Decision procedures for verification

February 3, 2019

1. **Propositional logic**
   - Syntax; semantics; models, validity, satisfiability, entailment, equivalence;
   - Translation to CNF/DNF (in particular structure-preserving translations!);
   - Resolution: soundness; completeness (multiset orderings; ordering on clauses; the model construction; idea of completeness proof)
   - The DPLL method (only the method, no soundness/completeness proofs required)
2. **First-order logic**
   - Syntax, semantics: models and assignments; validity, satisfiability; Entailment and equivalence;
   - Validity vs. unsatisfiability.
   - The theory of a structure; Logical theories (syntactic/semantics view).
   - Normal forms and Skolemization
   - Herbrand interpretations (definition)
   - General resolution:
     resolution for ground clauses, Robinson's idea;
     unification (definition of a most general unifier; algorithm for computing a most general unifier; no proofs required),
     lifting lemma (idea),
     saturation of sets of general clauses, refutational completeness of general resolution (idea), ordered resolution with selection, redundancy
   - Herbrand's theorem, Craig Interpolation, the theorem of Löwenheim-Skolem (only statements)
3. **Decidable fragments of first-order logic**
   - Variable-free formulae
   - The Bernays-Schoenfinkel class
     (definition, main idea in decidability proof)
   - The Ackermann class
     (definition, rough idea of decidability proof presented in the lecture)

- The monadic class (definition, idea of decidability proof presented in the lecture)

4. **Satisfiability with respect to a theory**
   - T-validity vs. T-satisfiability.
5. **Decision procedures for checking satisfiability with respect to a theory for conjunctions of literals**
   - **Single theories**
     - Theory of uninterpreted function symbols
       (validity of univ. formulae; satisfiability of ground formulae)
       Satisfiability check using congruence closure on DAGs (the algorithm presented in the lecture)
     - Difference logic (method for checking satisfiability, idea of proof)
     - Linear arithmetic over $\mathbb{Q}$ and $\mathbb{R}$:
       * Fourier-Motzkin Quantifier Elimination
   - **Combinations of theories**
     - Combinations of theories (definition: syntactical vs. semantical view; examples)
     - The Nelson/Oppen procedure for reasoning in combinations of theories over disjoint signatures
       * the method
         (purification; propagation - guessing version vs. backtracking version)
       * soundness and completeness
         (completeness: definition of stable infinity; role of stable infinity; idea of completeness proof)
       * deterministic version and convexity
6. **Satisfiability modulo a theory for sets of clauses**
   - DPLL(T)
7. **Theories of data structures**
   - The array property fragment (definition; decision procedure (the 7 steps)).