2012

Black-Box Test Case Generation from TFM Module Interface Specifications and Usage Statistics

Katsuya Iwata
Iowa State University

Follow this and additional works at: http://lib.dr.iastate.edu/etd
Part of the Computer Sciences Commons

Recommended Citation

This Thesis is brought to you for free and open access by the Graduate College at Digital Repository @ Iowa State University. It has been accepted for inclusion in Graduate Theses and Dissertations by an authorized administrator of Digital Repository @ Iowa State University. For more information, please contact digirep@iastate.edu.
Black-box test case generation from TFM module interface specifications and usage statistics

by

Katsuya Iwata

A thesis submitted to the graduate faculty in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE

Major: Computer Science

Program of Study Committee:
David M. Weiss, Major Professor
Andrew S. Miner
Srikanta Tirthapura

Iowa State University
Ames, Iowa
2012
Copyright © Katsuya Iwata, 2012. All rights reserved.
DEDICATION

I dedicate this thesis to my wife Harumi without whose support I would not have been able to complete this work. I also dedicate this thesis to my family, friends, and coworkers in Canon Inc. whose loving attention, thought, and guidance encouraged me before and during my graduate education.
# TABLE OF CONTENTS

## LIST OF FIGURES

<table>
<thead>
<tr>
<th>List of Figures</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>v</td>
</tr>
</tbody>
</table>

## ACKNOWLEDGEMENTS

<table>
<thead>
<tr>
<th>Acknowledgements</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>vi</td>
</tr>
</tbody>
</table>

## CHAPTER 1. INTRODUCTION

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1</td>
<td>Goal of this thesis</td>
<td>1</td>
</tr>
<tr>
<td>1.2</td>
<td>Structure of this thesis</td>
<td>3</td>
</tr>
</tbody>
</table>

## CHAPTER 2. BACKGROUND

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1</td>
<td>Software Testing Technique</td>
<td>4</td>
</tr>
<tr>
<td>2.2</td>
<td>Formal Specification Technique</td>
<td>7</td>
</tr>
<tr>
<td>2.3</td>
<td>Statistical Software Testing Technique</td>
<td>17</td>
</tr>
</tbody>
</table>

## CHAPTER 3. APPROACH

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1</td>
<td>TFM Module Interface Document for Component Testing and Integration Testing</td>
<td>23</td>
</tr>
<tr>
<td>3.1.1</td>
<td>Assumptions - Module Interface Specification</td>
<td>23</td>
</tr>
<tr>
<td>3.1.2</td>
<td>Module Interaction Trace Specification</td>
<td>24</td>
</tr>
<tr>
<td>3.1.3</td>
<td>Input and Output Specification</td>
<td>26</td>
</tr>
<tr>
<td>3.2</td>
<td>Statistics Document Development</td>
<td>29</td>
</tr>
<tr>
<td>3.3</td>
<td>Testing Trace Generation Method</td>
<td>31</td>
</tr>
<tr>
<td>3.3.1</td>
<td>Trace Postconditions</td>
<td>31</td>
</tr>
<tr>
<td>3.3.2</td>
<td>Monitored Variable Constraints</td>
<td>32</td>
</tr>
<tr>
<td>3.3.3</td>
<td>Test Case Generation Algorithm</td>
<td>33</td>
</tr>
</tbody>
</table>

## CHAPTER 4. EVALUATION

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1</td>
<td>Feasibility of Test Case Generation - Example Application: Floating Weather Station</td>
<td>37</td>
</tr>
</tbody>
</table>
## LIST OF FIGURES

2.1 Test Procedure .......................................................... 5  
2.2 Functions and Notations for Predicates (See Additional Definitions in Appendix A) .......................................................................................... 12  
2.3 Closed-form Solution for value - Conditional Expressions Format .................................................. 14  
2.4 TFM Module Interface Document for a Stack Module ...................................................................... 15  
2.5 Closed-form Solution for pushes - Conditional Expressions Format .............................................. 16  
3.1 Overview of Test Case Generation Process ..................................................................................... 21  
3.2 Overview of Testing Process ........................................................................................................ 22  
3.3 Primitive Functions on Event Descriptors .................................................................................... 25  
3.4 Upper-Face Only Module Interface ............................................................................................... 26  
3.5 Module Interface Specification .................................................................................................... 28  
3.6 Output Delegation ....................................................................................................................... 28  
3.7 Output Behaviors Definition of Module B with Statistics Annotations ........................................ 30  
3.8 Monitored Variable Constraints ................................................................................................. 33  
4.1 FWS simulator GUI .................................................................................................................... 38  
4.2 Generated Testing Trace (Test Case) ............................................................................................ 39  
B.1 FWS Module Hierarchical Structure .......................................................................................... 47  
B.2 FWS Uses Relation ................................................................................................................... 47  
C.1 SensorDriver module Before Transpose ..................................................................................... 49
I would like to take this opportunity to express my thanks to those who helped me with various aspects of conducting research and the writing of this thesis. First and foremost, Dr. David M. Weiss for his warm advice and guidance throughout this research and the writing of this thesis. His precise insights and extensive knowledge significantly enhanced my work. I also thank Ms. Laurel Tweed for her advice and suggestions on my writing. Her advice profoundly improved the structure and language of this thesis. I also thank Canon Inc. for giving the opportunity of studying computer science and the financial assistance during the writing of this work. I also thank my committee members for their efforts and contributions to this work: Dr. Andrew S. Miner and Dr. Srikanta Tirthapura. I additionally thank Dr. Hridesh Rajan for his guidance during my initial stage of my computer science study and Dr. Andrew S. Miner for his inspiring lecture.
CHAPTER 1. INTRODUCTION

This chapter explains the centrality of verification and testing to the software industry, the contribution of this thesis, and an overview of related work.

1.1 Goal of this thesis

Society is coming to use and rely more and more on computer systems, such as safety critical systems, business systems, home appliance systems, entertainment systems, and mobile systems. Our dependence on such computer systems raises people’s awareness of the social importance of the software quality in these systems. The quality of software is eventually determined when a product is released. A product manager usually has to make the decision on when to release a product using collected software quality data; however, because software is substantially complex, methods for measuring software quality are sometimes inadequate. Consequently, a product manager may be pressured to make a release decision to meet the product release schedule with uncertain software quality. This thesis proposes a statistical software testing technique [23, 42, 24, 25] to provide a rationale for software quality to help make this management decision.

Software quality is measured with verification and validation. Verification is a method used to ensure that a product is built correctly. Validation is a method to ensure that the correct product is built [6]. While both methods are important, this thesis will focus on verification. Well-known software verification techniques are testing, review, program proving, and model checking. This thesis will focus on testing. The number and importance of test cases that are performed in testing and the absence of errors during executing those test cases gives a measure of the confidence of software quality.
The problem of testing is that the combinatorial number of input values is exponential on the sum of the number of input variable bits, which is large; thus, testing all combinations of input values is usually impractical. Hence, many testing approaches to determine important testing input value combinations have been proposed. The black-box testing techniques [5, 26] in particular deliver benefits for testing large and complex software, since they only use specifications that abstract away details of source code.

The first issue of black-box testing is how to identify use cases to test. A use case is a detailed description of a sequence of transactions between system and actors that exist outside the system. Black-box testing lists testing input patterns that can be derived from specifications, such as requirement specifications or module interface specifications. In industry, testers usually identify use cases with the prediction of possible usages of the product; however, since testers perform the usage prediction individually and ad-hoc, the prediction depends on the testers' individual skills and preferences, which can cause uncertain software quality. Several researchers have suggested methods for improving this use cases identification. Jacobson [16] introduced a systematic process to identify use cases. His process incorporated UML use case diagrams and produced the use cases. However, since the description of use cases is written in a natural language, which has ambiguity, the exhaustive listing of all use cases is difficult. Some researchers proposed identification methods using formal specifications such as Z[2], VDM [1], and state machine [8]. By utilizing its formalism, they could generate an exhaustive list of use cases that are specified. However, since most specification languages are difficult to write because of their complicated model construction, they are rarely adopted in industry. Among them, Trace Function Method (TFM) is reportedly beneficial [33, 3, 37, 29]. It is formal but relatively intuitive, conforms to the information hiding principle [31], and has reader-friendly tabular format. In this thesis, we identify use cases with TFM specifications.

The second issue of black-box testing is how to prioritize test cases. The exhaustive listing of use cases of a large software component yields an intractable number of use cases. Development organizations have a limited time for testing cases; thus, we have to prioritize them to reduce the number of test cases to perform. Whittaker [42, 9] modeled the system as a discrete-time Markov chain where the transitions are user operations, and generated prioritized test cases.
with a random choice of transitions in the Markov chain; however, they left the discussion on how to identify states and transitions of the Markov chain as an open question. Woit [43] generated prioritized test cases from a list of pairs (event, class of system’s executed events) with an occurrence probability. The event is an invocation of an access program of a component. Although she introduced classes of executed events, she left room to discuss how to identify those classes. Musa [24, 25] proposed the operational profile, which profiles each user operation with its occurrence probability and importance and prioritizes user operations to test. Although this approach is reportedly beneficial [25], the identification of the set of user operations relies on an informal refinement process, which makes completing an exhaustive list of user operations a complex task.

In this thesis, we propose a black-box testing method that derives important test cases with usage statistics, and enables a product manager to make a release decision with a rationale, “the important use cases specified in the usage statistics are tested and have no error.” First, we propose a method to specify components with TFM module interface specifications. Then, we propose a way to associate module usage statistics with the TFM module interface specification. Finally, we propose a method to generate a prioritized list of black-box test cases for component testing and integration testing [5] from the TFM module interface specification with usage statistics.

1.2 Structure of this thesis

This thesis consists of seven sections. Chapter 2 describes the background of this research. Chapter 3 explains the proposed technique. Chapter 4 evaluates the proposed technique with an example application and chapter 5.1 discusses the limitations and improvements. Chapter 5.2 describes related work and comparisons with the proposed technique. Finally, chapter 5.3 summarizes this research, and suggests areas for further research.
CHAPTER 2. BACKGROUND

2.1 Software Testing Technique

Testing approaches are usually categorized as follows: unit testing, component testing, integration testing, system testing, acceptance testing, and regression testing [5, 26, 11]. Unit testing checks the correctness of behaviors of the smallest piece of software that can be independently tested. Component testing checks the correctness of behaviors of an integrated assembly of one or more units/components and associated data objects. A software unit is usually a module\(^1\). A component is a set of modules. In this thesis, we consider that unit testing is a particular case of component testing; thus any method applicable to component testing is applicable to unit testing. Integration testing checks the correctness of interactions among the components such as inter-component calls, returns, and data handling. System testing checks the existence or absence of required properties including non-functional properties such as performance, usability, and security. A built product or a major component is tested in system testing since nonfunctional properties usually can only be tested after the product or major component is built. Acceptance testing checks the conformance of the system to the latest user needs. When requirements changes are included in software, regression testing shows, by repetition of tests, that the software behaviors are unchanged except for the required changes. Although a testing procedure is usually ad hoc and individualized by the software application and organization, most organizations conduct their testing approach in the order described in Figure. 2.1 when they test a new product or changes. In this thesis, we focus and improve component testing and integration testing.

In component testing and integration testing, all errors\(^2\) can be detected if all the possible

\(^1\)Software projects are organized as a set of work assignments. A module is a work assignment [31].

\(^2\)An error is a design flaw or deviation from a desired or intended state [19]. A bug (fault) is an incorrect
Figure 2.1  Test Procedure

combination of input values are tested; however, testing all is usually impossible because the combinatorial number of input values is too high. For example, an input value in an integer variable domain has $2^b$ values where $b$ is the number of bits for an integer value. If we have $n$ integer variables, then the combinatorial number of input values is $2^b \times 2^b \times ... = 2^{nb}$. Thus, the number of the combinations of input values is exponential on the number of the bits of input variables and the number of input variables. Hence, we have to select only a partial set of input value combinations in practice.

A test case is a pair of input history and output values under a program execution environment. Test cases are selected using two approaches: black-box testing (functional testing) and white-box testing (structural testing) [5, 11]. Black-box testing is an approach to develop test cases for each equivalence class of input variables. The equivalence classes are documented in software specifications. White-box testing is an approach to develop test cases for each interesting code structure, such as conditional branches in source code. The limitation of white-box testing is that one cannot determine whether all equivalence classes are tested, since the source of test cases is the source code, which says nothing about the equivalence class specified.

3Each input variable is a time function and has a history.

4An equivalence relation is a relation that is reflexive, transitive, and symmetric. An equivalence class is a class for objects that satisfy an equivalence relation. If we partition the input value domain into equivalence classes (equivalence classes of input values), the testing result on one object in an equivalence class is the same as the testing result on any object in the equivalence class.
in the specification. The limitation of black-box testing is that even if all equivalence classes are tested, one cannot detect errors that are caused by incorrect coding for some input value combinations in an equivalence class. Accordingly, both test case development approaches should be used as long as possible; however, as the number of input and output variables, i.e. the size of component, grows, the total number of white-box and black-box test cases becomes, again, intractable. Therefore, many researchers have proposed approaches to selecting an important partial set of test cases. Among them, black-box testing especially delivers benefits to this problem solving, since it does not use the knowledge of source code, which is too detailed and large, but uses software specifications that abstract away details of source code.

