SWE-4805: Software Verification and Validation

Introduction

Md. Nazmul Haque
Lecturer, IUT

Department of Computer Science and Engineering
Islamic University of Technology

December 14, 2021

Contents

- Seven myths of formal methods [1]
- Seven more myths of formal methods [2]

Seven Myths of Formal Methods [1]

1. Formal methods can guarantee that software is perfect.

Fact: Formal methods are fallible. It has some intrinsic limitations, and it arises from two facts-

- Some things can never be proved.
- We can make mistakes in the proof of those things we can prove.

Seven Myths of Formal Methods [1]

2. Formal methods are all about program proving.

Fact: Formal methods are all about specifications.

Formal methods denote the use of mathematics in software development. The main activities are-

- Writing a formal specification.
- Proving properties about the specification.
- Constructing a program by mathematically manipulating the specification, and
- Verifying a program by mathematical arguments.

Seven Myths of Formal Methods [1]

3. Formal methods are only useful for safety critical systems.

Fact: Formal specifications help with any system.

Formal methods should be used wherever the cost of failure is high.

Seven Myths of Formal Methods [1]

4. Formal methods require highly trained mathematicians.

Fact: The mathematics for specification is easy.

For example, in an Alloy Analyzer, the only branches of mathematics we need to write specifications are **set theory** and **relational logic**.

Seven Myths of Formal Methods [1]

5. Formal methods increase the cost of development.

Fact: Writing a formal specification decreases the cost of development.

Seven Myths of Formal Methods [1]

6. Formal methods are unacceptable to users.

Fact: Formal specifications help users understand what they are getting.

The specification captures what the user wants before it is built.

Seven Myths of Formal Methods [1]

7. Formal methods are not used on real, large-scale software.

Fact: Formal methods are used daily on industrial projects.

- Transaction processing
- Hardware
- Compilers
- Software tools

Seven Facts of Formal Methods [1]

Instead of perpetuating the seven myths, seven facts are offered to replace them-

1. Formal methods are very helpful at finding errors early on and can nearly eliminate certain classes of errors.
2. They work largely by making you think very hard about the system you propose to build.
3. They are useful for almost any application.
4. They are based on mathematical specifications, which are much easier to understand than programs.
5. They can decrease the cost of development.
6. They can help clients understand what they are buying.
7. They are being used successfully on practical projects in industry.

Seven More Myths of Formal Methods [2]

8. Formal methods delay the development process.

The Inmos T800 floating-point unit chip, produced using Z and the Occam Transformation System, was finished **12 months ahead** of schedule.

The application of Z (and more recently B) to IBM's CICS system resulted in **9 percent savings in development costs**.

Seven More Myths of Formal Methods [2]

9. Formal methods lack tools.

Z, Alloy Analyzer, TLA (Temporal Logic of Actions), TLA+ and so on are available.

Seven More Myths of Formal Methods [2]

10. Formal methods replace the traditional engineering design methods.

One of the major criticisms of formal methods is that they are not so much "methods" as formal systems.

Seven More Myths of Formal Methods [2]

11. Formal methods only apply to software.

Formal methods can be applied equally well to **hardware** design and **software** development. Indeed, this is one of the motivations of the HOL theorem prover that was used to verify parts of the Viper microprocessor.

Seven More Myths of Formal Methods [2]

12. Formal methods are unnecessary.

Although there are occasions in which formal methods are in a sense "overkill," in other situations they are very desirable.

In fact, the use of formal methods is recommended in any system where **correctness** is of concern.

Seven More Myths of Formal Methods [2]

13. Formal methods are not supported.

Formal methods (in particular Z, VDM, CSP, and CCS) are taught in most UK undergraduate computer science courses.

Seven More Myths of Formal Methods [2]

14. Formal-methods people always use formal methods.

ANY QUESTION ?
THANK YOU !

Acknowledgements

[1] Hall, Anthony. "Seven myths of formal methods." IEEE software 7.5 (1990): 11-19.

[2] Bowen, Jonathan P., and Michael G. Hinchey. "Seven more myths of formal methods." IEEE software 12.4 (1995): 34-41.