CMSC 630 Review

Course Topic Formal methods

- Verification frameworks
  - Sys
  - Spec
  - sat
- Verification methodologies
  - Proof
  - Algorithmic (“model-checking”)
- Sample frameworks
  - Hoare / Owicki-Gries
  - Temporal logic
  - Process algebra

Hoare / Owicki-Gries Review

- Sequential guarded-command language syntax, semantics
- Preconditions, postconditions
- Hoare triples
- Partial vs. total correctness
- Axioms and inference rules for Hoare triples
- Loop invariants
- Soundness, completeness, relative completeness
- Proof outlines
- Concurrent guarded-command language syntax, semantics
- Interference freedom

Temporal Logic Review

- Kripke structures
- Linear- vs. branching-time
- Linear-Time Temporal Logic (LTL) syntax, semantics
- Expressing properties in LTL
- CTL* syntax, semantics
- Path quantifiers
- CTL* vs. LTL vs. CTL
- CTL model-checking via proof
- Complete lattices and fixpoints of monotonic functions
- Recursive characterizations of CTL operators
- CTL model-checking proofs and circularity
- Algorithmic CTL model checking for finite-state systems
- Kleene's fixpoint theorem
- Binary decision diagrams

Process Algebra

- CCS syntax and semantics
- Static and dynamic operators in CCS
- Representing state machines, system architecture in CCS
- Strong bisimulation, strong equivalence
- Bisimulation, observational equivalence
- Congruences and observational congruence
- Hennessy-Milner Logic
- Axiomatizations for strong equivalence, observational congruence
- Unique Fixpoint Induction
- Guardedness
- Algorithms for strong, observational equivalence