As explained, black-box testing identifies equivalence classes and tests them. As in section 1.1, the first issue was identifying use cases, i.e. equivalence classes of input variables. Many researchers have proposed formal specification languages to specify equivalence classes of input variables exhaustively; thus, section 2.2 explains the formal specification technique. The second issue was prioritizing and selecting test cases. **Statistical software testing** is a testing method that performs the test case prioritization with usage profiles. **Profiling** is a program analysis technique that measures characteristics such as function call frequencies of usage and memory usage and produces a usage profile that shows the statistics. Section 2.3 summarizes this statistical software testing technique.

---

5Note the relation between a use case and an equivalence class of input variables is one-to-one mapping.
2.2 Formal Specification Technique

A description of a system is written or spoken accurate information about the system [32]. A document of a system is a written description, and should always have official status. A specification of a system is a description that specifies the required and intended (designed) properties of the system. As software and development organizations become larger, documenting specifications takes on a new significance: specification documents help a team of engineers 1) design; 2) review the design; 3) maintain the software with low cost; 4) make responsibilities clear; 5) make software easy to inspect, hence, easy to change and reuse; 6) reduce design flaws from incomplete design; 7) derive black-box test cases. Although the set of documents differs by development processes or development team organizations, development projects produce the following specification documents: 1) system requirements; 2) module structures; 3) module interfaces; 4) module internal design. As for the component testing and integration testing use, module structure and module interface specification documents give testers the correct (required and intended) behaviors of modules.

Although several definitions of the term, module exist, we use Parnas’ definition. Software projects are organized as a set of work assignments, and a module is a collection of programs to be implemented as a work assignment [31, 28]. Similar but different terms are component and class. In this thesis, we make a clear distinction between component, class and module. A component is a collection of programs distributed as a unit and used in several systems without modification [33]. A class in Object-oriented programming is a software element describing an abstract data type [6] and its partial or total implementation [22]. In other words, a module is a unit for work decomposition, a component is a unit for program deployments, and a class in Object-oriented programming is a unit for design or implementation. A module may include several components or classes. A component may include several modules or classes. A class may be used in several classes or components.

Modules are designed using the information hiding principle [31]. Information hiding [7] is a

---

6 An abstract data type is a set of objects defined by the list of operations, or features, applicable to these objects, and the properties of these operations. [22]

7 Encapsulation is a mechanism to bundle data with functions operating on that data. On the other hand, information hiding is a design effort to enable independent development and independent changes.
design principle in which each module is designed to hide its design decisions that are difficult or likely to change in future, so that one can change those decisions later, separately from the rest of modules. The design decisions may be concerned with data structures, procedures, hard-coded parameters, algorithms, etc.

A module is specified with a module interface specification, which may use a formal specification language. The module interface specifies input-output relations of the module. Many approaches for writing module interface specification have been proposed [40]. These approaches can be generally categorized by the orientation of their approach.

- **State-oriented:**
  Z [2] or VDM [1] is a language that describes system with input values, output values, state variables, and actions that changes the state variable’s value.

- **Process-oriented:**
  LOTOS, Estelle, or SDL [17] is a language that describes system as a set of processes.

- **Operation-oriented:**
  Algebraic representations, such as Type Algebra Theory, Larch/CLU, and Initial Algebra Theory, are languages that describe the semantics of operations with a set of axioms [40].

- **Behavior-oriented:**
  Trace representations, such as Trace Assertion Method (TAM) and Trace Function Method (TFM) [33, 3, 37, 29], are languages that describe outputs. TAM describes a set of axioms about traces, which is a history of inputs and outputs, and the final output. TFM describes outputs as functions on traces.

Whereas all representations except trace representations require the identification of inner-module data, trace representations require the specification of only externally observable module inputs and outputs. Thus, trace representations conform to the information hiding principle, which hides the inner design of modules, and are suitable for the module interface specification. In this thesis, we use trace representations.
Trace Assertion Method (TAM) identifies canonical traces and equivalence of traces [4]. TAM is not intuitive for engineers in practice because it is axiomatic. Parnas and Dragomiroiu proposed the Trace Function Method (TFM) [33], which specifies only output values with predicates on traces. Since TFM does not have canonical traces and equivalences of traces, it is a direct representation to the module input-output relations, and TFM has proven its usefulness in limited industrial cases [29, 30, 3, 37]. In this thesis, we utilize this TFM.

Then, how can we write and read TFM module interface specification? In trace representations, a software module is viewed as a state machine where state transitions occur at discrete points of time. TFM introduces the following terms [33]:

- An **event** is a transition trigger of the state machine. At an event, a software module performs the combination of the following:
  
  - Reading all of the input variable values;\(^8\)
  
  - Changing the inner state of the state machine;
  
  - Updating some of the output variable values.\(^9\)

- An **abbreviated event descriptor** \(^10\) is a set of tuples:
  
  - Input variable name and value before the event;\(^11\).
  
  - Output variables name and value after the event.

In this thesis, we call an abbreviated event descriptor an **event descriptor** for simplicity.

A possible syntax of event descriptors is described in BNF as follows:

---

\(^8\) These variables include global variables and input variables via access program arguments. Each variable is considered as a time function and has a value at an event.

\(^9\) These variables include global variables and output variables via return values of access programs.

\(^10\) A full event descriptor is values of all variables before and after the event. Variable values unchanged by events are also included in full event descriptors.

\(^11\) Access program names are considered as input variables. The value of the variable is the name of the access program.
event_descriptor ::= (PGM : func, parameter_list)

func ::= Name of an access program

parameter_list ::= parameter, parameter_list | parameter

parameter ::= 'input_variable < type > : value | output_variable' < type > : value

input_variable ::= Name of an input variable

output_variable ::= Name of an output variable

value ::= constant

The letter “_” means an empty string. “type” includes all data types and abstract data types that typed programming languages such as C, C++, and Java accept. With this syntax, an example event descriptor that has a function name myfunction, an input variable myin, a global variable myglobal, and an output variable myout is as follows:

(PGM:myfunction, 'myin<int>:100, 'myglobal<int>:10, myout'<int>:30, myglobal'<int>:10).

• A trace is a finite sequence of event descriptors. Possible representation of the trace with abbreviated event descriptors is as follows. The period concatenates two event descriptors.

(PGM:myfunction1, 'myin<int>:100, 'myglobal<int>:10, myout'<int>:30, myglobal'<int>:10).(PGM:myfunction2, 'myglobal<int>:10, myglobal'<int>:100)

This trace is equivalent to the following execution steps:

Step1. myfunction1 is called with myin=100, myglobal=10 and returned myout=30, myglobal=10.

Step2. myfunction2 is called with myglobal=10 and returned myglobal=100.

• A TFM module interface specification consists of the following:

   – A complete description\(^\text{13}\) of inputs and their data type (section 1 in Figure. 2.4);

\(^{12}\)In this thesis, a global variable is a variable that is shared among modules. Note that a global variable can be an input variable or an output variable

\(^{13}\)A description is complete when all required description for the document are described[33].
– A complete description of outputs and their data type (section 2 in Figure. 2.4);

– A complete description of access programs and event descriptors (section 3 in Figure. 2.4);

– A set of relations of the value of each output variable and the history of events. These relations are described with predicates in a tabular form (section 4 in Figure. 2.4);

– **Auxiliary functions**\(^{14}\) that are any functions to simplify the predicates, if desired (section 5 in Figure. 2.4);

– We may also associate the document with supplemental descriptions, such as design issues, document review questions, test cases, and others, for software development processes.

The output behaviors definition (section 4 in Figure. 2.4) specifies a “set of relations of the value of each output variable and the history of events.” In this definition, the output values are specified by conditioning the event history with predicates on traces. In this thesis, we refer to the predicates on traces as **trace predicates**. Trace predicates and output value definitions may use the following denotations, which are summarized in Figure 2.2 in detail.\(^{15}\)

1) **Primitive functions on event descriptors** that refer to data in an event descriptor;

2) Notations for an **empty trace** and the **trace concatenation**;

3) **Basic functions on traces** that traverse traces and return some data;

4) **Useful function generators on predicates and traces** that traverse traces and return some data that satisfies predicates.

The purpose of the basic functions and useful function generators are to make the predicate description compact. In addition to these functions or function generators, specification writers may add more **auxiliary functions** (section 5 in Figure. 2.4) to make descriptions as compact and readable as possible.

\(^{14}\) An example auxiliary function is \texttt{inIntegerRange}(x) ≡ (Lower bound value of int) ≤ x ≤ (Upper bound value of int). This function helps simplifying predicates that uses the range.

\(^{15}\) More denotations are summarized in Appendix A
Figure 2.2 Functions and Notations for Predicates (See Additional Definitions in Appendix A)
Example:

Figure 2.4 describes a possible TFM module interface document for a stack module. The stack module is simplified for an explanation, so it does not consider the case when the stack is full.

- TFM specifies the value of each output variable and the return of auxiliary functions in closed-form solutions (equations) at the output behaviors definition (section 4 in Figure 2.4) and auxiliary functions definition (section 5 in Figure 2.4). The output behavior definition is given as a set of functions whose domain is traces \( T \) and whose range is output values. The auxiliary function definition is given as a function whose domain is variable values or traces and whose range is some values.

TFM may use a tabular format. The tabular format to define output behavior definition and auxiliary function definition has two parts, the trace predicates columns that is immediately right of the equivalence symbol ‘\( \equiv \)’, and the value column that is enclosed by a heavy line. The tabular format is interpreted as meaning that, an output variable value or an auxiliary function return value is equal to a value in the value column if the trace predicates in the corresponding row of the trace predicates columns are true. For example, the definition of value in Figure 2.4 is equivalent to the conditional expressions shown in Figure 2.3. The definition of pushes in Figure 2.4 is equivalent to the ones shown in Figure 2.5. Note that the output value column may have recursive definitions, such as \( \text{pushes}(T_1,T_2) \equiv \text{pushes}(T_1,\text{subseq}(T_2)) \), to define the output value by traversing traces.

- In this stack module, the most recent PUSH event is canceled by a POP event. In order to make the output behavior definition compact, we defined the auxiliary function pushOnlyTrace that strips all canceled PUSH events and POP events and returns a trace that has only PUSH events that have not been removed by POP event. pushOnlyTrace also strips failed PUSH events (a PUSH event fails if its input value is out of the range).
In this thesis, values in the event descriptor definitions are described as ‘*’. For example, \((\text{PGM: TOP}, \text{value’}<\text{int}>:*\)). This ‘*’ means that the value may be any value in its variable data type.

\[
\text{value}(T) \equiv \begin{cases} 
\text{top}(p(1,T)) & \text{if } \text{PGM}(r(1,T))=\text{TOP} \\
\text{value}(p(1,T)) & \text{if } \text{PGM}(r(1,T))=\text{PUSH} \\
\text{value}(p(1,T)) & \text{if } \text{PGM}(r(1,T))=\text{POP} \\
\text{Undefined} & \text{if } T=\_ 
\end{cases}
\]

Figure 2.3 Closed-form Solution for value - Conditional Expressions Format
[Section 1] Input Variables Definition

<table>
<thead>
<tr>
<th>Variable Name</th>
<th>Data Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>in</td>
<td>int</td>
</tr>
</tbody>
</table>

[Section 2] Output Variables Definition

<table>
<thead>
<tr>
<th>Variable Name</th>
<th>Data Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>top</td>
<td>int</td>
</tr>
<tr>
<td>value</td>
<td>int</td>
</tr>
</tbody>
</table>

[Section 3] Access Programs and Event Descriptors Definition

<table>
<thead>
<tr>
<th>Program Name</th>
<th>Input Variable</th>
<th>Output Variable</th>
<th>Event Descriptor</th>
</tr>
</thead>
<tbody>
<tr>
<td>PUSH</td>
<td>in</td>
<td>top</td>
<td>(PGM: PUSH, 'in&lt;int&gt;:<em>,top&lt;int&gt;:</em>)</td>
</tr>
<tr>
<td>POP</td>
<td>_</td>
<td>top</td>
<td>(PGM: POP, top&lt;int&gt;:*)</td>
</tr>
<tr>
<td>TOP</td>
<td>_</td>
<td>value</td>
<td>(PGM: TOP, value&lt;int&gt;:*)</td>
</tr>
</tbody>
</table>

[Section 4] Output Behaviors Definition

\[
top(T) \equiv \begin{cases} 
\text{pushOnlyTrace}(T) = _ & \text{Undefined} \\
\text{pushOnlyTrace}(T) \neq _ & 'in(r(1,\text{pushOnlyTrace}(T)))
\end{cases}
\]

\[
\text{value}(T) \equiv \begin{cases} 
\text{PGM}(r(1,T)) = \text{TOP} & \text{top}(p(1,T)) \\
\text{PGM}(r(1,T)) = \text{PUSH} & \text{value}(p(1,T)) \\
\text{PGM}(r(1,T)) = \text{POP} & \text{value}(p(1,T)) \\
T = _ & \text{Undefined}
\end{cases}
\]

[Section 5] Auxiliary Functions Definition

\[
\text{pushOnlyTrace}(T) \equiv \text{pushes(_,T)}
\]

\[
\text{pushes}(T_1,T_2) \equiv \begin{cases} 
T_2 = _ & T_1 \\
(T_2 = _) \land \neg \text{noeffect(oldest}(T_2)) & \text{pushes}(T_1,\text{subseq}(T_2)) \\
(T_2 = _) \land \neg \text{noeffect(oldest}(T_2)) \land \text{PGM(oldest}(T_2)) = \text{PUSH} \land \text{PGM}(\text{oldest}(T_2)) = \text{POP} & \text{pushes}(_{1,\text{subseq}(T_2)}) \\
T_1 = _ & \text{pushes}(p(1,T_1),\text{subseq}(T_2))
\end{cases}
\]

\[
\text{noeffect}(e) \equiv [(\text{PGM}(e) = \text{PUSH}) \land \neg \text{inrange('in(e))}] \lor [\text{PGM}(e) = \text{TOP}]
\]

\[
\text{inrange}(i) \equiv (\text{Lower Bound Value of int}) \leq i \leq (\text{Upper Bound Value of int})
\]

