</td>
<td>survived</td>
<td>survived</td>
<td></td>
</tr>
</tbody>
</table>

**Kernel_kernel.** However, the newly added direct test cannot detect the two GPU mutants with MID = 2 and MID = 9. Upon investigation, we found in the execution configuration for function *padKernel_kernel*, the numbers of blocks in the two dimensions are the same, i.e., $gridDim.x = gridDim.y = 1$ (see Line 14). Also, the condition in Line 4 of Listing 6.19 restricts the larger indexes of parallel threads for computation. Therefore, adding the direct tests cannot detect the difference of replacing $blockIdx.y$ to $blockIdx.x$.

To detect Mutant 2, we need to modify the numbers of blocks in the two dimensions to different values, e.g., set $gridDim.x = 4$ and $gridDim.y = 1$ (see Line 15). Moreover, we need to set the values of $kernelH$ and $kernelW$ (see Line 17&18) big enough so that the difference of the value $y$ can affect the output of $d_Dst$ array.

Together with this example, we can see that adding direct tests can kill most C mutants, but not all the GPU mutants. The remaining GPU mutants are more challenging to be killed as their differences with the original program are more subtle to tell. Only given test inputs with specific values and execution settings, these GPU mutants can be detected. This shows that the outputs of the GPU program are easily affected by test inputs and execution configurations. Thus, the corresponding test cases designed according to these types of GPU mutants are of higher quality and can detect more potential GPU-specific bugs in the systems. Therefore, it requires more effort to design delicate tests to kill a GPU mutants than the conventional C mutants.

Compared to conventional mutation operators, GPU-specific ones are better at guiding the engineers to design more delicate tests to detect the subtle differences in GPU programming. The efforts required to kill GPU mutants are higher than the conventional.

### 6.8. Threats To Validity

**External validity:** First, our results are based on the CUDA programming model; the results might be different when using other GPU programming models. Second, concerning the subject selection, we chose six GPU projects in total to evaluate our approach. All the projects are benchmark projects from the CUDA SDK [6], and are widely used in the research domain; this can minimise the threats caused by subjects. Moreover, there might exist errors in the GPU hardware and the CUDA toolkit. To avoid this threat,
we conduct our experiment on different NVIDIA graphic cards and different releases of CUDA toolkit.

**Internal validity:** The main threat to internal validity for our study is the implementation of MUTGPU for the experiment. To reduce internal threats to a large extent, we carefully reviewed and tested all code to eliminate potential faults in our implementation. Another threat to internal validity is the detection of equivalent mutants through manual analysis. However, this threat is unavoidable and shared by other studies that attempt to detect equivalent mutants [165, 252].

**Construct validity:** The main threat to construct validity is the measurement we used to evaluate our methods. We used the percentage of non-equivalent mutants and the mutation score as key metrics in our experiment, both of which have been widely used in other studies on mutation testing.

### 6.9. Related Work

With wide-spread applications of GPUs in High Performance Computing (HPC) [134, 336] and safety-critical domains (e.g., medical science [332] and automotive [225]), there have been increasing attentions on the quality assurance of GPU applications [158, 303], such as dynamic analysis [82] and formal verification [78, 227].

Most related to our approach are *fault injection* techniques in GPGPU applications. Farazmand et al. [137] attempted to quantify the Architectural Vulnerability Factor (AVF) of GPU hardware structures using statistical fault injection. They injected faults into register files, local memory, and active mask stack to characterise the vulnerability of different micro-architectural structures in GPUs to soft errors. Yim et al. [374] developed a mutation-based fault injection tool for automated reliability testing of GPU devices. They modeled both single- and multi-bit errors in the architecture state to represent the silent data corruption (SDC) error.

Fang et al. [135] proposed a fault injection methodology to evaluate the error resilience of the GPGPU applications. They aimed at injecting the faults that represent real *hardware* errors where they adopted the single-bit-flip fault model to simulate transient faults in GPU processors. Hari et al. [173] presented an fault injection-based framework called SASSIFI for GPU application resilience evaluation, especially on soft errors. SASSIFI serves two kinds of tasks: (1) inject bit-flip errors into the register file for AVF analysis; (2) inject errors in the outputs of the instructions for error propagation evaluation.

All the above studies have targeted the errors related to the GPU hardware. While we focus on the software aspect of GPU applications where we design mutation operators in the ways that engineers could make mistakes in GPU programming.

