ETH zürich

Alexander J. Summers

Program Verification

Exercise Sheet 3: SMT Solving Algorithms

Assignment 1 (Propositional Abstraction)

Give examples of a theories T, T-formulas A and corresponding propositional abstractions A^p such that (you can choose different examples for each part):

1. A is unsatisfiable, but A^p is satisfiable.
2. For some satisfiable T-formula B, $A \models B$ but $A^p \not\models B^p$
3. A and A^p are equivalent

Assignment 2 (Theory Deduction)

On slide 67, it is explained that we can ask a theory solver to produce additional literals implied by the current candidate model. Such a step can augment the other deduction steps in DPLL, such as unit propagation.

In principle, it is possible to allow a theory to produce literals which were not in the original formula. For example, if we have already added $a \leq b$ and $b \leq c$ to the current model, the theory solver could be allowed to add $a \leq c$ to the current model, even if this literal does not occur in the input formula. What problem could this potentially lead to in the overall algorithm? Can you think of circumstances in which such theory deductions could still be safely allowed?

Assignment 3 (Applying Nelson-Oppen)

Apply non-deterministic Nelson-Oppen to the formula $\neg(f(i) - f(j) = 0) \wedge i - j = 0$. How many "guesses" of equivalence relations could possibly be needed, in the worst case? Note that you will have to act as a theory solver for the two theories (for these formulas, it should not be hard to simulate a theory solver's behaviour).

Apply deterministic Nelson-Oppen to the formula, instead. Note that the sub-theory of Presburger Arithmetic *without* inequalities is convex, as is the theory of uninterpreted functions. Is Presburger arithmetic in general convex?

Assignment 4 (Theory Combination)

A theory T is *consistent* if $\emptyset \not\models_T \bot$.

Give examples of theories T_1 and T_2 which are consistent, but whose combination are not (hint: consider the requirements for applying Nelson-Oppen combination to two theories).