CMPSCI 266 - Formal Specification and Verification
Winter 2009

Course Flow

The following is an attempt to layout the flow of the course for this quarter. This is a **rough estimate** and should be treated as such.

Introduction and Overview
- Proving vs. Testing
- Consistency vs. Correctness
- Total Correctness vs. Partial Correctness
- Current Government and Industrial Interest in Verification

Program Proofs
- Assertions, Loop Invariants, Induction

Axiomatically Defined Languages
- Verification Condition Generation
  - Symbolic Execution
  - Backwards Substitution

Abstract Data Types
- Hoare-like Axiomatic Specifications
- Algebraic Specifications

Introduction to ASLAN and the ASLAN Verification System

Description of Other Verification Systems and Comparison of the Different Approaches
- FDM
- Larch
- ASTRAL
- Z
- VDM

Special Verification Topics
- Temporal Logic
- Concurrent Processes
- Realtime Specifications

Applications of Verification Technology
- Secure Operating Systems
- Network Protocols
- Encryption Protocols

Problems and Limitations of Formal Verification