Text

Description automatically generated

Formatting and Checking Weakest Precondition Proofs in Dafny

Project Proposal

by

**Jacob Freeman**

School of Information Technology and Electrical Engineering

University of Queensland

Submitted for the degree of Bachelor of Software Engineering (Hons)

Under the supervision of Professor Graeme Smith

Submitted: 31/3/2022

Table of Contents

[1 Introduction 1](#_Toc98949456)

[1.1 Topic 1](#_Toc98949457)

[1.2 Purpose 2](#_Toc98949458)

[1.3 Goals 2](#_Toc98949459)

[1.4 Scope 2](#_Toc98949460)

[2 Background 3](#_Toc98949461)

[2.1 Formal Methods 3](#_Toc98949462)

[2.2 Weakest Precondition Proofs and Hoare Logic 4](#_Toc98949463)

[2.2.1 Hoare Triples 5](#_Toc98949464)

[2.2.2 Assignment Axiom 5](#_Toc98949465)

[2.2.3 Precondition Strengthening 5](#_Toc98949466)

[2.2.4 Sequencing Rule 6](#_Toc98949467)

[2.2.5 Conditional Rule 6](#_Toc98949468)

[2.2.6 While Rule 6](#_Toc98949469)

[2.2.7 While Rule for Total Correctness and Termination 7](#_Toc98949470)

[2.2.8 Additional Equivalence Rules 7](#_Toc98949471)

[2.3 Teaching of Formal Methods 8](#_Toc98949472)

[2.3.1 Advantages of Tool Support 8](#_Toc98949473)

[2.3.2 Disadvantages of Tool Support 9](#_Toc98949474)

[2.3.3 Justification 10](#_Toc98949475)

[2.4 VSCode IDE 10](#_Toc98949476)

[2.5 Dafny Functionality 11](#_Toc98949477)

[2.5.1 Calc Function 11](#_Toc98949478)

[2.6 Preliminary Software Architecture Diagrams 12](#_Toc98949479)

[2.6.1 Student Extension 12](#_Toc98949480)

[2.6.2 Educator Extension 13](#_Toc98949481)

[2.7 Prototype User Interface – Student Extension 14](#_Toc98949482)

[2.7.1 Weakest Precondition Input 14](#_Toc98949483)

[2.7.2 Logic or Rule Input 14](#_Toc98949484)

[2.7.3 Syntax Error Indicator 14](#_Toc98949485)

[2.7.4 Syntax Error Hover 14](#_Toc98949486)

[2.8 Prototype User Interface – Educator Extension 15](#_Toc98949487)

[2.8.1 Verification Function Call 15](#_Toc98949488)

[2.8.2 Verification Display 15](#_Toc98949489)

[2.8.3 Verification Method Button 15](#_Toc98949490)

[2.8.4 Verification Method Display 15](#_Toc98949491)

[3 Project Tasks 16](#_Toc98949492)

[3.1 Project Deliverables 16](#_Toc98949493)

[3.2 Student Tool Development 16](#_Toc98949494)

[3.3 Educator Tool Development 16](#_Toc98949495)

[3.4 Extension Educator Tool Development 16](#_Toc98949496)

[4 Project Plan 17](#_Toc98949497)

[5 Risks 17](#_Toc98949498)

[5.1 Time Management 17](#_Toc98949499)

[5.2 Lack of Expertise 18](#_Toc98949500)

[5.3 Worldly Inhibitors 18](#_Toc98949501)

[6 Appendix 19](#_Toc98949502)

[7 Bibliography 22](#_Toc98949503)

List of Figures

[Figure 1: Hoare Logic Notation [4] 4](#_Toc98949504)

[Figure 2: Hoare Triple Notation [4] 5](#_Toc98949505)

[Figure 3: Hoare Assignment Axiom Notation [4] 5](#_Toc98949506)

[Figure 4: Precondition Strengthening Notation [4] 5](#_Toc98949507)

[Figure 5: Sequencing Rule Notation [4] 6](#_Toc98949508)

[Figure 6: Conditional Rule Notation [4] 6](#_Toc98949509)

[Figure 7: While Rule Notation [4] 7](#_Toc98949510)

[Figure 8: While Loop for Total Correctness 7](#_Toc98949511)

[Figure 9: Variable Declaration Syntax 8](#_Toc98949512)