### 6.10. Conclusion and Future Work

This chapter aims to explore whether GPU programming can benefit from mutation testing. Compared to the CPU, the GPU differs greatly in the architecture and the programming model, thus, GPU programming comes with its own set of challenges. Upon observation, we found GPU code with issues of memory management, thread management and atomic operations can easily pass the test suite selected with conventional muta-
tion operators. Thus, we propose nine GPU-specific mutation operators according to the main syntactic differences between CPU and GPU programming.

To evaluate our approach, we present a tool coined MUTGPU and conduct an experiment on six CUDA systems. Our results show promising findings that GPU programming can benefit from mutation testing in three ways: (1) conventional mutation operators can guide engineers to write simple direct tests; (2) GPU-specific mutation operators can lead to more delicate test cases (thus higher quality and more test effort); (3) equivalent mutants can help in bug detection.

This chapter makes the following contributions:

- nine GPU-specific mutation operators;
- a mutation tool (MUTGPU [389]) working on CUDA;
- comparison of conventional and GPU-specific operators;
- a preliminary experiment on six GPU applications [389].

**Future work.** In the future, we aim to conduct additional case studies on more realistic GPU systems. Also, we would like to explore another GPU platforms, such as OpenCL.
This chapter concludes this thesis by first revisiting our research questions from Chapter 1, discussing the main threats to validity, and outlining the recommendations for future work.

### 7.1. Research Questions Revisited

In this section, we are going to revisit the research questions we propose in Chapter 1. We present the main takeaways from the answers to those research questions.

**RQ2 How is mutation testing actually applied?**

In Chapter 2, we have reported on a systematic literature review on the application perspective of mutation testing based on a collection of 191 papers from 22 venues. Through a detailed reading of this research body, we derive an attribute framework that is consequently used to characterise the selected studies in a structured manner. This attribute framework generalises and details the essential elements related to the actual application of mutation testing, such as in which circumstances mutation testing is used and which mutation testing tool is selected. In particular, a generic classification of mutation operators is constructed to study and compare the mutation operators used in the experiments described.

Our main findings from the systematic literature review are: (1) Most studies (70.2%) use mutation testing as a fault-based evaluation method in different quality assurance processes. Those studies mainly target the unit level. (2) Many of the supporting techniques for making mutation testing truly applicable are still under-developed. The two key problems, namely the equivalent mutant detection problem and the high computation cost of mutation testing issues, are not well-solved in the context of our research body. (3) A deeper understanding of mutation testing is required, such as what particular kinds of faults mutation testing is good at finding. (4) The awareness of appropriately reporting mutation testing in testing experiments should be raised among the researchers. The first three findings further attract our attention, resulting in RQ3 - RQ6.
**RQ3** *Can compression techniques be used to speed up mutation testing?*

In Chapter 3, we have conducted a detailed investigation of different compression techniques to speed up mutation testing using 20 open-source projects. We have introduced and investigated six compression strategies based on two clustering algorithms and three mutant selection strategies. In particular, we use overlapped and FCA groupings to cluster mutants based on their reachability and necessity condition against the test suite, and then apply mutant selection (three selection strategies, i.e., pure random, random with knowledge of mutation locations and random with mutation operator types) to decide which ones need to be executed in strong mutation. Also, we consider 10% random sampling and weak mutation methods as baselines.

The results of our empirical study show that mutant compression techniques can effectively speed up strong mutation testing up to 94.3 times with an accuracy > 90%. *FCA-based compression* is the fastest strategy, while *overlapped grouping* with the mutation location knowledge in mutant selection is the most accurate. In comparison, *weak mutation* attains a higher absolute error (23%) and lower accuracy (75%). *Random sampling* with 10% as sampling percentage is statistically less accurate than all mutant compression strategies, and worse in terms of speed-up than four compression strategies (excluding the two with knowledge of mutation locations).

Another important finding is that *mutation location trumps mutation operator information when selecting mutants to evaluate for strong mutation*. Hence, we suggest researchers should take into account the mutation locations in addition to the mutation operators when detecting redundant or subsuming mutants (e.g., [46, 202, 219]).