Figure 2.4 TFM Module Interface Document for a Stack Module
\[
\text{pushes}(T_1, T_2) \equiv \begin{cases} 
T_1 \\
\text{pushes}(T_1, \text{subseq}(T_2)) \\
\text{pushes}(T_1, \text{oldest}(T_2), \text{subseq}(T_2)) \\
\text{pushes}(\_, \text{subseq}(T_2)) \\
\text{pushes}(p(1, T_1), \text{subseq}(T_2)) \\
\end{cases}
\]

if \( T_2 = \_ \)

if \( -(T_2 = \_) \land \text{noeffect}(\text{oldest}(T_2)) \)

if \( -(T_2 = \_) \land \text{noeffect}(\text{oldest}(T_2)) \land [\text{PGM}(\text{oldest}(T_2)) = \text{PUSH}] \)

if \( -(T_2 = \_) \land \text{noeffect}(\text{oldest}(T_2)) \land [\text{PGM}(\text{oldest}(T_2)) = \text{POP}] \land (T_1 = \_) \)

if \( -(T_2 = \_) \land \text{noeffect}(\text{oldest}(T_2)) \land [\text{PGM}(\text{oldest}(T_2)) = \text{POP}] \land \neg (T_1 = \_) \)
2.3 Statistical Software Testing Technique

Until the late 1970s, the goal of testing was to show that software worked. Myers [26] pointed out that one can corrupt the testing process with this goal as follows: the probability of showing that software does not work will increase as the software is tested, and hence, the software should be tested less. Another possible goal of testing was to find software errors (bugs). Since we do not know when in the future errors may occur, we do not know when to stop testing, and hence, cannot release products. In the 1980s, Beizer [5] claimed that the goal of software testing was to provide enough testing to ensure that the probability of failure can be accepted. He claimed that "enough" comes from a judgment of software reliability with a statistical measure. This is accomplished by statistical software testing.

Statistical software testing or statistical quality control is a testing method that constructs a predetermined number of test cases that are relatively more important than others [23, 42, 24, 25]. The importance is usually decided by considerations of the occurrence frequency and criticality of the use case. Specifically, statistical software testing develops usage statistics as usage profiles, prioritizes each usage with the statistics, and lists prioritized usages to test. Consequently, the absence of errors in the list of usages provides a statistical rationale for the certification of software quality.

Musa proposed to create the usage statistics for each pair (user group, system mode) to reduce the effect of population size to the statistics [24, 25]. A user group is an independent group of users, such as administrators or customers. A system mode is an independent coarse-grained state of the system, such as an error recovery mode, a daily use mode, or the nuclear power plant shutdown mode [17].

How are those statistics derived? They can be developed in two ways: measurements and estimations. First, the criticality can be derived only from estimations. If the product is a safety critical system, the estimation may come from a hazard analysis [19] of the system. A

---

16 **Reliability** is the probability that a component will perform its intended function satisfactorily for a prescribed time and under predetermined environmental conditions [19].

17 **Criticality** is the parameter that shows the severity of effect when the software part fails.

18 A **usage** is a use case. The relation between a use case and an equivalence class of input variables is one-to-one mapping; thus, the relation between a usage and an equivalence class of input variables is also one-to-one.
usage may be assigned a high criticality factor if found to cause hazards during hazard analysis. Alternatively, we may consider that usages with frequent bug fixes or modifications usually have bugs[27] [39], and hence, their criticality is larger than others.

Secondly, we have two options for deriving the occurrence probability. The first option is counting the occurrences of each usage during program executions and calculating their occurrence probabilities. The occurrence counting may be done with execution logs that are saved during a usage monitoring test to test the user interface or user satisfaction of products, or family of products[41] in the market, if possible. The second option for deriving it is estimations. The estimation should be done by a group of people who know the product usage well and can estimate the adequate occurrence probability of each equivalence class.

Example:

Consider an online sales system as an example. Assume that we want to develop usage statistics for the system.

- The system usages were identified as follows: \{Search products, Purchase products, Register selling products, Website appearance configuration, Database operations\}.
- The system had three groups of users: \{buyers, sellers, system administrators\}, and the respective groups had different ways of using the system.
- Three system modes were identified as follows: \{customer mode, maintenance mode, survey mode\}.

The number of people in the system administrators group was smaller than others, and although the survey mode was rarely used, it was important; thus, to avoid false prioritizations, we develop statistics for each user group to remove the factor of population size from the statistics.

---

19 Technically, the log embedding may be done with Aspect-Oriented Programming library such as AspectJ and AspectC++. If we want to insert logging code at compile-time, we may develop a compile-time logging code insertion program. If we want to embed logging code at run-time, run-time instrumentation mechanisms such as dynamic Aspect-Oriented Programming may be options.
Then, we measure/estimate and calculate each occurrence probability and criticality adequately, which is summarized as Table 2.1. This table is the usage statistics of the system.

Table 2.1 Example of Usage Statistics

<table>
<thead>
<tr>
<th>User Group</th>
<th>System Mode</th>
<th>Usage</th>
<th>Occurrence Probability (%)</th>
<th>Criticality (1..100)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Buyer</td>
<td>Customer Mode</td>
<td>Search products</td>
<td>80</td>
<td>20</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Purchase products</td>
<td>20</td>
<td>80</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Register selling products</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Website appearance configura-</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>tion</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Database operations</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Seller</td>
<td>Customer Mode</td>
<td>Search products</td>
<td>20</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Purchase products</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Register selling products</td>
<td>80</td>
<td>90</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Website appearance configura-</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>tion</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Database operations</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Administrator</td>
<td>Maintenance Mode</td>
<td>Search products</td>
<td>10</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Purchase products</td>
<td>10</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Register selling products</td>
<td>20</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Website appearance configura-</td>
<td>30</td>
<td>30</td>
</tr>
<tr>
<td></td>
<td></td>
<td>tion</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Database operations</td>
<td>30</td>
<td>50</td>
</tr>
<tr>
<td>Survey</td>
<td>Mode</td>
<td>Search products</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Purchase products</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Register selling products</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Website appearance configura-</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>tion</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Database operations</td>
<td>90</td>
<td>90</td>
</tr>
</tbody>
</table>
Then, the final issue is how to develop test cases using the usage statistics. In statistical software testing, a testing priority of each usage is calculated with the statistics, and is used to prioritize the usage. Algorithm 1 is an example algorithm for developing a prioritized list of usages, and hence, test cases. An example output for (user group, system mode)=(Administrator, Maintenance Mode) in Table 2.1 is shown in Table 2.2. A larger priority has a higher priority.

**Algorithm 1** Derive a prioritized list of usages (test cases) with usage statistics

**Input:** Usage statistics:

\[ Pr: \text{(User group)} \times \text{(System mode)} \times \text{(Usage)} \rightarrow \text{(Occurrence probability)} \]

\[ Cr: \text{(User group)} \times \text{(System mode)} \times \text{(Usage)} \rightarrow \text{(Criticality)} \]

**Output:** A list of pairs \((\text{usage}, \text{priority})\) in the priority descending order:

\[ L: \text{(Usage)} \times \text{(Priority)} \]

1: for each pair \((\text{user group } g_i, \text{ system mode } m_j)\) do
2: for each usage \(u_k\) of \((g_i, m_j)\) do
3: Calculate the priority \(p_k\) of \(u_k\).
   \[
   p_k = 100 \times \frac{Pr(g_i,m_j,u_k)}{\sum_{u_k \text{of } (g_i,m_j)} Pr} \times \frac{Cr(g_i,m_j,u_k)}{\sum_{u_k \text{of } (g_i,m_j)} Cr}
   \]
4: Insert \((u_k, p_k)\) to \(L\) between the elements \(l_1 = (u_1, p_1)\) and \(l_2 = (u_2, p_2)\) where \(p_1 \geq p_k \geq p_2\).
5: end for
6: end for

**Table 2.2** Example list of pairs \((\text{usage}, \text{priority})\)

<table>
<thead>
<tr>
<th>Usage</th>
<th>Priority (1..100)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database operations</td>
<td>15</td>
</tr>
<tr>
<td>Website appearance config</td>
<td>9</td>
</tr>
<tr>
<td>Register selling products</td>
<td>2</td>
</tr>
<tr>
<td>Search products</td>
<td>5</td>
</tr>
<tr>
<td>Purchase products</td>
<td>5</td>
</tr>
</tbody>
</table>

This example algorithm multiplies the occurrence probability and criticality of a usage to calculate its priority; however, the calculation method is not limited to this in the statistical software testing. We may choose an appropriate calculation method for each application.
CHAPTER 3. APPROACH

This thesis presents a new black-box test case generation method for component testing and integration testing. Figure 3.1 outlines the work presented in this thesis, and Figure 3.2 describes the overall data flow of component testing and integration testing. As shown in Figure 3.1, first, we get TFM module interface documents, measure or estimate usage statistics of modules, and associate them with the TFM module interface documents. These documents work as usage statistics documents. Finally, using the usage statistics document and a predetermined test plan that is a tuple (number of test cases, user type, system mode), we generate a prioritized list of black-box test cases for component testing and integration testing.

![Figure 3.1 Overview of Test Case Generation Process](image)

Note that Figure 3.2 omits some software design phases to give a rough view.
Figure 3.2 Overview of Testing Process
3.1 TFM Module Interface Document for Component Testing and Integration Testing

3.1.1 Assumptions - Module Interface Specification

**Definition:** A *trace specification* is an ordered pair (syntax specification, semantic specification), where a syntax specification is a decidable set\(^2\) of syntax sentences, and a semantic specification is a decidable set of assertions \(^3\).

In TFM, a conditional \{\text{trace predicates} \rightarrow \text{output value definition}\} in the output behaviors definition, i.e. an equation and its condition in the conditional expressions (Figure 2.3), is an assertion. Thus, the output behaviors definition has a decidable set of assertions and is the semantic specification.

**Definition:** A trace specification with its assertions \(\Gamma\) is **consistent** if there is no formula \(\theta\) such that \(\Gamma \vdash \theta\) and \(\Gamma \vdash \neg \theta\) \(^4\).

**Definition:** A trace specification with its assertions \(\Gamma\) is **total** if for any given trace constant \(T\), every output variables \(V\) has a constant \(a\), such that \(\Gamma \vdash (V(T) \equiv a)\), or \(V\) is defined as \((V(T) \equiv Undefined)\).\(^5\)

The rest of this thesis assumes that every module has consistent and total TFM specifications, which is written at the module interface design phase.\(^6\)

---

\(^2\) A *decidable set* is a set that has an algorithm that halts in a finite time to decide whether or not a given object is in the set. The decidable set is also called computable or recursive.

\(^3\) An *assertion* is a set of conditions that program states or variables must satisfy \(^15\).

\(^4\) An argument \(<\Gamma, \phi>\) where \(\Gamma\) is premises, and \(\phi\) is a conclusion is *derivable* if there is a deduction from some of its premises to its conclusion, which we denote as \(\Gamma \vdash \phi\) \(^38\).

\(^5\) Note a specification allows specifying partial functions.

\(^6\) The methodology to write or check TFM specifications is outside the scope of this project.
3.1.2 Module Interaction Trace Specification

We introduce an approach to write TFM module interface specification with module interactions. Conventional TFM module interface specifications have some syntax and semantics that complicate the specification of module interactions; thus, we relax them in section 3.1.2.1. Additionally, traces in TFM do not consider nesting events that appear in most test cases in integration testing. Therefore, we introduce new primitive functions in section 3.1.2.2.

3.1.2.1 Relaxation of Multiple Object Trace Representation

For component testing and integration testing, we want a single testing trace that has the information of the occurrence order of events on multiple objects; hence, we integrate traces of all objects and write it as $T$, and give an object name to any operation on the object via an input variable of the corresponding event.

Example:

An example is shown in the following trace. Two objects of Module A are instantiated in the first two events, and the rest of the events get their object value via each input variable.

$$
T = (PGM: ModuleA\_constructor, object' < ModuleA >: objectA1).
(PGM: ModuleA\_constructor, object' < ModuleA >: objectA2).
(PGM: ModuleA\_printHelloWorld, object < ModuleA >: objectA1).
(PGM: ModuleA\_printHelloWorld, object < ModuleA >: objectA2).
(PGM: ModuleA\_destructor, object < ModuleA >: objectA1).
(PGM: ModuleA\_destructor, object < ModuleA >: objectA2)
$$

\(^7\)When we say a trace constant $T$ in conventional TFM module interface specifications, $T$ is the trace of a primary object that we specify in the document. If the module interface contains interactions of two or more objects, the conventional TFM document separates each object’s trace with a notation $T.<objectname>$, where $<objectname>$ is the name of the object and $T.<self>$ is the trace of the primary object[33].
3.1.2.2 Nesting Event Trace

A **nesting event** is a sub event that is invoked by other events. We cannot represent nesting events with the current set of the primitive trace functions (which we reviewed in Chapter 2), because an event descriptor always requires the values of output variables, which we cannot derive until after all nested events are evaluated. Therefore, we separate an event that invokes other events into two. We adopt “InvokePGM” and “ReturnPGM” variable in addition to “PGM” variable and primitive functions, InvokePGM(e), ReturnPGM(e), and modified PGM(e) defined in Figure 3.3. Then, we specify all input variables in the event descriptor of InvokePGM and all output variables in the event descriptor of ReturnPGM.

