

Welcome to COMP4100, COMP6410 and COMP6312

Management of Software Quality

- Lecturers: Malcolm Newey and TBA (Chris Johnson?)
- Material: Formal Methods (MCN) and Process Techniques (TBA)
- Prerequisites
- 50-50 split between halves
- Labs in weeks 2 and 4
- Tutes in weeks 6,7,9 and 11
- Proposed Assessment Scheme

COMP4100 Lectures in 2007
(also COMP6410 and COMP6312)
by Malcolm Newey

Getting it Right, Formally

Lecture 1^a March 21, 2007

^aIf debugging is the process of removing bugs,
then programming must be the process of putting them in.

Scope of Formal Methods

- What's in a name?
- Is it agreed?
- Applied mathematics.
- Manipulable notations.

Purpose

- Relationship to Quality
- No nasty surprises!
 - Efficiency
 - Correctness
 - Adaptability
 - Liveness or Termination
- Are they useful?
- Are they used?
- Are they cost-effective?

Application by Industry

All these are are full of safety critical systems.

- AeroSpace systems
- Railways
- Process Control
- Military systems
- Computers
- Automotive

Application by Software Category

- Critical Systems
 - Safety critical
 - Security critical
 - Social critical
 - Cost critical
- Components
- Applets
- Proof carrying code

Life cycle correlation

- Specification - ambiguity, inconsistency, completeness
- Design - refinement
- Implementation - debugging & verification^a
- Testing - automation
- Documentation - rigour
- Maintenance - verification^b

^aIf it was hard to write, it should be hard to understand.

^bThe Definition of an Upgrade: Take old bugs out, put new ones in.

Related Computer Science

- Logics^a
- Theorem proving
- Semantics

”Because both the system’s privacy and the security of digital money depend on encryption, a breakthrough in mathematics or computer science that defeats the cryptographic system could be a disaster. The obvious mathematical breakthrough would be development of an easy way to factor large prime numbers.”

– Bill Gates from ”The Road Ahead,” p. 265.

^aSomeone who thinks logically provides a nice contrast to the real world.

Table of Contents

- Logic that is better than predicate calculus
- Infrastructure for theorem proving
- Automated reasoning
- Specification in Z, VDM, B or Object Z
- Petri Nets
- Temporal Logic and Model Checking

Notes on Prerequisite

- Is COMP2600 required?
- Automata Theory
- Skill with logic and set theory
- Functional programming language
- Notions of Program proof
- Z

What comes next?

- Introduction to HOL - Higher Order Logic
- Design of HOL - the system, that is.
- Forward proof in HOL
- Goal directed proof
- HOL as a representative of a class of interactive proof engines.

What Else We'll Cover Today

We will start working through a HOL course by Melham

- The intended audience is industry
- 10 years old and has some pimples
- Today we'll cover *Introduction*
- 5 other chapters will be covered in lectures FM2 to FM7