**RQ4** *How can production code quality in terms of testability and observability influence the mutation score?*

In Chapter 4, we have investigated our hypothesis that code quality especially regarding the *testability* and *observability* plays an essential role in mutation testing. We have collected 64 existing source code quality metrics for testability, and have proposed a set of metrics that specifically target observability. We have first investigated the relationships between testability/observability metrics and the mutation score involving six open source Java projects. We observe that the 64 existing code quality metrics are not strongly correlated with the mutation score (\(|\rho| < 0.27\)), while our newly proposed observability metrics do show a stronger correlation with the mutation score (\(|\rho| < 0.5\)). In particular, *test directness*, which measures the extent to which the production code is tested directly, seems to be the most essential factor.

To better understand the causality of our insights, we have continued our investigation with a case study of 16 methods that scored particularly bad in terms of mutation score. In particular, we have refactored these methods and/or added tests according to the anti-patterns that we established in terms of the code observability metrics. We found that these anti-patterns can indeed offer software engineers actionable insights to improve both the production code and the test suite, and improve the mutation score along with it.
In Chapter 5, we have proposed a novel mutation testing approach for physical computing systems. We first have designed nine mutation operators based on common mistakes we have observed that are typically made by programmers during the implementation of software. To enable mutation testing for physical computing systems, we have implemented a mutation testing tool coined MUTPHY working on the Raspberry Pi and Arduino platforms. Then, we have conducted two case studies on both Raspberry Pi and Arduino platforms involving nine physical computing projects.

For nine systems, our mutation testing tool generates a total of 1036 mutants of which 41% are not killed by the original test suite (and 1.2% of the overall mutants being equivalent mutants). Adding tests or reinforcing existing tests makes it possible to kill 94% of the non-equivalent surviving mutants. Our results have shown encouraging results in uncovering weaknesses in existing tests. Thereby, we can see that physical computing could benefit from mutation testing in guiding engineers to test systems more effectively and efficiently.

In Chapter 6, we aim to enable mutation testing for GPU programming to investigate whether GPU programs can benefit from mutation testing. To achieve this goal, we have developed a mutation testing tool named MUTGPU especially for GPU applications in the CUDA programming model. Considering the differences between CPU and GPU programming, we have designed nine new GPU-specific mutation operators in addition to conventional mutation operators. We have performed an empirical study involving six GPU projects from the CUDA Code Samples [6]. Our results have shown that the conventional mutation operators can guide the engineers to write direct tests for GPU programs, while GPU-specific mutation operators can lead to more delicate and more complex test cases, which cannot be exposed by the conventional mutation operators.

7.2. THREATS TO VALIDITY
The threats to validity address the question of how our results and conclusions might be wrong [247], which is an essential part to judge the quality of a research study. In this section, we describe the main threats to validity of this thesis by summarising the threats to validity for each research question (RQ2-RQ6). There are detailed analyses of threats to validity for each research question in their corresponding chapter.

**External validity:** The external validity is concerned with whether we can generalise the results outside the scope of our thesis [139]. The main external validity for our thesis is the subject systems selection. The ways we have attempted to mitigate this threat to validity is (1) selecting at least six projects that differ in size, number of test cases and application domain; (2) selecting open-source projects whenever possible to enable replications of our study; (3) selecting projects that have already been widely used in related studies. Nevertheless, although we aim for generalisability, we do acknowledge
that a broad replication of our study would mitigate any generalisability concerns even further.

**Internal validity:** The *internal validity* focus on how sure we can be that the treatment actually caused the outcome [139]. The main threat to internal validity for our thesis is in the self-implemented tools or scripts to conduct experimental studies. Except for the systematic literature review presented in Chapter 2, all the studies include at least a tool or script that we have implemented by ourselves. To eliminate potential faults in our implementations, we have carefully reviewed and tested all the code. Another threat to internal validity is the *equivalent mutant detection* [91] in our experiments. As a well-known *undecidable problem* [91], the *equivalent mutant detection* is unavoidable and shared by other studies on mutation testing that attempt to detect equivalent mutants or not [165, 252].

**Construct validity:** The *construct validity* concerns about the relation between the theory behind the experiment and the observation(s) [139], i.e., whether the observed outcome corresponds to the cause/treatment we think or not. The main threat to construct validity is the measurement we have employed to evaluate our methods. Our attempts to minimise this risk is by adopting evaluation metrics that are widely used in research (such as recall, precision, and AUC), as well as a sound statistical analysis to assess the significance (Spearman's rank-order correlation).