**Example:**

The example is shown in the following trace. This example describes the procedure that ModuleA_main program calls the access programs of Module B, ModuleB_func1 and ModuleB_func2, and returns “True” via an output variable, “result’.”

\[ T = (InvokePGM: ModuleA_main, 'in < Boolean > : True). \]
\[ (PGM: ModuleB_func1, out' < Boolean > : True). \]
\[ (PGM: ModuleB_func2, out' < int > : 100). \]
\[ (ReturnPGM: ModuleA_main, result' < Boolean > : True) \]

### Primitive functions on event descriptors

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Function</th>
<th>Semantics</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>InvokePGM(e)</td>
<td>InvokePGM:{event descriptor}−(string)</td>
<td>A function that returns the name of the event invoker access program at the event descriptor e</td>
<td>If ( e = (InvokePGM:myfunc,'in&lt;int&gt;:100), ) then ( InvokePGM(e)=myfunc )</td>
</tr>
<tr>
<td>ReturnPGM(e)</td>
<td>ReturnPGM:{event descriptor}−(string)</td>
<td>If ( e = (ReturnPGM:myfunc,out'&lt;int&gt;:1), ) then ( ReturnPGM(e)=myfunc )</td>
<td></td>
</tr>
<tr>
<td>PGM(e)</td>
<td>PGM:{event descriptor}−(string)</td>
<td>A function that returns the name of the access program in the event descriptor e</td>
<td>If ( e = (PGM:myfunc,'n&lt;int&gt;:100,out'&lt;int&gt;:1 ) or ( e = (InvokePGM:myfunc,'n&lt;int&gt;:100), ) then ( PGM(e)=myfunc )</td>
</tr>
</tbody>
</table>

Figure 3.3 Primitive Functions on Event Descriptors
3.1.3 Input and Output Specification

A module interface has an upper-face and a lower-face[33]. The upper-face shows a service that the module provides. The lower-face shows interactions with other modules. Figure 3.4 describes a module interface that has only an upper-face. Module A receives the value of inputs and returns the value of output variables. Although Module A is designed to use Module B, the use of Module B is not the service of Module A; thus, the use of Module B is hidden at Module A’s interface.

![Module Interface Diagram](image)

**Figure 3.4 Upper-Face Only Module Interface**

The upper-face only module interface specification delivers many benefits to software design, coding, and testing[10, 20]; however, testers need the lower-face specification to answer the following questions that arise during integration testing[5]:

- Does any improper call or return sequence exist?
- Does any inconsistent handling of data objects exist?

The lower-face might be specified in other documents, such as module internal design documents. Users of Module A need information about the required resources such as libraries, back-end servers, and

---

8Users can see what a module does without referring to its design details. Architects do not need to make premature decisions on design details when they design architecture. Implementers can choose the most effective implementation after careful considerations of external behaviors. Designers can distinguish what they can change, e.g. replaceable algorithm, from what they cannot, i.e. required services. Testers can design black box test cases.

9Users of Module A need information about the required resources such as libraries, back-end servers, and
cation must be formally defined. Therefore, we specify module interactions formally in TFM module interface documents.

We specify the output variables of a module that are actually returned from the module, and specify the used program events in trace predicates. Figure 3.5 shows what to specify with specific variables. Note that a module interface no longer specifies all service’s output variables. Some of them are specified only in used modules. We call it output delegation. The benefits of the output delegation are as follows:

- It enables the separation of concerns at module interfaces since some output value specifications are delegated to the used modules that exclusively offer those output services.

- We still can derive all services of the module from its interface specification if we aggregate all outputs in its used modules and itself.

Note that trace predicates on input values can be mapped to Meyer’s precondition[21], and trace predicates on output values with invoked access programs and returned values from the invoked access programs can be mapped to postcondition.

Example:

An example TFM interface document is shown in Figure 3.6. In this example, Sequencer’s access program “run” provides a service to set a robot arm angle to a constant “100” degrees and return “True”. RobotArmDriver has “setAngleTo100” that controls the arm physically and sets its angle to “100”. Since “run” calls “setAngleTo100”, “result” has the trace predicate that includes “setAngleTo100.”
Sequencer Module Interface Specification

Import Module
RobotArmDriver

Access Program

<table>
<thead>
<tr>
<th>Program Name</th>
<th>Input Variable</th>
<th>Output Variable</th>
<th>Event Descriptor</th>
</tr>
</thead>
<tbody>
<tr>
<td>run</td>
<td>void</td>
<td>result:Boolean</td>
<td>{PGM:run, result&lt;Boolean&gt;}</td>
</tr>
</tbody>
</table>

Output Behaviors Definition

\[
\text{result}(T) \equiv \begin{cases} 
\text{PGM}(r(1,T)) = \text{setAngleTo100} & \text{PGM}(r(2,T)) = \text{run} & \text{ TRUE} \\
\text{PGM}(r(2,T)) \neq \text{run} & \text{result}(p(2,T), r(1,T)) \\
\text{PGM}(r(1,T)) \neq \text{setAngleTo100} & \text{result}(p(1,T)) \\
T = \text{Empty} & \text{Undefined} 
\end{cases}
\]

RobotArmDriver Module Interface Specification

Access Program

<table>
<thead>
<tr>
<th>Program Name</th>
<th>Input Variable</th>
<th>Output Variable</th>
<th>Event Descriptor</th>
</tr>
</thead>
<tbody>
<tr>
<td>setAngleTo100</td>
<td>void</td>
<td>angle:int</td>
<td>{PGM: setAngleTo100, angle&lt;int&gt;}</td>
</tr>
</tbody>
</table>

Output Behaviors Definition

\[
\text{angle}(T) \equiv \begin{cases} 
\text{PGM}(r(1,T)) = \text{setAngleTo100} & 100 \\
\text{PGM}(r(1,T)) \neq \text{setAngleTo100} & \text{angle}(p(1,T)) \\
T = \text{Empty} & \text{Undefined} 
\end{cases}
\]

Figure 3.5 Module Interface Specification

Figure 3.6 Output Delegation
3.2 Statistics Document Development

As we saw in Chapter 2, a black-box test case is developed for each equivalence class of input values. In trace representations, a trace includes all input values; thus, an equivalence class of input values has an one-to-one correspondence to an equivalence class of traces. How can we find equivalence classes of traces in a TFM document? TFM documents specify the value of each output variable in a closed-form solution. This closed-form solution has two types of right hand side: 1) an output value definition or 2) a recursive definition with trace transformation functions. For example, RobotArmDriver in Figure 3.6 has the following equations:

\[
\begin{align*}
\text{angle}(T) &\equiv 100 \quad \text{if } PGM(r(1,T)) = \text{setAngleTo100} \quad (3.1) \\
\text{angle}(T) &\equiv \text{angle}(p(1,T)) \quad \text{if } PGM(r(1,T)) \neq \text{setAngleTo100} \quad (3.2) \\
\text{angle}(T) &\equiv \text{Undefined} \quad \text{if } T = \text{Empty} \quad (3.3)
\end{align*}
\]

On the right hand side, the equation (3.1) and (3.3) has each output value definition, and the equation (3.2) has a recursive definition with a trace transformation function \(p(1,T)\). If the TFM document is total, the trace transformation function eventually transforms the trace \(T\) into the one that satisfies the predicates of an equation that has an output value definition on its right hand side, (3.1) or (3.3) in this example. Since an equivalence class of traces delivers the same output values, the equivalence class has an one-to-one correspondence to the equation with an output value definition.

Therefore, we associate usage statistics with each equivalence class of traces, which is an equation with the output value definition in TFM documents, to prioritize the test case for the equivalence class. Then, we develop the occurrence probability and criticality of each equation for each user type and system mode with the same approach as the one explained in Chapter 2, and use them to calculate a priority of each equivalence class of traces and generate test cases. For rest of this thesis, we make an assumption that reasonable occurrence probabilities and criticalities of each equivalence class of traces can be developed for each module.

\(^{10}\) An equivalence relation is a relation that is reflexive, transitive, and symmetric. An equivalence class is a set of objects that satisfies an equivalence relation. Any event history in an equivalence class derives the same output values.
**Example:** An example of the statistics annotated document is shown in Figure 3.7. This is an example module that controls a heater switch. If the room temperature \( \text{temperature} \) is less than or equal to 50°F, then the access program \( \text{func} \) turns on the heater switch, which is \( \text{heaterON} \equiv \text{true} \). This example says that the occurrence probability of the class that has \( \text{heaterON} < \text{boolean} : \text{true} \) is “60/100” and the one that has \( \text{heaterON} < \text{boolean} : \text{false} \) is “40/100.” The criticality of the class that has \( \text{heaterON} < \text{boolean} : \text{true} \) is “30/100” and the one that has \( \text{heaterON} < \text{boolean} : \text{false} \) is “70/100.” These values can be used to calculate a priority of each equivalence class of traces.

<table>
<thead>
<tr>
<th>Output Behaviors Definition</th>
<th>{User Type, System Mode}</th>
<th>Occurrence Probability</th>
<th>Criticality</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \text{heaterON}(T) \equiv )</td>
<td>( \text{PGM}(r(1,T)) = \text{func} ) ( \text{temperature}(r(1,T)) \leq 50 )</td>
<td>TRUE</td>
<td>60/100</td>
</tr>
<tr>
<td></td>
<td>( \text{temperature}(r(1,T)) &gt; 50 )</td>
<td>FALSE</td>
<td>40/100</td>
</tr>
<tr>
<td></td>
<td>( \text{PGM}(r(1,T)) \neq \text{func} )</td>
<td>( \text{heaterON}(p(1,T)) )</td>
<td>-</td>
</tr>
</tbody>
</table>

Figure 3.7  Output Behaviors Definition of Module B with Statistics Annotations
3.3 Testing Trace Generation Method

3.3.1 Trace Postconditions

To generate testing traces, we “symbolically” execute [18] TFM module interface specification using usage statistics, we construct testing traces, and we aggregate constraints of input values. Before we propose a test case generation algorithm, we introduce new concepts, trace postconditions and monitored variable constraints. A trace postcondition is a conditional whose antecedent is a trace constant with a last event that has unevaluated output values, and whose consequent is a trace constant all of whose output values are evaluated. This evaluated means that some value or meta-variable is assigned to all output variables of the event. A meta-variable is a variable that is replaced by a constant in the test case generation algorithm that will presented in section 3.3.3. An example trace postcondition is as follows:

\[
T.\left( \text{PGM}: \text{func}, \ 'in < \text{int} > : a, \ out' < \text{int} > : \text{UNEVAL} \right) \rightarrow \\
T.\left( \text{PGM}: \text{func}, \ 'in < \text{int} > : a, \ out' < \text{int} > : a \right)
\]

“a” is a meta-variable. This conditional means that if a trace constant ends with an event descriptor (PGM:func, ‘in<int>:a, out'<int>:*) whose out’ is “UNEVAL” (unevaluated), then, the trace constant after the evaluation of the last event will be the consequent of the conditional whose out’ has the meta-variable “a”.

Another case of the trace postcondition is when an event invokes other modules’ access programs. As section 3.1.2.2 explained, we evaluate such an event to a separated pair of InvokePGM and ReturnPGM with its invoked events in the middle. For example, if Module A’s access program funcA invokes funcB that is an access program of Module B, its trace postcondition is as follows:

\[
T.\left( \text{PGM}: \text{funcA}, \ \text{result}' < \text{Boolean} > : \text{UNEVAL} \right) \rightarrow \\
T.\left( \text{InvokePGM}: \text{funcA} \right). \\
(PGM : \text{funcB}, \text{UNEVAL}). \\
(ReturnPGM : \text{funcA}, \ \text{result}' < \text{Boolean} > : \text{True})
\]
Here, “funcB” has the output “UNEVAL” that means any outputs can occur. This is because we delegate output tasks to “funcB” and the evaluation of Module A’s event does not clarify the outputs of “funcB” unless they are handled as the return values of funcB and inputs to Module A in the interface specification of Module A. The formal syntax of trace postconditions is as follows in BNF:

\[
\text{postcondition} ::= \text{T.trUneval} \rightarrow \text{T.trEval} \\
\text{trUneval} ::= e\text{Uneval} \\
\text{trEval} ::= e\text{Eval}|e\text{Eval}.\text{trEval} \\
\text{eUneval} ::= (\text{PGM} : \text{func}, \text{in}, \text{outUneval}) \\
\text{eEval} ::= (\text{programVar} : \text{func}, \text{in}, \text{outEval}) \\
\text{programVar} ::= \text{PGM}|\text{InvokePGM}|\text{ReturnPGM} \\
\text{func} ::= \text{Name of an access program} \\
\text{in} ::= i, \text{in}|i|_\text{inVar<type>}:\text{val} \\
\text{i} ::= \text{inVar<type>}:\text{UNEVAL} \\
\text{inVar} ::= \text{Name of an input variable} \\
\text{outUneval} ::= o\text{Uneval}, o\text{Uneval}|o\text{Uneval}|_\text{oUneval} \\
\text{outEval} ::= o\text{Eval}, o\text{Eval}|o\text{Eval}|_\text{oEval} \\
\text{oUneval} ::= o\text{Var<type>:UNEVAL}|\text{UNEVAL} \\
\text{oEval} ::= o\text{Var<type>:val} \\
\text{outVar} ::= \text{Name of an output variable} \\
\text{val} ::= \text{constant}|\text{meta variable}
\]

### 3.3.2 Monitored Variable Constraints

Inputs can be categorized into the following two variables:\(^{11}\):

- A **monitored variable** that is a variable whose value is determined externally. Physical values, such as sensor data, are the values of the monitored variables.