[Figure 10: Method Assignment Syntax 8](#_Toc98949513)

[*Figure 11: Dafny IDE colouring Style* 11](#_Toc98949514)

[Figure 12: Calc Example [9] 11](#_Toc98949515)

[Figure 13 - Student Extension Diagram 12](#_Toc98949516)

[Figure 14 - Educator Extension Diagram 13](#_Toc98949517)

[Figure 15 - Student Extension Prototype Interface 14](#_Toc98949518)

[Figure 16 - Protype Syntax Error Hover 15](#_Toc98949519)

[Figure 17 - Educator Extension Prototype Interface 15](#_Toc98949520)

[Figure 19: Example of Precondition Strengthening 19](#_Toc98949521)

[Figure 20: Example of Postcondition Weakening 19](#_Toc98949522)

[Figure 21: Example of the Sequencing Rule 19](#_Toc98949523)

[Figure 22: Backwards Reasoning 20](#_Toc98949524)

[Figure 23: If/Else Weakest Precondition Proof 20](#_Toc98949525)

[Figure 24: Loop weakest precondition proof 20](#_Toc98949526)

[Figure 25: Example of Total Correctness 21](#_Toc98949527)

[Figure 26: Example of Method Assignment [10] 21](#_Toc98949528)

# Introduction

## Topic

Formal verification is slowly growing in industry adoption. Since 2011, engineers at Amazon Web Services (AWS) have been using formal methods technology known as TLA+ [1] and now Dafny[[1]](#footnote-1) across their business. Facebook have also been integrating their formal methods technology called INFER into their products since 2013 [2]. As education institutions continue to offer courses related to formal methods and students are continually educated on the importance of formal methods, its popularity will increase further. However formal methods are not the simplest topic to teach and requires intricate theorems to be taught to students in a short amount of time. “In industry, formal methods have a reputation of requiring a huge amount of training and effort to verify a tiny piece of relatively straightforward code, so the return on investment is only justified in safety critical domains such as medical systems and avionics.” [1]. This is made even more difficult by learning the verification techniques by hand. These handwritten proofs can be difficult to format and analyze, not only for students but for educators to verify and mark in an assessment context.

This thesis project delves into the topic of formal methods. More precisely, how can a tool be developed to support students format their proofs and how can educators verify these proofs in the Dafny programming language. The proofs investigated are weakest precondition proofs and forms the backbone of many formal verifiers. This proposal introduces formal methods and examines Hoare logic as this is what weakest precondition proofs are reasoned with. The tool will need to analyze and verify this rigorous mathematical logic. The Dafny programming language is explored and its accompanying constructs and architecture. Overall, this project makes the connection between formal methods and tool supports in teaching.

Ultimately, students and educators will use the tool under different circumstances. Students will need to use the tool when completing tutorial exercises and assignments, the tool will provide them with assistance for formatting their proofs checking that their proofs are syntactically and semantically correct, strategically neglecting to verify the correctness of these proofs. Furthermore, educators will need to verify the student’s proofs for correctness to save time when marking assessments. This tool may also be utilized in the teaching environment e.g. when an example of a proof is shown in class. These different use cases will need to be separated from one another so that students cannot access the tools capabilities available only to educators.

## Purpose

The purpose of this project is to develop a tool or multiple tools to support in the teaching of formal methods using the Dafny programming language, meeting both students and educators needs and requirements.

## Goals

The goal is to develop tools that provide the following functionality:

* Implement a user-friendly format for students to enter their weakest precondition logic into VSCode
* The syntax and semantics of the weakest precondition logic will be checked for errors and provide suggestions to the user in VSCode
* Verify the correctness of the weakest precondition proof entered
* Provide output as to what weakest precondition logic is correct and why it may not be correct in VSCode
* In case of verification errors, allow educators to see how the weakest precondition proofs were verified so that manual marking is still possible.

Extension:

* Implement a way to mark weakest precondition proofs entered in an online format such as an online quiz

## Scope

The scope of this project is to provide a tool support for writing and verifying weakest precondition proofs to students and educators. These proofs are written in Dafny and no other programming language. Dafny is taught using the development environment bundled in VSCode Studio, the tool must be an extension of this environment, so that students and educators can easily integrate the new tool into the existing environment. The weakest precondition proof entails the following formal method topics:

* Assignment Axiom
* Precondition Strengthening
* Sequencing Rule
* Conditional Rule
* While Rule
* Termination

Students should not be able to access the educators tool abilities, so distribution and access needs to be limited and authenticated. The scope, of this project is anything that can be included in a VSCode extension to assist in the tool’s creation. An extension task is to provide marking to students answers on online quiz’s which have the same formal method topics but different software pathways into Dafny for verification will be required, which is yet to be determined.

