

Formal Specification and Verification

List of Topics

- **Propositional logic**

- Syntax, semantics
- Translation to CNF (also structure preserving translation; optimized translation)
- Methods for checking validity, satisfiability, entailment:
 - * Inference Systems and Proofs - Example: Hilberts Deductive System
 - * The Resolution Procedure
 - * Sequent calculi
 - * The DPLL procedure
 - * BDDs; OBDDs.

- **First-order logic**

- Syntax, semantics
- Logical theories (definitions; theories vs. models; example)
- Herbrand models, Term algebras, free algebras

- **Specification**

- Algebraic specification (without the introduction to CASL)
- Transition systems; Program graph representation; links
- Timed automata (definition), hybrid automata (definition)

- **Verification**

- Temporal logic
 - * LTL (syntax, semantics)
 - * CTL (syntax, semantics)
 - * Comparison between LTL and CTL
 - * Model checking
 - Problem description
 - Algorithm which computes the set of states at which a CTL formula holds
 - Implementation based on OBDDs
- Propositional dynamic logic
 - * Syntax, semantics
 - * Axiom system for PDL:
 - Soundness and Completeness: definitions; proof idea;
 - * Finite model property \leftrightarrow decidability
 - * Using a (given) sequent system for proving formulae in PDL.

- Deductive verification for infinite state systems: An introduction
 - * Succinct representation of sets of states and of transitions between sets of states using formulae.
 - * Verification problem: Program + Description of the bad states
 - Succinct representation using formulae
 - Initial state, error state, transition relation, computation,
 - Checking safety: compute set of reachable states
 - post operator (idea); iterations; Forward reachability analysis
 - pre operator (idea); Backward reachability analysis (idea)