Expanding the proof rule base of AtelierB automated prover - Research Proposal

Agata Borkowska, UID: 1690550, *MSc in Computer Science, University of Warwick*

***Abstract*—AtelierB is a tool for formal software development through refinement, using the B-method. It incorporates an automated prover, which has been recognized as the most thorough prover for B set theory, and has been used as a basis for many others. Nevertheless it has multiple shortcomings. Various approaches have been suggested and taken to improve its performance, including extensions to the proof rule base, created by the users. In this work we aim to create such an extension, ensuring that all added rules are sound and well-reasoned. We also aim to identify any limitations of this approach. The secondary goal is to improve the robustness of the software without straying from pure B method, and taking into account the ease of use. As a metric of our success, we use the benchmarks proposed by Conchon and Iguernala [1].**

***Index Terms*—B method, formal verification**

I. Introduction

The aim of formal specification and verification is to ensure the correctness of software. While overall less popular than quality assurance through testing, it is most commonly used in safety-critical areas, such as air traffic control, railway routing, or medical cyber-physical systems, or where testing is too costly or puts the users at risk. It allows for certifying that a given piece of software works as intended, and is error-free.

Various methods and approaches have been developed. In this project, we shall focus on the B-method, allowing for formal specification through refinement of abstract machines.

II. Related Works

A. Applications of B-method

B. Available models

C. Methods for verifying proof rules

D. Case studies

[Verification of ProB goes here]

III. Project Aims

A secondary aim of the project is to understand and assess the limitations of this approach to improve the functionality of automated provers.

It is expected that over the course of this project, new questions and ideas will arise. Some, but not all may be pursued, while others will be identified as areas for further research.

A. Choice of Scenarios

To recognize the most commonly problematic proof obligations, we will collect a few scenarios created by various research groups or companies. This will ensure that the issues with the prover will not be user-specific.

The most important criteria in choosing third party models will be created using only B-method (and not extensions to it, such as Event-B), and that they will be well-documented, especially in terms of tools used for verification.

As it has been identified in the literature review, the industry that most commonly uses the B-method in practice is Railway, and there are models available online [cite]. However, it is well within the scope of this project to assess if there are problems common to different scenarios.

Thus, the railway industry will be the primary focus, however we will compare the improvements made across a range of scenarios, not limited to this area.

B. Metrics

C. Expected learning outcomes

D. Appropriateness of Research Methods

IV. Project Management

A. Methodology

B. Timeline

Key dates, as listed by the CS907 Dissertation Project website, are:

- **19th January:** Registration of dissertation topics
- **16th February:** Submission of project proposals
- **24-28th April:** Project presentations

- **6th July:** Submission of interim reports
- **14th September:** Submission of dissertation

It is also important to take into account dates of terms, which are 9th January to 18thMarch for the Spring Term, and 24th April to 1st July for the Summer term, with the university examinations commencing on or after the 15th May, and being spread over a period of about two weeks. Therefore, it is to be expected that little progress will be made during Spring Term and especially in May, with the bulk of the work being done over holiday and after the examination period.

The Gantt chart in Fig. X shows an estimate of the project's timeline.

C. Progress

D. Constraints and Risks

1) Copyrights for AtelierB software:

2) Requirement for knowledge outside the subject area: The B-method relies heavily on first order logic and Zermelo-Fraenkel set theory, and especially the latter is beyond the scope of the course (MSc in Computer Science). Fortunately, this area has been covered in depth during my previous degree (BA in Mathematics).

3) Risk of data loss or machine failure: A GitHub repository has been set up to contain a remote back up of the work done so far, thus also safeguarding against theft or loss of data storage devices. It has the additional benefits of allowing work from multiple machines, and convenient tracking of changes. The address of the repository is: https://github.com/agata-borkowska/dissertation .

This is a reasonable precaution we have deemed it to be sufficient, provided the changes are committed whenever significant progress has been made.

4) Time estimates: This project is intended to be flexible, and following an agile approach. It is fully expected that over the course of this project, new questions will occur, and we may or may not choose to pursue them. Thus, it should be noted that the presented timeline is very rough. There are however a couple of milestones, such as the end of performing a review of existing methods and scenarios, and the beginning of benchmarking, which should not be postponed. To this end, time to work on the project will be scheduled and adhered to, and progress will be reported to the Supervisor.

Additionally, regular meetings with the Supervisor will aid with keeping it on track, Her advice will also be helpful in assessing if the pace of work is sufficient.

Therefore, mistakes in the estimates of time taken to complete tasks are not a severe issue.

V. Concluding remarks

References

[1] S. Conchon and M. Iguernlala, "Increasing Proofs Automation Rate of Atelier-B Thanks to Alt-Ergo" in *Proc. 1st Int. Conf. Reliability, Safety and Security of Railway Systems* (RSSRail 2016), Springer, 2016, pp. 243-253