# Background

## Formal Methods

Since the birth of computer programs, and all the development that has gone into these increasingly complex programs, why aren’t these programs error free? Most programs are affected by parameters that are hard to define and control. In an IT sense, the software development process brings faults and bugs into the program. Formal methods allow programmers to reduce the amount of these faults, by applying formal methods during development. Formal methods are “mathematically rigorous techniques and tools for the specification, design and verification of software and hardware systems” [3], simply formal methods are used to verifying that programs do what they are supposed to do. This means that program specifications of statements use mathematical logic and formal verification consists of arduous deductions in this logic. The power of formal methods is that it can deduce verification over the entire state of the program and that these deductions hold for all possible inputs. However formal methods cannot be used throughout the entirety of the development process due to the complexity of the code or lack of tool support. Formal methods are typically reserved for high-level design on safety and security critical mechanisms.

When a program is developed, the first step is to generate a specification that describes the programs desired behavior and should be correct and unambiguous. This specification is then translated into code by the programmer. This is when human error gets introduced into the program as misinterpretation of the specification can occur. Then there is also the large size of some programs, which are difficult to specify. Typically, the program is tested during and after its implementation so that no errors or faults are present. Testing large programs can be very time-consuming resulting in it being unfeasible. In terms of critical systems, the correct functionality needs to be guaranteed, which needs extensive testing or a way to prove the program matches the specification. Formal specifications leave no room for misinterpretation. This is where formal methods are introduced to guarantee the correctness of a program, given the formal method used doesn’t contain faults of its own or that the specification is incorrect. In summary, formal method tools are used to detect errors more frequently and earlier as it is done at computer processing speeds compared to the manual speed of a human.

## Weakest Precondition Proofs and Hoare Logic

A formal proof of a program is a combination of hypotheses statements culminating with the conclusion statement, such that each statement is an example of an axiom or continues from a previous statement by a rule of logical inference. If denotes the entire program of statements, then denotes that S can be proven, also known as a theorem. To prove such assertions certain methods of how to do so must be known. The axioms of Hoare logic are specified by schemas detailed below and logical inference rules can be specified with the notation in Figure 1.

Figure 1: Hoare Logic Notation [4]

This demonstrates that the conclusion can be proved from which are hypotheses. [4]

Simply weakest preconditions are logically obtained, to prove that the precondition given for the program is a subset of the weakest precondition, hence verifying the program for correctness.

Examples of Hoare logic implemented with Dafny can be found in the [Appendix](#_Appendix).

### Hoare Triples

Weakest precondition proofs are assembled on top of Hoare triple logic. Simply, a Hoare triple is written as:

Figure 2: Hoare Triple Notation [4]

Where is a precondition, is a statement and is a postcondition. A Hoare triple is valid when S is executable when is true and can also be proven as true afterwards. Formally, Hoare triples follow the syntax convention of using curly brackets around assertions. As a whole, weakest precondition proofs chain together multiple, more complex Hoare triples or assertions to ascertain the weakest precondition in larger bodies of code. [5]

### Assignment Axiom

The assignment axiom shows that the variable after executing the assignment , equals the expression . Witness that if statement is true after the assignment, then the statement generated by replacing for in must be true before execution of the statement. Hence, is defined as substituting all occurrences of with in . This logical axiom is the building block for backwards reasoning and is denoted as:

Figure 3: Hoare Assignment Axiom Notation [4]

### Precondition Strengthening

Hoare logic allows preconditions to be strengthened following backward reasoning. This is denoted as:

Figure 4: Precondition Strengthening Notation [4]

As backwards reasoning the typically used to verify programs, precondition strengthening is commonly used.

### Sequencing Rule

The assignment axiom is the foundation for weakest precondition proofs but can only be used to evaluate individual statements. As shown in the example below, statements and can be sequenced together because has postcondition , and has precondition , resulting in a formal sequence. Intuitively, larger programs can be analyzed using the assignment axiom by sequencing together multiple statements and the pre and postconditions accompanying these statements, making them Hoare triples.