\(^{11}\)These names correspond to the variable names defined in the four-variable model[34, 36].
• An **input variable** that is a variable whose value is derived from access programs of other modules.

Input variable values are determined by software itself, so they are derivable from its specification; however, monitored variable values are derivable as domains, not values. The domains are specified as constraints in TFM documents. We call the collection of these constraints as **monitored variable constraints**. An example is shown in Figure 3.8. Consider the input variable \( 'temperature \) is the monitored variable. The value of \( 'temperature \) is not specified for each equivalence class of traces, but its monitored variable constraints are specified as “\( 'temperature \leq 50 \)” or “\( 'temperature > 50 \).”

![Output Behaviors Definition](image)

**Figure 3.8** Monitored Variable Constraints

### 3.3.3 Test Case Generation Algorithm

Finally, we generate test cases with the following steps:

**Step1.** Derive trace postconditions for each equivalence class of traces from the TFM module interface specifications.

Derive monitored variable constraints for each equivalence class of traces from the TFM module interface specifications.

**Step2.** Initialize an output trace \( T_{test} \) with a given start event.

**Step3.** For the oldest unevaluated event in \( T_{test} \), query the TFM module interface specification and get equivalence classes of traces that have **possibly-satisfiable** trace predicates on a given trace constant. A **possibly-satisfiable** trace predicate is a predicate that can be satisfied in future event evaluations, i.e. value or meta-variable assignments to variables. (Stage 0, i or i+2 in appendix D)
Step 4. Choose one equivalence class of traces randomly using the usage statistics.

Get the consequent of the trace postcondition that is associated with the chosen equivalence class of traces, and insert the consequence of the trace postcondition into $T_{test}$.

Get the monitored variable constraints that are associated with the chosen equivalence class of traces, and add the constraints to the monitored variable constraints collection.

(Stage 0, i+1 or i+2 in appendix D)

Step 5. Repeat Step 3-4 until all events in $T_{test}$ are evaluated or the length of $T_{test}$ reaches the predetermined length in a test plan.

Step 6. Generate monitored variable values using monitored variable constraints and a certain probability distribution. (Stage i+3 in appendix D) \(^{12}\)

Note that the query in step 3 may return several possibly-satisfiable predicates, since an event is nondeterministic until all its nesting events are evaluated and all monitored variables are determined. The detailed pseudo-code is described in algorithm 2, 3, 4. An example testing trace generation will be described in section 4.1.

---

**Algorithm 2 Testing Trace Generation**

1. **Input** Name of a program to invoke: $f$ and Name of its module: $m$
2. **Input** Usage statistics specifications for a particular user type and system mode: $S$ and Trace max length: $l$
3. Initialize a trace $T_{test}$ with $\{(PGM : f, *)\}$
4. Initialize a list of monitored variable constraint expressions $CONS$ with $Empty$
5. Initialize a key-value map of meta variable and value $VARS$ with $Empty$
6. **CALL** EventEvaluation (See Algorithm 3) with $T_{test}, srcIndex = 0, S, l, CONS, VARS$ and **UPDATE** $T_{test}, CONS, VARS$
7. Generate the value of monitored variables to satisfy $CONS$ and set them in $VARS$
8. Replace meta variables in $T_{test}$ with the corresponding values in $VARS$
9. **Output** $T_{test}$ and return

---

\(^{12}\)The probability distribution may be any distribution that has some rational. It may be a uniform distribution if we want to uniformly test input values in the domain.
**Algorithm 3 EventEvaluation**

1. **Input** A trace: $T$ and an event index of $T$ to evaluate: $srcIndex$
2. **Input** Usage statistics specifications: $S$ and Trace max length: $l$
3. **Input** A list of monitored variable constraint expressions: $CONS$
4. **Input** A key-value map of meta variable and value: $VARS$

   /*Part1. Append events produced by the event at $srcIndex$ in $T$*/
5. **CALL** QueryPossiblySatisfiableEquivalenceClasses with the sub-list of $T$ between 0 and $srcIndex$, function name at $srcIndex$ in $T$, module name at $srcIndex$ in $T$, $CONS$, and $VARS$ and 
   **OBTAIN** all candidate equivalence classes (i.e. equations with an output value definition) 
   that the sub-list of $T$ between 0 and $srcIndex$ will be classified with any future events 
6. Randomly select an equivalence class $ec$ from the all candidate equivalence classes using each 
   occurrence probability and criticality 
7. Overwrite or insert the events in the trace postcondition consequence of $ec$ to $T$. The events 
   whose index exceeds the trace length upper bound $l$ are truncated. 
8. Add the monitored variable constraints of $ec$ to $CONS$
9. if the index exceeds the upper bound length $srcIndex > l$ then 
10. **Output** $T, CONS, VARS$ and return 
11. end if

   /*Part2. Append events produced by all nested events*/
12. Increment $srcNextIndex = srcIndex + 1$
13. Initialize $lastIndex = srcIndex$
14. **for** all of the inserted nested events **do**
15. **CALL** EventEvaluation with $T_{test}, lastIndex, S, l, CONS, VARS$ and 
16. **UPDATE** $T, lastIndex, CONS, VARS$
17. **CALL** QueryPossiblySatisfiableEquivalenceClasses (See Algorithm 4) with the 
   sub-list of $T$ between 0 and $lastIndex$, function name of the event at $srcIndex$ in $T$, 
   module name of the event at $srcIndex$ in $T$, $CONS$, and $VARS$ and 
   **OBTAIN** all candidate equivalence classes that the sub-list of $T$ between 0 and 
   $lastIndex$ will be classified with any future events 
18. Randomly select an equivalence class $ec$ from the all candidate equivalence classes using 
   each occurrence probability and criticality 
19. Increment $srcNextIndex = srcNextIndex + 1$
20. Overwrite the sub-list of the produced trace in $ec$’s trace postcondition consequence 
   between $srcNextIndex$ and the last element index onto $T$ from the position of $lastIndex$. 
21. **end for**
22. if ReturnPGM(event at $lastIndex$ in $T \neq $ null) then 
23. Increment $lastIndex = lastIndex + 1$
24. end if
25. **Output** $T, lastIndex, CONS, VARS$ and return
Algorithm 4 QueryPossiblySatisfiableEquivalenceClasses

1: **Input** A trace: $T$
2: **Input** Name of a program to invoke: $f$ and Name of its module: $m$
3: **Input** Usage statistics specifications: $S$
4: **Input** A list of monitored variable constraint expressions: $CONS$
5: **Input** A key-value map of meta variable and value: $VARS$
6: In $m$’s module interface specification in $S$, find and get equations (pairs of an output value definition and its trace predicates), $eq$, that have the trace postcondition for $f$
7: for each equation $eq$ do
8:    Initialize $T_{temp} = T$
9:    **REEXAMINE TRANSFORMED:**
10:   Extract the preconditions of the last event in $T_{temp}$ from $eq$’s predicate
11:   Check whether $T$ with $CONS$ and $VARS$ satisfies the preconditions with a predicate solver
12:   if satisfied then
13:      if the output value of $eq$ is a trace transformation function then
14:         Transform $T_{temp}$ with the trace transformation function in the output value definition of $eq$
15:         **GO TO** REEXAMINE.TRANSFORMED to reexamine the transformed trace $T_{temp}$
16:      else
17:         Add $eq$ to the set of equations $SATEQ$
18:      end if
19:   end if
20: end for
21: **Output** the equivalence classes that correspond to $SATEQ$ and return
CHAPTER 4. EVALUATION

4.1 Feasibility of Test Case Generation - Example Application: Floating Weather Station

This section describes an example application to show that the proposed test case generation is feasible. Floating weather stations (FWS) are buoys that are deployed at sea and monitor the wind speed and periodically report the data via radio. The family of FWS is developed with the FAST (Family-Oriented Abstraction, Specification, and Translation) process [41]. As example software, we derived a member of FWS family that has a whale sensor. The whale sensor monitors whales with sonars, and its sensor driver program returns true if it detects whales.

The software system consists of 7 modules. The size of the program coded in Java is 10 classes, 38 methods, and 400 LOC. We ran the program with a FWS simulator program (Figure 4.1) written in Java (this work used the simulator code in [41]).

The module structure and representative process structure is presented in the module guide, the module hierarchical structure, and the uses relation in Appendix B. Although the original FWS family member has multiple threads, this example system is single-threaded for simplicity.

The usage statistics, trace postconditions, and monitored variable constraints are presented in Appendix C. The pair of expected user type and system mode is limited to one pair for simplicity. We measured occurrence probabilities with a simulator execution recording that prints out and records event descriptors as a log using Java reflection, JavaVM stack tracing, and hard-coding to get variable names and values. We set all criticality values at the same value for simplicity; thus, we used only occurrence probabilities for prioritizing. Trace postconditions and monitored variable constraints are derived as presented in section 3.3.3. In this example, we
derived trace postconditions and monitored variable constraints from trace predicates manually, but we could automate this derivation process since all trace postconditions are defined formally in trace predicates.

Consider that we test an access program \texttt{FWS\_init} with a maximum testing trace length 37. The service of \texttt{FWS\_init} is periodically receiving the sensor value five times and transmitting the averaged sensor value. We performed the test case generation algorithm and derived one test case shown in Figure 4.2. Detailed intermediate states in the test case generation algorithm are described step-by-step in appendix D. The nesting events are indented. The monitored variable values that testers have to create are enclosed by a thin line, and the service output is enclosed by a heavy line.

Testers can 1) determine how they should input monitored variable values; 2) check whether the program returned the service output values as indicated in the testing trace (in Figure 4.2, the output of \texttt{TransmitDriver\_sendWindSpeed} is the service output.); 3) check whether their testing program produced the sequence of events as indicated in the testing trace. Checking the service output values corresponds to component testing, and checking the sequence of events corresponds to integration testing; thus, testers can perform component testing and integration testing with the generated testing trace.
Figure 4.2 Generated Testing Trace (Test Case)
4.2 Computation Termination and Efficiency of Test Case Generation

Algorithm

Algorithm 2 **does not halt** if there exists a recursive output value definition that does not have a solution. In this case, algorithm 4 (line 14) will evaluate recursion infinitely many times and does not terminate. However, such a recursive output value definition does not exist if the TFM specification is **total** (as explained in section 3.1.1). Except for such a case, algorithm 2 **halts** either when the number of event descriptors in a generated trace reaches a threshold, or when an initial access program that we input to the algorithm returns its outputs.

Algorithm 2 (line 7) is **NP-complete** if a set of monitored variable constraints $CONS$ makes a satisfying assignment as hard as 3-SAT or other NP-complete problems. If monitored variable value assignments are not as hard as NP-complete problems, the efficiency of algorithm 2 is calculated as follows and is **polynomial time**:

Consider $l_{\text{max}}$ is the maximum length of testing trace that is predetermined in a test plan, $b_{\text{max}}$ is the maximum number of equations in the simultaneous equations of the output behavior definition, $s_{\text{max}}$ is the maximum time for solving a trace predicate on a trace constant, $|V|$ is the number of all monitored variables.

Since the length of the output testing trace has an upper-bound $l_{\text{max}}$, the running time of algorithm 4 is $Q = O(l_{\text{max}}s_{\text{max}}b_{\text{max}})$, the running time of algorithm 3 is $E = O(l_{\text{max}}^2s_{\text{max}}b_{\text{max}})$, and the running time of algorithm 2 is $O(E + |V|) = O(l_{\text{max}}^2s_{\text{max}}b_{\text{max}} + |V|)$, which is polynomial time.
CHAPTER 5. CONCLUSION AND SUMMARY

5.1 Limitations and Improvement Idea

To adopt the presented approach, we needed to 1) identify modules and 2) prepare module interface specification documents in TFM. Identifying modules is difficult if performed on some ongoing software development projects with unidentified modules, but a large amount of code. In this case, we might have to refactor the software to identify them. Preparing TFM module interface documents is also difficult without strong tool support such as a trace predicate consistency checker, totalness checker, and editor tool with auto completions. We should develop these tools in future.

Second, we needed to measure or estimate usage statistics. The estimation is difficult if the module interface is complicated. If we visualize the behavior in other representations that are better at the graphical visualization, such as sequence diagrams and behavior animations, the prediction will be easier. The measurement is difficult if we do not want to sacrifice the program execution speed for recording the execution log. We may activate the logging only at the recording phase and deactivate it when we release the product; however, some behaviors may change if the execution timing changes because of logging. Thus, we need a practical solution for those behavior recordings in future.

Third, we generated test cases in traces. Testers need to follow the event sequence in traces and execute the program. In order to facilitate the testing process, we should develop a harness program that drives the target programs along a given testing trace, much as Hoffman proposed a harness program for a single module testing trace [12].

