Decision Procedures

Jochen Hoenicke

Software Engineering
Albert-Ludwigs-University Freiburg

Winter Term 2019/2020

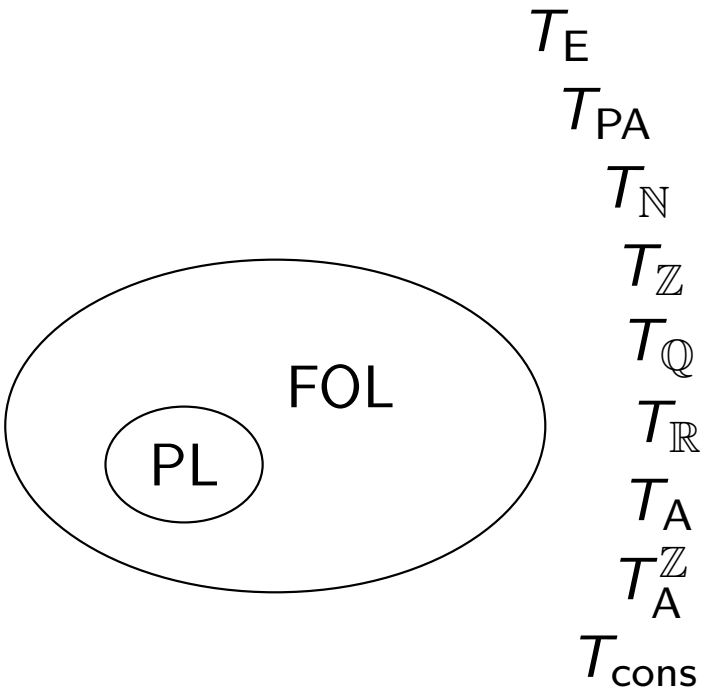
Conclusion

Topics

Topics
Propositional Logic
First-Order Logic
First-Order Theories
Quantifier Elimination for $T_{\mathbb{Z}}$ and $T_{\mathbb{Q}}$
Congruence Closure Algorithm (T_{E}, T_{cons}, T_{A})
Dutertre–de Moura Algorithm ($T_{\mathbb{Q}}$)
DP for Array Property Fragment
Nelson-Oppen
DPLL(T) with Learning
Program Correctness
Interpolation

Logics

PL	Propositional Logic
FOL	First-Order Logic
T_x	Theories



Theories and their DPs

Theory	Full	Array Prop.	Quant. free	Conj. quant. free
T_{E}	✘	-	✔	✔
T_{PA}	✘	-	✘	✘
$T_{\mathbb{Z}}$	✔	-	✔	✔
$T_{\mathbb{Q}}$	✔	-	✔	✔
$T_{\mathbb{R}}$	✔ (-)	-	✔ (-)	✔ (-)
T_{A}	✘	✔	✔	✔
$T_{\mathsf{A}}^{\mathbb{Z}}$	✘	✔	✔	✔-
T_{cons}	✘	-	✔	✔
$T_1 \cup T_2$	-	-	✔ (-)	✔ (-)

- What is an atom, a literal, a formula?
- What is an interpretation?
- What does $I \models F$ mean, how do we compute it?
- What is satisfiability, validity?
- What is the duality between satisfiable and valid?
- What is the Semantic Argument?
- Write down the proof rules.
- How can we prove $P \wedge Q \rightarrow P \vee \neg Q$?
- What is $\Leftrightarrow$ (equivalent) and $\Rightarrow$ (implies)?
- What Normal Forms do you know (NNF, DNF, CNF)?
- How are formulae converted into normal form?

DPLL for Propositional Logic

- What is a Decision Procedure?
- What is equisatisfiability; why is it useful?
- How can we convert to CNF with polynomial time complexity?
- What is a clause?
- What does DPLL stand for?
- What is Unit Propagation (UP)?
- What is Pure Literal Propagation (PLP)?
- Why is the DPLL algorithm correct?
- What is the worst case time complexity of DPLL?

First-Order Logic

- What is a variable, a constant, a function (symbol), a predicate (symbol), a term, an atom, a literal, a formula?
- How do first-order logic and predicate logic relate?
- What is an interpretation in FOL?
- Why is D_I non-empty?
- What does α_I assign?
- What is an x-variant of an interpretation?
- How do we compute whether $I \models F$?
- What is satisfiability, validity?
- What are the additional rules in the Semantic Argument?
- What is soundness and completeness of Semantic Argument?
- Normal forms. What is PNF (prenex normal form)?
- Is validity for FOL decidable?