Figure 5: Sequencing Rule Notation [4]

### Conditional Rule

The examples shown until now have only involved linearly sequenced statements. Although, conditional statements such as if/else have multiple possible branches adding complexity to the Hoare triple. The conditional rule follows the following notation:

Figure 6: Conditional Rule Notation [4]

### While Rule

When analyzing loops in weakest precondition logic, while loops are used instead of the more widely used for loop, due to their simplicity in verification. While loops separate the initial statements, loop guard and step statement, used in for loops. Loops are more complex to prove as it is unknown how many times the loop will be executed or when the loop terminates. Therefore, the postcondition can be satisfied with the use of a loop invariant, denoted . A loop invariant can be considered as a precondition and a postcondition for the loop as it needs to hold immediately before and after the loop, as well as in every point during the loop’s execution. Ultimately when the while loop is exited the loop guard, denoted won’t hold. When writing a loop invariant, the programmer typically gets inspired by either the postcondition or the loop guard. The while rule follows the following notation:

Figure 7: While Rule Notation [4]

### While Rule for Total Correctness and Termination

The correctness of a program is defined by whether it terminates. If a program does not terminate than unexpected results can happen, and errors can be thrown. Using the Hoare triple notation of , if program is started in any state, then is satisfied and will terminate to a state satisfying . This is known as total correctness when the program always terminates to the correct results. Partial correctness of a program occurs when the program terminates with the right result, but termination isn’t precisely known. Hence a termination proof is need for total correctness.

Most loops typically terminate. So, when proving a loops correctness, a proof involving the termination metric needs to be computed. In this notation, is known as the loop variant and changes as the loop iterates. strictly decreases as after on a domain set , typically dependent on the loop guard . As is finite and is strictly decreasing, t cannot decrease forever as it is restricted by . In Hoare logic the specifications only hold if a loop terminates. Termination metrics can be proven using the following notation:

Figure 8: While Loop for Total Correctness

Termination proofs are typically grouped in with the weakest precondition proof using ghost variables. Ghost variables can be assigned with the body of the program without being included in the code’s compilation.

### Additional Equivalence Rules

There are a wide range of equivalence rules that can be used in the formal verification. However, the rules highlighted here add extra syntax and semantics to the proof.

#### Variable Declarations

When a variable is declared in the program, all instances of that variable are assigned in the precondition. This is denoted by the syntax:

Figure 9: Variable Declaration Syntax

#### Method Assignments in Recursion

If a method is assigned to a variable, then both the pre- and postconditions of the method are used in the adjoining precondition in the program. This assignment follows the following notation, where denotes the methods precondition, R denotes the methods postcondition, is the return value of the method and denotes postcondition of the program:

Figure 10: Method Assignment Syntax

## Teaching of Formal Methods

### Advantages of Tool Support

In the context of using formal methods in software engineering, tool support is critical for increasing productivity and reducing mistakes in development. Often students are afforded the chance to use tool support when completing small projects. However, this is usually allowed after students have had to learn formal methods by hand, which is typically difficult at first. This leads to students enjoying the high automation that the formal method tool support provides.

As formal methods consist of complex mathematical concepts, students tend to take extra time to solidify their knowledge, slowing down the teaching process. However, many formal method courses offered at tertiary educational institutions are like a software project in the context that there are time constraints. This limits the extensiveness of the teaching content, restricting the course of more complex formal method topics. Hence courses use tool support to decrease the steep learning curve many students have when learning formal methods, but only after they have learnt formal methods from hand. By exposing students to tool supports for formal methods, helping facilitate the tools development will lead to a higher adaption of formal methods in industry.[6] This can be achieved because five years ago, there were about 40 universities who had been or were using Dafny in teaching. [[2]](#footnote-2)

Formalization and its accompanying tool supports are essential for software analysis. It is very popular to analyze software in more informal ways by using diagrams. As this is generally accepted in the programming community, providing rigid formal specifications of the programs intended functionality leads to more accurate programs. Formal specifications of even the smallest programs may be wrong, without tool supports as hand-written verification attempts are prone to human errors. Therefore, verification proofs regarding the correctness of programs must be automated. Even a lightweight formalization tool can save time, for example decreasing the amount of test cases. [7]