Fourth, the proposed test case generation algorithm aggregates monitored variable constraints and finds a monitored variable value assignment that satisfies the set of constraints;
thus, the test case generation algorithm can be NP-complete (as discussed in section 4.2). If possible, such a set of monitored variable constraints should be avoided when we write specifications. TFM module interface specification editor tools should have a constraints difficulty check capability and warn users of the difficulties of satisfying assignments.

Finally, we have considered only single-threaded programs, not multi-threaded programs. If we accommodate multi-threaded programs, we might need to introduce additional functions to be used in predicates such as a function that returns thread ID. Furthermore, we might need to simulate the thread dispatching mechanism in the test case generator. These are all considerations for future work.

### 5.2 Related Work

We proposed a method to specify module interactions with TFM. Module interactions are usually specified with UML sequence diagrams. Since a UML sequence diagram is a graphical representation, especially if the interaction has conditional branches, the diagram becomes large and its layout poor. As a practical alternative, our proposed method not only expresses interactions with text of trace predicates in tabular format, which is compact, but is relatively easy to exhaustively specify.

Many CASE tools incorporate test case generation into a state machine based specification framework [14, 8, 7]. In particular, MaTeLo has a feature to input usage profiles and generate test cases. Its approach is similar to Whittaker’s approach [42, 9]. However, since they are based on Markov chains, we need to identify the states of modules that are not externally visible and do not conform to the information hiding principle. In our approach, we identify only externally visible events to the module, which conforms to the information hiding and is beneficial, as explained in Section 3.1.3.

Our oracle\(^1\) is based on the satisfaction of the trace predicate. Hoffman’s approach [12] generated test cases for single modules with module interface specifications as oracle. Peters’ approach [35] generated oracles for single modules with LD-relation specification. However,\(^1\)Oracle is any means that provides information about the (correct) expected behavior of a component [13].
none of them generated the oracle or test cases for multiple modules, i.e. component testing and integration testing.

5.3 Summary

We proposed a black-box testing method that derives important test cases from usage statistics. The method specified large components with TFM module interface specifications and associated module usage statistics with the TFM module interface specification. Finally, we showed that the method could generate a prioritized list of testing traces for component testing and integration testing from the TFM module interface specification with usage statistics.

Consequently, the proposed method enables a product manager to make a release decision with a rationale, “the important use cases specified in the usage statistics are tested and have no error.”
APPENDIX A.  FUNCTIONS AND NOTATIONS FOR PREDICATES
### Primitive functions on event descriptors

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Function</th>
<th>Semantics</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>PGM(e)</code></td>
<td><code>PGM(event descriptor) → (string)</code></td>
<td>A function that returns the name of the access program in the event descriptor <code>e</code></td>
<td><code>if e=(PGM:myfunc:in=nt&gt;100, out&lt;nt&lt;1), then PGM(e)=myfunc</code></td>
</tr>
<tr>
<td><code>V(e)</code></td>
<td><code>V(event descriptor) → (data type of V)</code></td>
<td>A function that returns the value of <code>V</code> before the event of the event descriptor <code>e</code> (if <code>e</code> may be any input variable)</td>
<td><code>if e=(PGM:myfunc:in=nt&gt;100, out&lt;nt&lt;1), then in(e)=100</code></td>
</tr>
<tr>
<td><code>V(e)</code></td>
<td><code>V(event descriptor) → (data type of V)</code></td>
<td>A function that returns the value of <code>V</code> after the event of the event descriptor <code>e</code> (if <code>e</code> may be any output variable)</td>
<td><code>if e=(PGM:myfunc:in=nt&gt;100, out&lt;nt&lt;1), then out'(e)=1</code></td>
</tr>
</tbody>
</table>

### Notation for traces

<table>
<thead>
<tr>
<th>Notation</th>
<th>Semantics</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>__</code></td>
<td>This is an empty trace.</td>
</tr>
<tr>
<td><code>T1.T2</code></td>
<td>A period <code>.</code> concatenates two traces.</td>
</tr>
</tbody>
</table>

### Basic functions on traces

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Function</th>
<th>Semantics</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>Len(T)</code></td>
<td><code>Len(trace) → (integer)</code></td>
<td>A function that returns the length of the trace <code>T</code> (the number of event descriptors in the trace)</td>
<td><code>if T=E1.E2.E3 where E1 is an event descriptor, Len(T)=3.</code></td>
</tr>
<tr>
<td><code>r(n, T)</code></td>
<td><code>r(integer) × (trace) → (event descriptor)</code></td>
<td>A function that returns the nth most recent event descriptor in the trace <code>T</code>. <code>r(n)=Undefined.</code></td>
<td><code>if T=E1.E2.E3 where En is an event descriptor, r(1,T)=E3, r(2,T)=E2, r(3,T)=E1, r(4,T)=Undefined.</code></td>
</tr>
<tr>
<td><code>oldest(T)</code></td>
<td><code>oldest(trace) → (event descriptor)</code></td>
<td>A function that returns the first (oldest) event descriptor in the trace <code>T</code>. <code>oldest(T)=E1.</code></td>
<td><code>if T=E1.E2.E3 where En is an event descriptor, oldest(T)=E1.</code></td>
</tr>
<tr>
<td><code>p(n, T)</code></td>
<td><code>p(integer) × (trace) → (trace)</code></td>
<td>A function that returns the prefix trace of <code>r(n, T)</code> in the trace <code>T</code>. <code>p(0)=Undefined.</code></td>
<td><code>if T=E1.E2.E3 where En is an event descriptor, p(1,T)=E1.E2, p(2,T)=E1, p(3,T)=E1</code></td>
</tr>
<tr>
<td><code>subseq(T)</code></td>
<td><code>subseq(trace) → (trace)</code></td>
<td>A function that returns the trace <code>T'</code> such that <code>subseq(T)=E2.E3</code></td>
<td><code>if T=E1.E2.E3 where En is an event descriptor, subseq(T)=E2.E3</code></td>
</tr>
<tr>
<td><code>r_call(pg, T)</code></td>
<td><code>r_call(string) × (event descriptor)</code></td>
<td>A function that returns the most recent event descriptor which access program name is <code>pg</code> in the trace <code>T</code></td>
<td><code>if T=E1.E2.E3 where En is an event descriptor, and </code>E1<code>is invoked by a program</code>pg<code>and</code>E2<code>and</code>E3<code>are not invoked by</code>pg<code>, then r_call(pg,T)=E1.</code></td>
</tr>
</tbody>
</table>

### Useful function generators on traces and predicates

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Function</th>
<th>Semantics</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>exist(P, T)</code></td>
<td><code>exist predicate × (trace) → (boolean)</code></td>
<td>A function that returns <code>true</code> if and only if there exists an event descriptor in <code>T</code> that satisfies <code>P</code>, otherwise <code>false</code>.</td>
<td><code>if T=E1.E2.E3 where En is an event descriptor, and </code>E1<code>satisfies</code>P<code>, then exist(P,T)=true.</code></td>
</tr>
<tr>
<td><code>c_st(P, T)</code></td>
<td><code>c_st(predicate) × (trace) → (event descriptor)</code></td>
<td>A function that returns the most recent event descriptor in <code>T</code> that satisfies <code>P</code>.</td>
<td><code>if T=E1.E2.E3 where En is an event descriptor, and </code>E1<code>, </code>E2<code>, and </code>E3<code>satisfy</code>P<code>, then c_st(P,T)=E3.</code></td>
</tr>
<tr>
<td><code>oldest_st(P, T)</code></td>
<td><code>oldest_st(predicate) × (trace) → (event descriptor)</code></td>
<td>A function that returns the first (oldest) event descriptor in <code>T</code> that satisfies <code>P</code>.</td>
<td><code>if T=E1.E2.E3 where En is an event descriptor, and </code>E1<code>, </code>E2<code>, and </code>E3<code>satisfy</code>P<code>, then oldest_st(P,T)=E1.</code></td>
</tr>
<tr>
<td><code>idx_c_st(P, T)</code></td>
<td><code>idx_c_st(predicate) × (trace) → (integer)</code></td>
<td>A function that returns the index of the most recent event descriptor in <code>T</code> that satisfies <code>P</code>. The index starts from <code>1</code>.</td>
<td><code>if T=E1.E2.E3 where En is an event descriptor, and </code>E1<code>, </code>E2<code>, and </code>E3<code>satisfy</code>P<code>, then idx_c_st(P,T)=3.</code></td>
</tr>
<tr>
<td><code>idx_oldest_st(P, T)</code></td>
<td><code>idx_oldest_st(predicate) × (trace) → (integer)</code></td>
<td>A function that returns the index of the first (oldest) event descriptor in <code>T</code> that satisfies <code>P</code>. The index starts from <code>1</code>.</td>
<td><code>if T=E1.E2.E3 where En is an event descriptor, and </code>E1<code>, </code>E2<code>, and </code>E3<code>satisfy</code>P<code>, then idx_oldest_st(P,T)=1.</code></td>
</tr>
<tr>
<td><code>extract(P, T)</code></td>
<td><code>extract(predicate) × (trace) → (trace)</code></td>
<td>A function that returns a trace that has only the event descriptors in <code>T</code> that satisfies <code>P</code>.</td>
<td><code>if T=E1.E2.E3 where En is an event descriptor, and </code>E1<code>and</code>E3<code>satisfy</code>P<code>, then extract(P,T)=E1.E3.</code></td>
</tr>
</tbody>
</table>
APPENDIX B.  FWS MODULE GUIDE

• Behavior-Hiding Modules

  – Controller
    Secret: How to control the execution sequence of FWS
  – MessageGenerator:
    Secret: How to obtain monitored data and transmit averaged data in a message

• Device Interface Modules

  – Sensor Device Driver
    Secret: How to monitor and control the wind speed sensors and whale sensors.
  – Transmitter Device Driver
    Secret: How to control the transmitter

• Software-Design-Hiding Modules

  – SensorMonitor
    Secret: How to obtain data from sensors and store it for later retrieval.
  – DataBanker
    Secret: How to store the most recent wind data and whale data
  – Averager
    Secret: How to process the current DataBanker data to produce a current wind data and whale data estimate
Figure B.1  FWS Module Hierarchical Structure

Figure B.2  FWS Uses Relation
APPENDIX C. FWS MODULE INTERFACE SPECIFICATION

Note: output behaviors definition and auxiliary function definition tables are transposed to save paper space. For example, the trace semantics part of SensorDriver module interface is equivalent to Figure C.1.
Trace Postcondition | Monitored Variable Constraints | Executed Count | Total Sample | Occurrence Probability
--- | --- | --- | --- | ---
sensorData(T) \equiv \text{Pre}([LT,SensorDriver_get]=\{True\}) \rightarrow \text{newSensorReading( windSpeed(r(i,T)), whalePassing(r(i,T)))} \rightarrow T.(\text{PGM}:\text{SensorDriver_get}, \text{windSpeed<int>:UNEVAL}, \text{whalePassing<Boolean>:UNEVAL}, \text{sensorData'<SensorReading>:UNEVAL}) 
\rightarrow T.(\text{PGM}:\text{SensorDriver_get}, \text{windSpeed<int>:aa}, \text{whalePassing<Boolean>:bb}, \text{sensorData'<SensorReading>:newSensorReading(aa,bb)})
INTMIN \leq aa \leq INTMAX, bb = TRUE v FALSE
114
114
100
V_j \{ \neg \forall (\text{Predicate}(i,j)) \} \rightarrow \text{Undefined} \rightarrow \text{Undefined}
- \rightarrow \text{0} \rightarrow \text{0} \rightarrow \text{0}
Module Index

<table>
<thead>
<tr>
<th><strong>Behavior Hiding</strong></th>
<th><strong>Controller</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Message Generator</strong></td>
</tr>
<tr>
<td><strong>Software Design</strong></td>
<td><strong>Sensor Monitor</strong></td>
</tr>
<tr>
<td><strong>Device Interface</strong></td>
<td><strong>Averager</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Data Banker</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Sensor Driver</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Transmit Driver</strong></td>
</tr>
</tbody>
</table>

Auxiliary Functions

<table>
<thead>
<tr>
<th><strong>Trace Predicates</strong></th>
<th>( R(i,T) = \text{evt} )</th>
<th>( R(i,T) \neq \text{evt} )</th>
<th>( R(i,T) = \text{Empty} )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \text{Prefix}(i,T,\text{evt}) \equiv { \text{TRUE},i } )</td>
<td>( \text{Prefix}(i+1,T,\text{evt}) \equiv { \text{FALSE},i } )</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Trace Predicates</strong></th>
<th>( R(i,T) = \text{evt} )</th>
<th>( R(i,T) \neq \text{evt} )</th>
<th>( R(i,T) = \text{Empty} )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \text{Postfix}(i,T,\text{evt}) \equiv { \text{TRUE},i } )</td>
<td>( \text{Postfix}(i+1,T,\text{evt}) \equiv { \text{FALSE},i } )</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| **suffix(i,T) \equiv \text{subseq}[T]** |

<table>
<thead>
<tr>
<th><strong>Trace Predicates</strong></th>
<th>'quit'</th>
<th>'quit'</th>
</tr>
</thead>
<tbody>
<tr>
<td>( r(i,i,T) \neq \text{Empty} ) if ( \text{id}_{\text{SensorMonitor}}(i,i,T) \neq \text{Empty} ) ( \text{PGM}(R(i,T))=(\text{MessageGenerator}_r_u_n,i,T) ) ( =\text{TRUE} )</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| **T.loopEvents() \equiv \text{T}** |
| \( \text{T} \equiv \text{T} \) |