First-Order Theories

- What is a theory?
- What is a signature Σ?
- What do T-valid and T-satisfiable mean?
- What is T-equivalent?
- What is a decision procedure for a theory?
- What is a fragment of a theory?
- What are the most common fragments (quantifier-free, conjunctive)?
- What theories do you know?
- What are their axioms?
- What fragments of these theories are decidable?
- Bonus Question: Is there any closed formula in T_{PA} that is satisfiable but not valid? What about $T_{\mathbb{Z}}$, $T_{\mathbb{Q}}$?

Quantifier Elimination

- What is Quantifier Elimination?
- Does $T_{\mathbb{Z}}$ admit quantifier elimination? What does it mean?
- Why is it enough to eliminate one existential quantifier over a quantifier-free formula?
- How can we eliminate more than one quantifier?
- What is $\widehat{T_{\mathbb{Z}}}$?
- What is Cooper's method?
- What is Ferrante and Rackoff's method ($T_{\mathbb{Q}}$)?
- What is the Array Property Fragment?
- What do all quantifier elimination methods of the lecture have in common?
- What is the complexity of quantifier elimination?
- Why is quantifier elimination a decision procedure?

Congruence Closure Algorithm

- What is the congruence closure algorithm?
- How does it work for T_E?
- What are the data structures; what are the operations?
- What complexity does the algorithm have?
- What are the extensions for T_{cons}?
- What is the complexity?
- How did we prove correctness of the decision procedure?

Simplex Based Algorithm

- Which theory does the algorithm of Dutertre and de Moura decide?
- How does the algorithm work?
- How can we convert an arbitrary formula to the required format for the algorithm?
- What is the tableau?
- What is a pivot step?
- Does the algorithm terminate?
- What is the complexity?

Decision Procedure for T_{A}

- How does the DP for the quantifier-free fragment of T_{A} work?
- What is the complexity?
- What is $T_{\mathrm{A}}^{=}$?

Array Property Fragment

- What is the Array Property Fragment of $T_{\mathrm{A}}/T_{\mathrm{A}}^{=}$?
- Why are there so many restrictions?
- What are the transformation steps?
- How are quantifiers eliminated?
- What is λ and why is it necessary?
- Why is the decision procedure correct?
- What is the Array Property Fragment of $T_{\mathrm{A}}^{\mathbb{Z}}$?
- What are the differences between $T_{\mathrm{A}}^{\mathbb{Z}}$ and T_{A}?
- Why do we not need λ for $T_{\mathrm{A}}^{\mathbb{Z}}$?
- Why is the decision procedure correct?
- How can we check this fragment?

Nelson-Oppen

- What is the Nelson-Oppen procedure?
- For what theories does it work? For which fragment of the theory?
- What is a stably infinite theory?
- Why is it important that theories are stably infinite?
- What are the two phases of Nelson-Oppen?
- What is the difference between the non-deterministic and deterministic variant of Nelson-Oppen?
- What is a convex theory?
- What is the complexity of the deterministic version for convex/non-convex theories?

DPLL(T)

- How can we extend the DPLL algorithm to decide T-satisfiability?
- What is a minimal unsatisfiable core?
- How can we compute it efficiently for, e.g., $T_{\mathbb{Q}}$?
- What is the relation between min. unsat. core and conflict clause?
- Why is the algorithm correct, why does it terminate?
- How can we extend it to more than one theory?

Program Correctness

- What is a specification?
- What types of specification are in a typical program? (Precondition, postcondition, loop invariants, assertions)
- When is a procedure correct (partial/total correctness)?
- What is a basic path? Why is it useful?
- How do we prove correctness of a basic path?
- What is a verification condition?
- What is the weakest precondition?
- How do we compute the weakest precondition?
- When is a program partially correct?

Interpolants

- What is an interpolant?
- What is the symbol condition?
- Why is an interpolant useful?
- How can we compute interpolants in T_E?
- How can we compute interpolants in $T_{\mathbb{Q}}$?
- How can we compute interpolants for DPLL proofs?

General hints for exam

- You should learn definitions (formally).
  This includes the rules (Semantic Argument, DPLL with learning).
- You should understand them (informally).
- You should know important theorems.
- Knowing the proofs is a plus. Don't lose yourself in the details!
- You should be able to apply the decision procedures.
  Do the exercises! Invent some new exercises and solve them!
- You should know some examples/counter-examples,
  e.g., why is quantifier elimination in $T_{\mathbb{Z}}$ not possible?
- When you feel well prepared, check if you can answer the questions in this slide set.
- When learning, do not leave out a topic completely!
- Learn in a group. Ask questions to each other and answer them as if you were in the exam.

Organisation

- There will be only oral exams for this lecture.
- You should have officially registered at the Prüfungsamt.
- The exams will be on February 26th, 2020