### Disadvantages of Tool Support

Many students have experience with tool supports when learning programming languages such as C and Java. These tool supports effectually assist students write, execute, and test their programs. Formal methods teachers tend to believe that tool support will also assist students learn formal methods. However, the use of tool supports may not be as effective as first thought, as specified by some educators of VDM and SOFL courses, that delve into formal specification techniques. [6]

Learning formal methods, and the specification language used, involves students to learn the syntax and semantics of this language. It has been obtained that the best way to learn the dynamics of a specification language is to write out the formal specifications by hand, as one would learn English as a second language. This teaching strategy is typically effective as exercises and projects given to students are small and increases student’s memory and depth of knowledge. By not having tools support, removes the student’s ability to ‘copy and paste’ specifications, without thinking and analyzing the specifications for themselves. The purpose of a formal method specification is not for a computer to directly do this analysis, but for the reader to understand the specification written. Therefore, writing by hand forces students to do this analysis in their head without the use of a tool support to help format their specifications. As specification languages don’t need to be compiled and run, not having a tool support won’t cause any major inconvenience. [6]

### Justification

Given that tool support has valid advantages and disadvantages, it can be seen that the benefits of the tool outweigh its limitations in regards to educational support when applied correctly. This depends on the educators to teach formal methods in a format where students don’t just use the tool because they are lazy, but because they are mentally stimulated by the topic and want validation in their work. Therefore, the tool proposed in this project will significantly benefit the student’s education.

## VSCode IDE

Program verifiers utilize three major integrated subsystems. Firstly, is the logic it uses, such as Hoare-style program logic or type theory, secondly is the automation mechanism such as decision procedures or proof search strategies. These 2 subsystems make up the proof system and affects how the programmer interacts with verification system through the manipulation of the input language. Thirdly, is the languages integrated development environment (IDE), which attempts to reduce the understandability of the proof system, making modifications simpler for the programmer. Dafny’s most developed IDE is an extension in Microsoft Visual Studio / Visual Studio Code (VS/VSCode) [8].

Users typically wonder if the verification has been completed. The user is made aware of the verification completion by a panel on the side bar in the bottom left of the screen that indications when the verification is occurring and when it is complete. Additional colors are added into the margins and scroll panel to display modification to the snapshot: green indicates that the new modification is verified, red indicates that the new modification is not verified, red arrows indicate any lines that may have been removed, and blue indicates that any other changes that may have been made. An example of these colors is shown in Figure 2. [8]

A screenshot of a computer

Description automatically generated with medium confidence

*Figure 11: Dafny IDE colouring Style*

## Dafny Functionality

### Calc Function

The calc function built into the Dafny language can be used to perform calculation proofs using program-oriented calculations. These proofs are determined using stepwise formula manipulation which typically utilizes changing a left-hand side equality into the right-hand side equality [9]. This functionality is very similar to the assertion function that asserts the correctness of an individual statement, the calc function has the ability to prove an entire program proof. This can be used within the project to verify the correctness of the students’ proofs from what is already built into Dafny.

calc == {

(x + y) \* (x + y);

x \* (x + y) + y \* (x + y);

x \* x + x \* y + y \* x + y \* y;

x \* x + x \* y + x \* y + y \* y;

x \* x + 2 \* x \* y + y \* y;

}

Figure 12: Calc Example [9]

## Preliminary Software Architecture Diagrams

### Student Extension

The student extension will follow the following software architecture:

Diagram

Description automatically generated

Figure 13 - Student Extension Diagram

The text entered by the user for the weakest precondition proof will be sent in String format for syntax analysis, which will require a rigorous algorithm. The errors determined by this analysis will then be send to the user interface for visual display in the form of squiggly lines and pop-up boxes.

### Educator Extension

The educator extension will follow the following software architecture:

Diagram

Description automatically generated

Figure 14 - Educator Extension Diagram

When the user calls the verification function (shortcut F10), the text of all the weakest precondition proofs will be sent for syntax analysis, similar to the student extension. Depending on the outcome of this analysis, a negative verification status may be sent to the user interface. Otherwise, if syntax standards are met, the weakest precondition proofs are sent for verification condition analysis, which will be a complex algorithm explained in 2.4. This will return either a positive or negative verification status to be displayed on the user interface. The educator will then be presented with a button for verification method viewing, which will return the analysis done to determine that verification condition, so that the educator can manually resolve any misinterpretations of the analysis, if these were to occur.

