Model Checking, SS2011: Exercise Sheet 10

June 7, 2011

Note. Slides relevant to this exercise sheet come from the lecture on June 7th.

Exercise 10.1. Write a proof for the following lemma following the guidelines in Tom Henzinger's "How to write a proof"[1]. Let us denote first order linear arithmetic implication by $\subseteq$, and propositional implication by $\sqsubseteq$. If

$$\alpha(S) = \psi$$

$$\alpha(T) = \phi$$

then

$$\psi \subseteq \phi \textit{ iff } \psi \sqsubseteq \phi$$

Exercise 10.2. Give the following Prolog programs.

1. Procedure `sublist`/2 that succeeds if the first parameter is a sublist of the second parameter.
2. Procedure `collatz`/2 such that `collatz(N,L)` succeeds if `L` is from left-to-right a collatz sequence that starts at `N` and stops at `1`.

Exercise 10.3. Test on past exercises each of the following modifications to the simple model checker presented in class.

1. Case 1 in slide 3: Do not add to the reached abstract state list a newly reached s if s is subsumed by some already reached abstract state.
2. Case 2 in slide 3: Drop s from the reached abstract state list if s is subsumed by some newly reached abstract state.
3. Combine cases 1 and 2.

Exercise 10.4. Prove that if our simple model checker (SMC) is modified combining cases 1 and 2 as described in exercise 10.3, the elements of the set of reachable states given by SMC are uncomparable.

[1] http://mtc.epfl.ch/courses/ProblemSolving-summer05/howtoproveit.pdf

Exercise 10.5. Consider the following code fragment.

```
res = 0;
while (x > 0 && y > 0) {
 res = res + x * y;
 x = x - 1;
 y = y - 1;
}
```

Use the method described in class to compute a ranking function that witnesses the termination of the code fragment.