CMSC 630 Review

- Propositional and predicate logic
  - Syntax
  - Semantics
  - Axioms and inference rules
  - SAT / SMT solving

- Verification frameworks
  - Sys
  - Spec
  - sat

- Verification methodologies
  - Proof
  - Algorithmic ("model-checking")

- Sample frameworks
  - Hoare
  - Temporal logics (linear-time, branching-time)
  - Process algebra

©2015 Rance Cleaveland. All rights reserved.
Propositional and Predicate Logic Review

- States
- \( \models \)
- Satisfiability / tautology
- Falsifiability / inconsistency
- Truth tables
- Davis-Putnam-Logemann-Loveland
- Sequent calculus
- Judgments
- Identity axiom / cut rule
- Left / right / logical / structural rules
- Soundness and completeness
- Data theories
- Free and bound variables
- Logical (Gödel) validity and completeness for predicate calculus
- SMT solving
Hoare Review

- Sequential guarded-command language syntax
- (Big-step) Structural Operational Semantics (SOS)
- Preconditions, postconditions
- Hoare triples
- Partial vs. total correctness
- Axioms and inference rules for Hoare triples
- Loop invariants
- Proof outlines
- Weakest liberal preconditions
- Soundness, completeness, relative completeness
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
- Complete lattices and fixpoints of monotonic functions
- Recursive characterizations of CTL operators
- Algorithmic CTL model checking for finite-state systems
- Kleene's fixpoint theorem
- Büchi automata and LTL model checking
Process Algebra

• CCS syntax and semantics
• Representing state machines, system architecture in CCS
• Strong bisimulation, strong equivalence
• Bisimulation, observational equivalence
• Congruences and observational congruence
• Hennessy-Milner Logic
• (Strong) bisimulation equivalence as a fixpoint
• Equivalence relations and partitions
• Algorithms for strong equivalence