## Prototype User Interface – Student Extension

The following prototype user interface provides an example for what the student extension can potentially do.

A screenshot of a computer

Description automatically generated with medium confidence

Figure 15 - Student Extension Prototype Interface

The important components of the extension are explained below:

### Weakest Precondition Input

The weakest precondition logic can be added into a new line anywhere within the Dafny program text without affecting the program. This is done by using comments to hide the added logic text from the Dafny text, in the format of ‘//{ logic }’. This format also maintains the syntax highlighting that Dafny has across the weakest precondition logic, such as highlighting functions yellow. From here, syntax errors can be sent to the weakest precondition logic separate from the Dafny program.

### Logic or Rule Input

Each weakest precondition logic input will be manipulated by some form of rule the simplify the logic. The names of these rules can be added in comment format after the weakest precondition proof for tutors to mark.

### Syntax Error Indicator

The syntax indicator seen in the interface above is a yellow squiggly line, the same as an error in the Dafny language. This indicator will highlight exactly the area of text that has the error. There is the potential for different types of errors to be displayed by different colors.

### Syntax Error Hover

VSCode enables the user to hover over the syntax error indicator to interpret exactly what the error is, this can be seen in the image above. These can be customized to whatever the specific error is enabling the student a precise debugging tool.

Graphical user interface

Description automatically generated with medium confidence

Figure 16 - Protype Syntax Error Hover

## Prototype User Interface – Educator Extension

The following prototype user interface provides an example for what the educator extension can potentially do.

Text

Description automatically generated

Figure 17 - Educator Extension Prototype Interface

The important components of the extension are explained below:

### Verification Function Call

Once the student’s logic is obtained, the educator can call the verification function by simply pressing F9 on the keyboard. This will trigger an event where all the weakest precondition logics will be analyzed, and a verification status will be determined.

### Verification Display

This will display the verification status of all the weakest precondition logic in a colored box after the weakest precondition input. It will either display verified or unverified, with the colors triggering an immediate indication of right and wrong to the educator.

### Verification Method Button

If the verification status is unusual or cannot be determined, then the educator has the ability to press a verification method button positioned after each verification condition displayed, this is not shown in the prototype image above.

### Verification Method Display

Once the verification method button is pressed an alternate button will appear to navigate the educator to an interactive screen for the educator to see how the program is being verified in Dafny, allowing the educator to oversee the verification process more precisely.

# Project Tasks

The project can be split into distinct parts, the deliverables the tool support available for the student and the tool support available for the educator. These distinct parts can be split up further into smaller tasks.

## Project Deliverables

The project has deliverables that are due by certain deadlines, these deadlines are provided below:

* Thesis Project Proposal (TBA)
* Thesis Seminar Presentation (TBA)
* Thesis Final Presentation + Poster (TBA)
* Thesis Document (TBA)

## Student Tool Development

The student tool support has the following tasks:

* Implement a user-friendly input for students to enter their weakest preconditions
* The syntax and semantics of the weakest precondition logic will be checked for errors
* Provide suggestions for fixing syntax and semantic errors to the user
* Provide suggestions for weakest precondition proof formatting to the user

## Educator Tool Development

The educator tool support has the following tasks:

* Verify the correctness of the weakest precondition proof entered in VSCode
* Provide output as to why the weakest precondition logic is correct and why it may not be correct

## Extension Educator Tool Development

* Verify the correctness of the weakest precondition proof entered in an online quiz format
* Provide output as to why the weakest precondition logic is correct and why it may not be correct

# Project Plan

* Thesis Project Proposal (S1W5)
* Thesis Seminar Presentation (S1W11)
* Student Tool (S1W13)
* Create method for students to enter weakest precondition proofs in Dafny
* Provide syntax highlighting to the weakest precondition proof
* Provide syntax errors to the weakest precondition proof
* Educator Tool (S2W6)
* Create function call for the verification to begin
* Verify the weakest precondition proof
* Print outcome of verification to screen
* Create method for educators to see the verification method
* Extended Educator Tool (S2W12)
* Thesis Final Presentation + Poster (S2W12)
* Thesis Document (S2W13)

# Risks

This project will be presented with several risks, however as this project has no practical/physical component the risks are minimal. The risks are outlined below:

## Time Management

Due to the unknown aspects of the project, even after extensive research is conducted the time need to complete the project to a sufficient standard is hard to predict. As this project has several deliverables with deadlines, these deadlines will need to be met with no barriers to their completion. This can be done by using extensive time management, a plan for time management is displayed in section 5. The deadlines set above are flexible and can be changed depending on what is appropriate, e.g. if more work needs to be done on the student extension, would mean pushing the deadline back. The extended educator tool is also optional depending on the development completion of the student and educator tools, potentially providing a buffer for those deadlines.

