CS389L: Problem Set 7

1. Recall that the Nelson-Oppen method requires the theories to be combined to be *stably infinite*. Give an example to demonstrate why this restriction is necessary. Specifically, give two theories T_1, T_2, and a $(T_1 \cup T_2)$- formula F such that F is unsatisfiable but we would conclude otherwise using the Nelson-Oppen method.

2. Consider the following formula F in $T_= \cup T_\mathbb{Z}$:

$$g(f(x-2)) = x + 2 \land g(f(y)) = y - 2 \land y = x - 2$$

   (a) Purify F by writing it as an equisatisfiable formula of the form $F_1 \land F_2$ such that F_1 is in $T_=$ and F_2 is in $T_\mathbb{Z}$.

   (b) Decide the satisfiability of F using the Nelson-Oppen method.

3. Recall that the DPLL(T) framework invokes the solver for theory T to learn conflict clauses and theory propagation lemmas. In this question, we will explore the inference of theory propagation lemmas.

   (a) Let D_T be a decision procedure for a conjunction of Σ_T literals. Describe how one can perform exhaustive theory propagation for T without modifying the decision procedure D_T. (Note: *exhaustive* means that we want to infer all theory propagation lemmas.)

   (b) Suppose T is the theory of equality with interpreted functions. Explain how we can infer theory propagation lemmas for this theory after running the congruence closure algorithm on the current partial assignment.

4. Consider the following program S:

```
y := 0; i:=0;
while(i<n) {
  t := 2i+1; y := y+t; i := i+1;
}
```

   Our goal in this problem is to prove the correctness of the Hoare triple $\{n > 0\}\ S\ \{y = n \times n\}$

   (a) State an inductive loop invariant I that is sufficient to prove the correctness of the above Hoare triple.

   (b) Compute the weakest precondition of I (from part (a)) with respect to the loop body B.

   (c) Show all VCs that are generated for proving the Hoare triple $\{n > 0\}\ S\ \{y = n \times n\}$ using invariant I from part (a).

5. Prove the correctness of the following derived proof rule for loops:

$$\frac{P \Rightarrow I \quad \vdash \{I \land C\}S\{I\} \quad I \land \neg C \Rightarrow Q}{\vdash \{P\} \text{ while}(C) \text{ do } S\ \{Q\}}$$