

CMPS 290G – Topics in Software Engineering
Winter 2004 – Software Validation and Defect Detection
Homework 4

Due: 2 March 2004

1. Consider the standard weakest precondition translation:

$$\begin{aligned}wp(x := E, Q) &= Q[E/x] \\wp(S_1; S_2, Q) &= wp(S_1, wp(S_2, Q)) \\wp(\text{if } E \text{ then } S_1 \text{ else } S_2, Q) &= (E \Rightarrow wp(S_1, Q)) \wedge (\neg E \Rightarrow wp(S_2, Q))\end{aligned}$$

What is the worst-case relationship between the size $|S|$ of a statement S and the size $|wp(S, Q)|$ of $wp(S, Q)$. That is, can you define a function f such that, for all statements S ,

$$|wp(S, Q)| \leq f(|S|)$$

2. Consider a *partial order* theory that contains a single predicate symbol “ $<$ ” that is irreflexive and transitive. Define a decision procedure for checking satisfiability in this theory.

This decision procedure *checkSatLits* should take as input a conjunction of literals, each of which is of the form $t_1 < t_2$ or $\neg(t_1 < t_2)$, and should decide if the conjunction is satisfiable. You should make this decision procedure asymptotically fast. You may express your algorithm in terms of standard graph operations if you like.

Extra credit: If the input conjunction is unsatisfiable, have the procedure *checkSatLits* return a precise tautology that explains that unsatisfiability.

3. Is the following formula satisfiable? Give a proof of your answer.

$$\begin{aligned}&g(g(z) - g(y)) \neq g(w) \\ \wedge &y \geq z \\ \wedge &z \geq y + w \\ \wedge &w \geq 0\end{aligned}$$