## Lack of Expertise

This project will be conducted under the supervision of Dr Graeme Smith with credentials: Bachelor of Engineering (Hons) and Doctor of Philosophy. His fellow contacts will also be utilized. As Dr Smith is an expert in the field of formal methods with industry and educational experience, the projects level of sophistication needed can be met. If the project becomes not feasible anymore and too difficult fallback options will need to be created in order to provide an adequate project deliverable.

## Worldly Inhibitors

The February 2022 flood in Brisbane where teaching at UQ was cancelled for a weak could have impacted the timeline of the project, however other formats for communicator were used for meetings with supervisor Graeme Smith. Another COVID-19 outbreak / variants could cause subsequent lockdowns and border closers, however as this has been ongoing for the past 2-3 years this should be nothing that can’t be handled.

# Appendix

Figure 19: Example of Precondition Strengthening

(assignment axiom)

(pure logic)

(precondition strengthening)

(laws of arithmetic)

(postcondition weakening)

Figure 20: Example of Postcondition Weakening

(i)

(ii)

(iii)

Therefore, (i) and (ii) can be sequenced.

(iv)

Furthermore, (iv) and (iii) can be sequenced.

(v)

Figure 21: Example of the Sequencing Rule

Figure 22: Backwards Reasoning

Figure 23: If/Else Weakest Precondition Proof

(Precondition Strengthening)

(Simplifying)

Figure 24: Loop weakest precondition proof

is

Figure 25: Example of Total Correctness

Figure 26: Example of Method Assignment [10]

# Bibliography

[1] T. R. Chris Newcombe, Fan Zhang, Bogdan Munteanu, Marc Brooker, Michael Deardeuff, "Use of Formal Methods at Amazon Web Services," 2014. [Online]. Available: <https://lamport.azurewebsites.net/tla/formal-methods-amazon.pdf>.

[2] D. D. Cristiano Calcagno, Jeremy Dubreil, Dominik Gabi, Pieter Hooimeijer, Martino Luca, Peter O’Hearn, Irene Papakonstantinou, Jim Purbrick, and Dulma Rodriguez, "Moving Fast with Software Verification," 2015. [Online]. Available: <https://scontent.fbne9-1.fna.fbcdn.net/v/t39.8562-6/240833217_205680324926309_8333067963679053381_n.pdf?_nc_cat=100&ccb=1-5&_nc_sid=ad8a9d&_nc_ohc=lX1oaHx01_EAX_AYpD7&_nc_ht=scontent.fbne9-1.fna&oh=00_AT8Y-NqGxzd2nkj_x290f9CxqmU3eUTeFalj6rcKZPWjjg&oe=623F0F2E>.

[3] M. K. Ioana Rodhe, "Overview of formal methods

in software engineering," 2015.

[4] M. Gordon, "Background reading on Hoare Logic," 2016.

[5] H. P. Krysta Yousoufian, Michael Ernst, David Notkin, and Dan Grossman. "Reasoning About Code, Part 1." <https://www.cs.williams.edu/~freund/cs326/ReasoningPart1.html> (accessed.

[6] K. T. Shaoying Liu, Toshinori Hayashi, Toshihiro Nakayama, "Teaching Formal Methods in the

Context of Software Engineering," 2014.

[7] R. B. Wolfgang Ahrendt, and Reiner H¨ahnle, "Integrated and Tool-Supported Teaching

of Testing, Debugging, and Verification," pp. 125-143, 2009.

[8] V. W. K. Rustan M. Leino, "The Dafny Integrated Development Environment," 2014.

[9] R. L. F. K. Rustan M. Leino, David R. Cok, *Dafny Reference Manual*, 2021.

[10] G. Smith, "Tutorial 3 Solutions," ed, 2021.

1. (K.R.M. Leino, private communication, 26 January, 2022) [↑](#footnote-ref-1)
2. (K.R.M. Leino, private communication, 23 February, 2022) [↑](#footnote-ref-2)