What are Formal Methods

A Layman's View

Edsger W. Dijkstra

- Program testing can be used to show the presence of bugs, but never to show their absence!

- If you want more effective programmers, you will discover that they should not waste their time debugging, they should not introduce the bugs to start with.

Natural language has problems

- “English is a foreign language” – for us not for US
- There is a lack of clarity when we use natural language
- It is sometimes difficult to use language in a precise and unambiguous way without making the document wordy and difficult to read (I prefer to use a block diagram)
- Several different requirements may be expressed together as a single requirement (This happens all the time even with guidelines)
- You can say the same thing in completely different ways. (We found that Indian and US read the same requirement in different ways and test them)

Definitions

- Formal methods are techniques used to model complex systems as mathematical entities. (They are more precise)
- The complex system behavior is broken down into smaller units and each one of these is defined as mathematical equations. This is the TRUTH.
- Defining systems formally allows the engineer to validate the system (mathematically correct behavior - mostly safety criteria) using other means than testing – like a proof of correctness

Formal Methods are not new

- 1969

An Axiomatic Basis for Computer Programming

C. A. R. Hoare
The Queen's University of Belfast, Northern Ireland*

- 1975

Guarded Commands, Nondeterminacy and Formal Derivation of Programs

Edsger W. Dijkstra
Burroughs Corporation

Three components

- Formal Specification
  - define a system using a modeling language. Modeling languages are fixed grammars which allow users to model complex structures out of predefined types (Z language)
- Verification
  - The engineer now has a set of theorems about his system. If the switch is on and BESCOM has not shutdown power IMPLIES light should be on.
  - The engineer now verifies this theorem and proves it correct.
  - He may find that for the light to glow the bulb should not be “fused”
- Implementation
  - This is converting the formal model to code for implementing on computer

Why so long for acceptance

- SHOES MUST BE WORN.
- DOGS MUST BE CARRIED.

$$\forall p : PERSON \bullet$$
$$(\exists s1, s2 : SHOE \bullet wears(p, s1, s2))$$
$$\wedge\ (\forall d : DOG \bullet isWith(p, d) \Rightarrow carries(p, d))$$

Light weight (semiformal??)

- Formal rigorous proof can be time consuming. In safety critical application the tool will have to be qualified.
- Industry has accepted that there is a necessity for formal proof but in few limited cases.
  - Operating system was certified using formal methods (testing was very difficult)
  - We have used this in SARAS for the autopilot mode transitions
  - AIRBUS has used it for removing low level testing of code

Advantages

- Experience shows that the act of capturing requirements using formal notations is of benefit as it forces the writer to ask questions that would otherwise be postponed until coding
- Requirements expressed in a formal notation can also be analyzed early to detect inconsistency and incompleteness
- Formalized requirements prevent misunderstandings that lead to error introduction (80% of error is due to requirements)
- Exhaustive verification is possible such that all of the structure is verified over all possible inputs and states

We have been always told of its disadvantages!!

Teaching to unsuspecting youngsters the effective use of formal methods is one of the joys of life because it is so extremely rewarding.

(Edsger Dijkstra)

izquotes.com

Have a great three days ahead!!