<table>
<thead>
<tr>
<th><strong>Data Type</strong></th>
<th><strong>Type Name</strong></th>
<th><strong>Attributes</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>MessageFor matWind</strong></td>
<td><strong>windSpeed:int</strong></td>
</tr>
<tr>
<td></td>
<td><strong>MessageFor matWhale</strong></td>
<td><strong>whalePassing:Boolean</strong></td>
</tr>
<tr>
<td></td>
<td><strong>SensorReading</strong></td>
<td><strong>windSpeed:int</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>whalePassing:Boolean</strong></td>
</tr>
</tbody>
</table>
Controller Module Interface Specification

Trace Event Syntax

<table>
<thead>
<tr>
<th>Program Name</th>
<th>Input Variable</th>
<th>Output Variable</th>
<th>Event Descriptor</th>
</tr>
</thead>
<tbody>
<tr>
<td>FWS_&lt;init&gt;</td>
<td>quit:Boolean</td>
<td>NONE</td>
<td>{PGM:FWS_&lt;init&gt;, 'quit&lt;boolean&gt;:q}</td>
</tr>
</tbody>
</table>

Trace Semantics

<table>
<thead>
<tr>
<th>Trace Predicates</th>
</tr>
</thead>
<tbody>
<tr>
<td>idx_oldest_st(PGM[(1,T)]=FWS_&lt;init&gt;, T)=i0</td>
</tr>
<tr>
<td>(idx_oldest_st(PGM[(1,T)]=DataBanker_&lt;init&gt;, T)=i1 ∧ [0&lt;i1])</td>
</tr>
<tr>
<td>(idx_oldest_st(PGM[(1,T)]=MessageGenerator_&lt;init&gt;, T)=i2 ∧ [1&lt;i2])</td>
</tr>
<tr>
<td>(idx_oldest_st(PGM[(1,T)]=SensorMonitor_&lt;init&gt;, T)=i3 ∧ [2&lt;i3])</td>
</tr>
<tr>
<td>suffix(i3,T)=loopEvents()</td>
</tr>
<tr>
<td>len(extract( ([PGM=SensorMonitor_run]∧'(quit=FALSE), T ) )=n</td>
</tr>
<tr>
<td>Vj { ¬[∧i (Predicate (ij))] }</td>
</tr>
</tbody>
</table>

where i is a number of row in this table, and j is a number of column in this table, and i and j don't include this cell's number.

Output Behavior Definition

| NONE(T) ≡ NONE |

Trace Postcondition

| T. (PGM:FWS_<init>, 'quit<boolean>:qq)→ |
| (PGM:DataBanker_<init>). |
| (PGM:MessageGenerator_<init>,object'<MessageGenerator>:ob1,UNEVAL). |
| (PGM:MessageGenerator_run, 'obj<MessageGenerator>:ob1,UNEVAL). |
| >n (*See a note below) |
| (ReturnPGM:FWS_<init>) |

Undefined

Monitored Variable Constraints

qq=FALSE v TRUE

Executed Count

1 0

Total Sample

1

Occurrence Probability (%)

100 0

*Note: [T] × n is the abbreviation of n times repeated T sequence. For example, [T] × 3 means T.T.T. This notation is introduced here to save paper space.
### MessageGenerator Module Interface Specification

#### Trace Event Syntax

<table>
<thead>
<tr>
<th>Program Name</th>
<th>Input Event Descriptor</th>
<th>Output Event Descriptor</th>
<th>Event Descriptor</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;init&gt;</td>
<td>NONE</td>
<td>object:MessageGenerator</td>
<td>(PGM:MessageGenerator_&lt;init&gt;, object:MessageGenerator::*)</td>
</tr>
<tr>
<td>run</td>
<td>thisObj:MessageGenerator</td>
<td>NONE</td>
<td>(PGM:MessageGenerator::run, thisObj:SensorMonitor::*)</td>
</tr>
</tbody>
</table>

#### Trace Semantics

- Pre(T, MessageGenerator_<init> = [TRUE, 0])
- Post(T, MessageGenerator_run = [TRUE, 1] ^ Post(T, Average_getWindSpeed = [TRUE, 2])^ Post(T, TransmitDriver_send = [TRUE, 3] ^ Pre(T, Average_getWhale = [TRUE, 5]) ^ whalePassing'(r(4, T)) = whalePassing'(r(5, T)) ^ Pre(T, Average_getWhale = [FALSE, 5]) ^ Pre(T, Average_getWhale = [TRUE, 5]) ^ Post(T, TransmitDriver_sendToWhaleSurveyCenter = [TRUE, 5]) ^ msg(r(5, T)) = new MessageFormatWhale(TRUE))

- Post(T, Average_getWindSpeed = [TRUE, 4])
- Post(T, TransmitDriver_send = [TRUE, 3])
- Post(T, Average_getWhale = [TRUE, 5])
- Post(T, Average_getWhale = [TRUE, 5])
- Post(T, TransmitDriver_sendToWhaleSurveyCenter = [TRUE, 5])

#### Output Behavior Definition

| NONE(T) = NONE | NONE(T) = NONE | object(T) = new MessageGenerator | Undefined |

#### Trace Postcondition

- T.(PGM:Average_getWindSpeed = averageData' <int> = arg, UNEVAL).
- T.(PGM:Average_getWhale = whalePassing'(boolea = FALSE, UNEVAL).
- (ReturnPGM:MessageGenerator_<run>)

- T.(PGM:Average_getWindSpeed = averageData' <int> = arg, UNEVAL).
- (ReturnPGM:MessageGenerator<_run))

#### Executed Count

| 22 | 2 | 1 | 0 |

#### Total Sample

| 24 | 0 | 0 | 0 |

#### Occurrence Probability

| 91.667 | 8.333 | 100 | 0 |
**Sensor Monitor Module Interface Specification**

### Trace Event Syntax

<table>
<thead>
<tr>
<th>Program Name</th>
<th>Input Variable</th>
<th>Output Variable</th>
<th>Event Descriptor</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;init&gt;</td>
<td>NONE</td>
<td>object: SensorMonitor</td>
<td>(PGM:SensorMonitor_&lt;init&gt;=&gt;object '&lt;SensorMonitor&gt;:*')</td>
</tr>
<tr>
<td>run</td>
<td>thisObj: SensorMonitor</td>
<td>NONE</td>
<td>(PGM:SensorMonitor_run='thisObj &lt;SensorMonitor&gt;:*')</td>
</tr>
</tbody>
</table>

### Trace Semantics

**Trace Predicates**

- Pre(1, T, SensorMonitor_<init>) = {True,i0}
- Pre(1, T, SensorMonitor_<init>) = {True,i0}
- Pre(1, T, SensorMonitor_<run>) = {True,i0}
- Post(1, T, SensorMonitor_<run>) = {True,i1}
- ['thisObj(r(i1,T))=object'(r(i0,T))]
- Post(1, T, SensorDriver_get) = (TRUE,i1)
- Post(1, T, DataBanker_write) = (TRUE,i4)
- ['sensorDataIn(r(i4,T))=sensorData'(r(i3,T))]

**Output Behavior Definition**

- NONE(T) = NONE
- object(T) = new SensorMonitor
- Undefined

**Trace PostCondition**

- T.(PGM:SensorMonitor_run,'thisObj<SensorMonitor> ОО) — T.
- (Invoke PGM:SensorMonitor_run,'thisObj<SensorMonitor> ОО).
- (PGM:ThreadSleep,'sleepTime(int)=1000).
- (PGM:SensorDriver_get,'windSpeed:int=UNEVAL,'whalePassing:Boolean=UNEVAL,sensorData<SensorReading>:dd).
- (PGM:DataBanker_write,'sensorDataIn<SensorReading>:dd).
- (Return PGM:SensorMonitor_run)

**Monitored Variable Constraints**

- -
- -
- -

**Executed Count**

- 114
- 1
- 0

**Total Sample**

- 114
- 1
- 0

**Occurrence Probability**

- 100
- 100
- 0
# Averager Module Interface Specification

## Trace Event Syntax

<table>
<thead>
<tr>
<th>Program Name</th>
<th>Input Variable</th>
<th>Output Variable</th>
<th>Event Descriptor</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>getWindSpeed</code></td>
<td><code>averageData</code> int</td>
<td><code>averageData</code> int</td>
<td><code>(PGM:Averager_getWindSpeed,averageData&lt;int&gt;</code></td>
</tr>
<tr>
<td><code>getWhale</code></td>
<td><code>whalePassing</code> bool</td>
<td><code>whalePassing</code> bool</td>
<td><code>(PGM:Averager_getWhale,whalePassing&lt;bool&gt;</code></td>
</tr>
</tbody>
</table>

## Trace Semantics

### Trace Predicates

<table>
<thead>
<tr>
<th>Predicate</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>Pre(i,T,Averager_getWindSpeed)</code> = <code>TRUE,i</code></td>
<td>Precondition for <code>getWindSpeed</code></td>
</tr>
<tr>
<td><code>Pre(i,T,Averager_getWhale)</code> = <code>TRUE,i</code></td>
<td>Precondition for <code>getWhale</code></td>
</tr>
<tr>
<td><code>Post(i0,T,DataBanker_read)</code> = <code>TRUE,i</code></td>
<td>Postcondition for <code>DataBanker_read</code></td>
</tr>
</tbody>
</table>

### Trace Postcondition

- `averageData[T]=$(readData[(int)listElement[]].value / readData[(int)listElement[]].length)`
- `whalePassing[T]=True`
- `whalePassing[T]=False`

### Monitored Variable Constraints

- `[(listItemAt[0]).whalePassing = True]` v `[(listItemAt[1]).whalePassing = True]` v `[(listItemAt[2]).whalePassing = True]` v `[(listItemAt[3]).whalePassing = True]` v `[(listItemAt[4]).whalePassing = True]`
- `[(listItemAt[0]).whalePassing = False]` v `[(listItemAt[1]).whalePassing = False]` v `[(listItemAt[2]).whalePassing = False]` v `[(listItemAt[3]).whalePassing = False]` v `[(listItemAt[4]).whalePassing = False]`

### Executed count

<table>
<thead>
<tr>
<th>Count</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Sample</td>
<td>24</td>
</tr>
<tr>
<td>Occurrence Probability</td>
<td>100</td>
</tr>
</tbody>
</table>
**DataBanker Module Interface Specification**

**Trace Event Syntax**

<table>
<thead>
<tr>
<th>Program Name</th>
<th>Input Variable</th>
<th>Output Variable</th>
<th>Event Descriptor</th>
</tr>
</thead>
<tbody>
<tr>
<td>init</td>
<td>NONE</td>
<td>NONE</td>
<td>(PGM:DataBanker_init;staticList&lt;list&lt;SensorReading&gt;&gt;+)</td>
</tr>
<tr>
<td>write</td>
<td>sensorDataIn:SensorReading</td>
<td>NONE</td>
<td>(PGM:DataBanker_write;staticList&lt;list&lt;SensorReading&gt;&gt;+, 'sensorDataIn:SensorReading')</td>
</tr>
<tr>
<td>read</td>
<td>NONE</td>
<td>readData:list&lt;SensorReading&gt;</td>
<td>(PGM:DataBanker_read;staticList&lt;list&lt;SensorReading&gt;&gt;+)</td>
</tr>
</tbody>
</table>

**Trace Semantics**

<table>
<thead>
<tr>
<th>Trace Predicates</th>
<th>Pre(L.T.DataBanker_init)(TRUE,i)</th>
<th>Pre(L.T.DataBanker_write)(TRUE,i)</th>
<th>Pre(L.T.DataBanker_read)(TRUE,i)</th>
<th>( \lor_j { \neg \lor_i { \text{predicate}(ij) } } ) where ( i ) is a number of row in this table, and ( j ) is a number of column in this table, and ( i ) and ( j ) don't include this cell's number.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Output Behavior Definition</td>
<td>NONE(T) ( \neg ) NONE</td>
<td>NONE(T) ( \neg ) NONE</td>
<td>readData(T) = new List('sensorDataIn(r(i1,T)), 'sensorDataIn(r(i2,T)), 'sensorDataIn(r(i3,T)), 'sensorDataIn(r(i4,T)),'sensorDataIn(r(i5,T)))</td>
<td>Undefined</td>
</tr>
<tr>
<td>Trace Postcondition</td>
<td>T.(PGM:DataBanker_init) \rightarrow T.(PGM:DataBanker_write; 'sensorDataIn &lt;SensorReading&gt; s0) \rightarrow T.(PGM:DataBanker_write; 'sensorDataIn &lt;SensorReading&gt; s0) \rightarrow T.(PGM:DataBanker_read; readData' &lt;SensorReading&gt; unforeval) \rightarrow T.(PGM:DataBanker_read; readData' &lt;SensorReading&gt; unforeval) \rightarrow T.(PGM:DataBanker_read; readData' &lt;SensorReading&gt; unforeval) \rightarrow T.(PGM:DataBanker_read; readData' &lt;SensorReading&gt; unforeval) \rightarrow T.(PGM:DataBanker_read; readData' &lt;SensorReading&gt; unforeval)</td>
<td>T.(PGM:DataBanker_read; readData' &lt;SensorReading&gt; unforeval)</td>
<td>Undefinend</td>
<td></td>
</tr>
<tr>
<td>Monitored Variable Constraints</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Executed Count</td>
<td>1</td>
<td>1</td>
<td>228</td>
<td>48</td>
</tr>
<tr>
<td>Total Sample</td>
<td>1</td>
<td>228</td>
<td>48</td>
<td>0</td>
</tr>
<tr>
<td>Occurrence Probability</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>0</td>
</tr>
</tbody>
</table>
**SensorDriver Module Interface Specification**

