Logical reasoning and programming, lab session 4

(October 19, 2020)

The following exercises require an SMT solver. For simplicity, you can use

- an online version of Z3, or
- an online version of CVC4,

or both. Even better, you can install Z3 or CVC4 yourself. Another option is to use pySMT, a convenient way how to experiment with various SMT solvers in Python. If you want to learn a bit more about the Z3 prover, you should start with this tutorial. Moreover, if you want to play with the Z3 prover in Python, check Programming Z3. However, if you want to experiment with SMT solvers in Python, you should try pySMT.

4.1 Symmetry breaking and PHP_n^{n+1} (cont'd). For details see Knuth's TAOCP on satisfiability or slides Symmetry in SAT: an overview.

4.2 Try BreakID.

4.3 Decide whether it is satisfiable in the theory of uninterpreted functions that

$$x = f(f(f(f(f(x))))) \wedge x = f(f(f(x))) \wedge x \neq f(x).$$

4.4 Try all the examples in the SMT-LIB Examples.

4.5 Show that $x - y > 0$ iff $x > y$ holds for integers, but does not hold for bit-vectors with a fixed length.

4.6 Let x be a 32 bit-vector. You want to verify that if you do $x \gg_s 31$ (arithmetic right shift is `bvashr`) followed by one of the following

- $(x \oplus y) - y$, or
- $(x + y) \oplus y$, or
- $x - ((x + x) \& y)$,

then you get the absolute value of x.

4.7 You can find many examples in Dennis Yurichev's SAT/SMT by Example.

4.8 If we want to combine theories in SMT using the Nelson–Oppen method, we require that both of them are stably infinite. Assume two theories $\mathcal{T}_1$ with the language $\{f\}$ and $\mathcal{T}_2$ with the language $\{g\}$, where f and g are uninterpreted unary function symbols. Moreover, $\mathcal{T}_1$ has only models of size at most 2 (for example, it contains $\forall X \forall Y \forall Z (X = Y \vee X = Z)$ as an axiom). Show that the Nelson–Oppen method says that

$$f(x_1) \neq f(x_2) \wedge g(x_2) \neq g(x_3) \wedge g(x_1) \neq g(x_3).$$

is satisfiable in the union of $\mathcal{T}_1$ and $\mathcal{T}_2$, but this is clearly incorrect.