Logical reasoning and programming, lab session 6

(October 25, 2021)

Some exercises require an SMT solver, e.g., CVC4 has an online version.

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

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

6.3 Let x be a 32 bit-vector. You want to verify that if you take $y = x \gg_s 31$ (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. For further details, check this webpage.

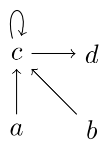
6.4 Try CBMC, using MiniSAT and Z3, on `f11`, `f12`, `f13`, and `f14` from this example. For details, see these lecture notes.

6.5 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.

6.6 We have a language that contains only one binary predicate symbol $\in$ and we have an interpretation $\mathcal{M} = (D, i)$ such that $D = \{a, b, c, d\}$ and $i(\in)$ is given by the following diagram:



Meaning that $x \in y$ iff there is an arrow from x to y. Decide whether the following formulae are valid in $\mathcal{M}$:

(a) $\exists X \forall Y (\neg(Y \in X))$,

(b) $\exists X \forall Y (Y \in X)$,

(c) $\exists X \forall Y (Y \in X \leftrightarrow Y \in Y)$,

(d) $\exists X \forall Y (Y \in X \leftrightarrow \neg(Y \in Y))$.

6.7 Show that the following formulae are valid and provide counter-examples for the opposite implications:

(a) $\forall X p(X) \lor \forall X q(X) \rightarrow \forall X (p(X) \lor q(X))$,

(b) $\exists X (p(X) \land q(X)) \rightarrow \exists X p(X) \land \exists X q(X)$,

(c) $\exists X \forall Y p(X, Y) \rightarrow \forall Y \exists X p(X, Y)$,

(d) $\forall X p(X) \rightarrow \exists X p(X)$.

6.8 Show that the "exists unique" quantifier $\exists!$ does not commute with $\exists$, $\forall$, nor $\exists!$.