### 7.3. **Recommendations for future work**

Although mutation testing has been investigated for over four decades, it is still facing numerous challenges for more broad applicability. This thesis aims to improve and extend the applicability of mutation testing, including speeding up mutation testing, deepening understanding of mutation testing and exploring new application domains. However, research on the applicability of mutation testing still needs a long way to go. In the following we envision four directions of future works based on the findings of this thesis.

- **R1: More tool support in integrated development environments (IDEs) is needed.**
  Most mutation testing tools, such as Mujava [240] and PiTest [13], are developed by third parties. The compatibility issue with the state-of-art IDEs (e.g., IntelliJ) is not well-solved. Developing seamless integration with IDEs (like has been done for JUnit) for mutation testing tools can greatly ease the difficulty of applying mutation testing in the daily work of developers, thus potentially accelerating the application of mutation testing.

- **R2: “Smart” and personalised mutation engine.**
  Most mutation testing tools provide the users with several options to choose from, for instance, the mutation operators to be used and which class/method to be mutated in the mutation testing. However, the mutation engine (i.e. the framework to create mutants) itself is not “smart” enough; this means the mutation engine just applies the selected mutation operators to the selected class/method mechanically to create mutants. Besides, every developer is unique and their common
programming mistakes are various. It would be very useful that the mutation engine can learn from mistake patterns of each developer and create personalised mutants for him/her. Such a “smart” and personalised mutation engine not only speeds up the process of mutation testing, but also guides the developer to write better production code and tests.

• **R3: Study the usability perspective of mutation testing by involving real developers.**

Based on Chapter 4, numerous studies have investigated how useful mutants are. Example studies include *mutant subsumption* [219], *stubborn* mutants [373], and *real-fault coupling* [201, 295]. These studies concern *mutant utility* [203], the efficacy of mutation testing. However, there are few works involving real developers in the empirical studies. We suggest a developer-centric study on mutation testing as it would allow to gain valuable insights on which mutants are found to be most useful.

• **R4: More attentions should be paid on domain-specific mutation testing.**

In Chapter 5 and Chapter 6, we have designed domain-specific mutation operators for physical computing systems and GPU programs. Compared to conventional mutation operators, we found domain-specific mutation operators to be more helpful in guiding the developers to locate the weaknesses of the programs and write better tests. We would like to encourage researchers to explore more application domains for mutation testing (such as intelligent agents).
REFERENCES


REFERENCES


REFERENCES


SERC-TR-41-P, Software Engineering Research Center, Department of Computer Science, Purdue University, Indiana, 1989.


[169] Jiawei Han, Jian Pei, and Micheline Kamber. *Data mining: concepts and techniques*. Elsevier, 2011.


<table>
<thead>
<tr>
<th>Reference</th>
<th>Citation</th>
</tr>
</thead>
</table>


CURRICULUM VITÆ

Qianqian ZHU

23-12-1990 Born in Wenzhou, Zhejiang Province, China.

EDUCATION

2015.11-2019.11 Ph.D. in Software Engineering
Delft University of Technology, Netherlands
Promotors: Prof. Dr. Andy Zaidman & Prof. Dr. Arie van Deursen
Co-promotor: dr. Annibale Panichella

2013.10-2014.10 M.Sc. in Computer Science
Imperial College London, UK
Grade: Distinction & TOP 3rd

2009.09-2013.06 B.Eng. in Biosystems Engineering
Zhejiang University, China
Grade: 4.11/5.0 & TOP 10%

EXPERIENCE

2015-2019 Reviewer
JSS, STVR, ICST, ICSE, SCAM, SANER

2019, 2020 Program committee member
Mutation Testing Workshop

2018 Web chair
The 15th International Conference on Mining Software Repositories (MSR 2018)

2017.04-2017.07 Teaching Assistant
Software Testing and Quality Engineering, prof. dr. A. van Deursen

2014.11-2015.02 Data Scientist
Go Capture, Shanghai, China

2009-2010 Steering committee member
College Students Association Union of Zhejiang University
LIST OF PUBLICATIONS

5. Qianqian Zhu and Andy Zaidman, Massively Parallel, Highly Efficient, but What About the Test Suite Quality? Applying Mutation Testing to GPU Programs, Proceedings of the 11th International Conference on Software Testing, Verification, and Validation (ICST), Porto, Portugal, 2020


THE APPLICATION PERSPECTIVE OF MUTATION TESTING