### Trace Event Syntax

<table>
<thead>
<tr>
<th>Function Call Event Descriptor</th>
<th>Input Variable</th>
<th>Output Variable</th>
<th>Event Descriptor</th>
</tr>
</thead>
<tbody>
<tr>
<td>SensorDriver_get</td>
<td>windSpeed:int, whalePassing:Boolean</td>
<td>sensorData:SensorReading</td>
<td>(PGM:SensorDriver_get,'windSpeed&lt;int&gt;:<em>', 'whalePassing&lt;Bool&gt;:</em>', sensorData'&lt;SensorReading&gt;:'*)</td>
</tr>
</tbody>
</table>

### Trace Semantics

<table>
<thead>
<tr>
<th>Trace Predicates</th>
<th>Output Behavior Definition</th>
<th>Trace Postcondition</th>
</tr>
</thead>
<tbody>
<tr>
<td>V[i ¬\land {Predicate (i,j)}]</td>
<td>Undefined</td>
<td>Undefined</td>
</tr>
</tbody>
</table>

### Monitored Variable Constraints

- INTMIN ≤ aa ≤ INTMAX,
- bb = TRUE v FALSE

### Executed Count

- Total Sample: 114
- Occurrence Probability: 100
### TransmitDriver Module Interface Specification

#### Trace Event Syntax

<table>
<thead>
<tr>
<th>Program Name</th>
<th>Input Variable</th>
<th>Output Variable</th>
<th>Event Descriptor</th>
</tr>
</thead>
<tbody>
<tr>
<td>sendWindSpeed</td>
<td><code>msg:MessageFormatWind</code></td>
<td><code>msg:MessageFormatWind</code></td>
<td><code>(PGM:TransmitDriver_sendWindSpeed,'msg:&lt;MessageFormatWind&gt;:*','msg:&lt;MessageFormatWind&gt;:*)</code></td>
</tr>
<tr>
<td>sendToWhaleSurveyCenter</td>
<td><code>msg:MessageFormatWhale</code></td>
<td><code>msg:MessageFormatWhale</code></td>
<td><code>(PGM:TransmitDriver_sendToWhaleSurveyCenter,'msg:&lt;MessageFormatWhale&gt;:*','msg:&lt;MessageFormatWhale&gt;:*)</code></td>
</tr>
</tbody>
</table>

#### Trace Semantics

<table>
<thead>
<tr>
<th>Trace Predicates</th>
<th>Output Behavior Definition</th>
<th>Trace Postcondition</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>Pre(l,T,TransmitDriver_sendWindSpeed)=\{True,i\}</code></td>
<td><code>msg(T)</code>='msg(r(l,T))`</td>
<td><code>T.(PGM:TransmitDriver_sendWindSpeed,'msg:&lt;MessageFormatWind&gt;:mm','msg:&lt;MessageFormatWind&gt;:UNEVAL) → T.(PGM:TransmitDriver_sendWindSpeed,'msg:&lt;MessageFormatWind&gt;:mm','msg:&lt;MessageFormatWind&gt;:mm)</code></td>
</tr>
<tr>
<td><code>Pre(l,T,TransmitDriver_sendToWhaleSurveyCenter)=\{True,i\}</code></td>
<td><code>msg(T)</code>='msg(r(l,T))`</td>
<td><code>T.(PGM:TransmitDriver_sendToWhaleSurveyCenter,'msg:&lt;MessageFormatWhale&gt;:mm','msg:&lt;MessageFormatWhale&gt;:UNEVAL) → T.(PGM:TransmitDriver_sendToWhaleSurveyCenter,'msg:&lt;MessageFormatWhale&gt;:mm','msg:&lt;MessageFormatWhale&gt;:mm)</code></td>
</tr>
<tr>
<td><code>\forall \{\neg\land (Predicate (i,j))\} \text{ where } i \text{ is a number of row in this table, and } j \text{ is a number of column in this table, and } i \text{ and } j \text{ don't include this cell's number.}</code></td>
<td></td>
<td><code>Undefined</code></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Monitored Variable Constraints</th>
<th>Executed Count</th>
<th>Total Sample</th>
<th>Occurrence Probability</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-</code></td>
<td>114</td>
<td>114</td>
<td>100</td>
</tr>
<tr>
<td><code>-</code></td>
<td>3</td>
<td>3</td>
<td>100</td>
</tr>
</tbody>
</table>


APPENDIX D. TESTING TRACE GENERATION ALGORITHM

INTERMEDIATE STATES

The intermediate states of the testing trace in the test case generation algorithm are described for particular stages.
Events beyond the upper-bound length of testing trace are truncated. This example has the upper-bound 37.

Meta-Variable Map=

<table>
<thead>
<tr>
<th>Key</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>qq</td>
<td>Monitored Variable</td>
</tr>
<tr>
<td>ob1</td>
<td>new MessageGenerator Instance</td>
</tr>
<tr>
<td>ob2</td>
<td>new SensorMonitor Instance</td>
</tr>
</tbody>
</table>

CON=

qq=FALSE
**Stage 1**

![Image of the text content](image-url)

**Stage 2**

![Image of the text content](image-url)

**Stage 3**

![Image of the text content](image-url)

Step 3. Query and get the possibly-satisfiable equivalence class.

The possibly-satisfiable equivalence classes are:
1. The one with "whalePassing(T) = TRUE;"
2. The one with "whalePassing(T) = FALSE;"

Step 4.

An equivalence class of traces is chosen. In this case, the one with "whalePassing = FALSE" is chosen with the probability 87.5/100.
Step 3.

A consequent of the trace postcondition of "Averager_getWhale" is inserted.

Step 3. Query again and get the possibly-satisfiable equivalence class.

The possibly-satisfiable equivalence classes are

1) the one with "whalePassing(T) = TRUE;"
2) the one with "whalePassing(T) = FALSE;"

Step 4. This case "whalePassing=FALSE" is chosen with the probability $87.5/100$.

*Note: Although the random choice is done twice, the probability of getting "whalePassing=FALSE" at this step remains $87.5/100$, since the probability of getting "whalePassing=FALSE" is $87.5/100$ no matter what value "whalePassing" has before, which leads to

\[
P'_{\text{whalePassing}=\text{FALSE}} = \sum_{v} P_{\text{whalePassing}=v} = \frac{87.5}{100} = \frac{87.5}{100}
\]

where $p'_{\text{whalePassing}=v}$ is the probability of eventually getting "whalePassing = v" at this step, and $p_{\text{whalePassing}=v}$ is the probability of getting "whalePassing = v" one step before this step.

```
(PGM: FWSS_init; quit<Boolean=true>);
(PGM: DataBanker_init);
(PGM: MessageGenerator_init; object<MessageGenerator>; obj1=new MessageGenerator);
(PGM: SensorMonitor_init; object<SensorMonitor>; obj2=new SensorMonitor);
(PGMD: SensorMonitor_run, thisObj<SensorMonitor>; obj2);
(PGM: DataBanker_init);
(PGM: TransmitDriver_sendWindSpeed. 'msg<MessageFormatWind>; mm1=new MessageFormat(cc1); msg='MessageFormatWind=mm1');
```

```
(PGM: FWSS_init; quit<Boolean=true>);
(PGM: DataBanker_init);
(PGM: MessageGenerator_init; object<MessageGenerator>; obj1=new MessageGenerator);
(PGM: SensorMonitor_init; object<SensorMonitor>; obj2=new SensorMonitor);
(PGMD: SensorMonitor_run, thisObj<SensorMonitor>; obj2);
(PGM: DataBanker_init);
(PGM: TransmitDriver_sendWindSpeed. 'msg<MessageFormatWind>; mm1=new MessageFormat(cc1); msg='MessageFormatWind=mm1');
(PGM: Averager_getAverage); (PGMD: DataBanker_readData 'in<DataReading>; new List(dd1, dd2, dd3, dd4, dd5)); (PGM: Averager_getWhale, whalePassing<Boolean>; true);
```

### Table 1: MetaVariableMap

<table>
<thead>
<tr>
<th>Key</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>cc</td>
<td>INTMIN ≤ cc ≤ INTMAX</td>
</tr>
<tr>
<td>bb1</td>
<td>INTMIN ≤ bb1 ≤ INTMAX</td>
</tr>
<tr>
<td>bb2</td>
<td>INTMIN ≤ bb2 ≤ INTMAX</td>
</tr>
<tr>
<td>aa1</td>
<td>INTMIN ≤ aa1 ≤ INTMAX</td>
</tr>
<tr>
<td>dd1</td>
<td>(windSpeed=aa1, whalePassing=bb1)</td>
</tr>
<tr>
<td>bb2</td>
<td>INTMIN ≤ bb2 ≤ INTMAX</td>
</tr>
<tr>
<td>aa2</td>
<td>INTMIN ≤ aa2 ≤ INTMAX</td>
</tr>
<tr>
<td>bb3</td>
<td>INTMIN ≤ bb3 ≤ INTMAX</td>
</tr>
<tr>
<td>dd2</td>
<td>(windSpeed=aa2, whalePassing=bb2)</td>
</tr>
<tr>
<td>aa3</td>
<td>INTMIN ≤ aa3 ≤ INTMAX</td>
</tr>
<tr>
<td>bb4</td>
<td>INTMIN ≤ bb4 ≤ INTMAX</td>
</tr>
<tr>
<td>dd3</td>
<td>(windSpeed=aa3, whalePassing=bb3)</td>
</tr>
<tr>
<td>aa4</td>
<td>INTMIN ≤ aa4 ≤ INTMAX</td>
</tr>
<tr>
<td>bb5</td>
<td>INTMIN ≤ bb5 ≤ INTMAX</td>
</tr>
<tr>
<td>dd4</td>
<td>(windSpeed=aa4, whalePassing=bb4)</td>
</tr>
<tr>
<td>aa5</td>
<td>INTMIN ≤ aa5 ≤ INTMAX</td>
</tr>
<tr>
<td>bb6</td>
<td>INTMIN ≤ bb6 ≤ INTMAX</td>
</tr>
<tr>
<td>dd5</td>
<td>(windSpeed=aa5, whalePassing=bb5)</td>
</tr>
</tbody>
</table>
Stage 3 (Last Stage)

```plaintext
InvokePGM:FWS_(init:'quit'='false')
(PGM:DataBanker_init).
(PGM:MessageGenerator_<init>:object='MessageGenerator':obj1)
(PGM:SensorMonitor_<init>:object='SensorMonitor':obj2)
(InvokePGM:SensorMonitor_run,'thisObj'SensorMonitor:obj2).
(PGM:ThreadSleep,'sleepTime'='1000').
(PGM:SensorDriver_get,'windSpeed'='55','whalePassing'='false','sensorData'SensorReading:dd5).
(PGM:DataBanker_write,'sensorDataIn'SensorReading:dd5).
(ReturnPGM:SensorMonitor_run)
(InvokePGM:SensorMonitor_run,'thisObj'SensorMonitor:obj2).
(PGM:ThreadSleep,'sleepTime'='1000').
(PGM:SensorDriver_get,'windSpeed'='55','whalePassing'='false','sensorData'SensorReading:dd5).
(PGM:DataBanker_write,'sensorDataIn'SensorReading:dd5).
(ReturnPGM:SensorMonitor_run)
```

**Step 6:**
Generate monitored variable values and populate all values in this testing trace.

<table>
<thead>
<tr>
<th>Key</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>qq</td>
<td>FALSE</td>
</tr>
<tr>
<td>ob1</td>
<td>new MessageGenerator Instance</td>
</tr>
<tr>
<td>ob2</td>
<td>new SensorMonitor Instance</td>
</tr>
<tr>
<td>aa1</td>
<td>45</td>
</tr>
<tr>
<td>bb1</td>
<td>FALSE</td>
</tr>
<tr>
<td>dd1</td>
<td>{windSpeed='aa1', whalePassing='bb1'}</td>
</tr>
<tr>
<td>aa2</td>
<td>51</td>
</tr>
<tr>
<td>bb2</td>
<td>FALSE</td>
</tr>
<tr>
<td>dd2</td>
<td>{windSpeed='aa2', whalePassing='bb2'}</td>
</tr>
<tr>
<td>aa3</td>
<td>50</td>
</tr>
<tr>
<td>bb3</td>
<td>FALSE</td>
</tr>
<tr>
<td>dd3</td>
<td>{windSpeed='aa3', whalePassing='bb3'}</td>
</tr>
<tr>
<td>aa4</td>
<td>52</td>
</tr>
<tr>
<td>bb4</td>
<td>FALSE</td>
</tr>
<tr>
<td>dd4</td>
<td>{windSpeed='aa4', whalePassing='bb4'}</td>
</tr>
<tr>
<td>aa5</td>
<td>55</td>
</tr>
<tr>
<td>bb5</td>
<td>FALSE</td>
</tr>
<tr>
<td>dd5</td>
<td>{windSpeed='aa5', whalePassing='bb5'}</td>
</tr>
<tr>
<td>rd1</td>
<td>List&lt;SensorReading&gt; List&lt;dd1,dd2,dd3,dd4,dd5&gt;</td>
</tr>
<tr>
<td>cc1</td>
<td>51</td>
</tr>
</tbody>
</table>
BIBLIOGRAPHY


