Homework #4

CS 474: Spring 2023

Due on Tue, Dec 10, 2024 11:59 PM Central

Homework Policy: You are allowed to collaborate with your classmates, but declare it in your submission. Even if you work on problems together, each student must write up their solution in their own words in their submission. The CS 473 course's page on academic integrity is a handy reference: https://courses.engr.illinois.edu/cs473/sp2023/integrity.html. Late submissions are not allowed. If you have personal circumstances that will prevent you from submitting on time, write to the course staff as soon as possible and we can try to work with you.

General Instructions: (1) For any problem where you are asked to come up with an encoding, do not simply give the final answer. Provide a high-level explanation for the choices made in your encoding and develop it step-by-step. Your solution must be easily understandable. (2) Whenever asked to encode a problem in Z3, describe the encoding at a high level if you have not already done so elsewhere in another problem/sub-problem. Do not copy-paste Z3 code into your submission. Upload the file(s) you write to a public GitHub repository and provide a link in your submission. Ensure that the time on the last commit does not exceed the deadline.

Points: Problem 1: 10+10 points, Problem 2: 10+10 points, Problem 3: 5+5+5+5 points Total: 60 points

Problem 1. In this problem you will prove a FOL formula valid by following the completeness procedure you learned: negate the formula, Skolemize it, and use systematic term instantiation to convert it to a quantifier-free formula, and finally check whether the quantifier-free formula is unsatisfiable using Z3.

For the formulas below, execute this procedure, giving precisely (i) the quantifier free formula obtained by instantiating terms of depth 0 only (i.e., using constants only) and (ii) showing that the obtained formula is unsatisfiable using Z3.

Task 1 Prove that under group axioms, there is no other identity.

Task 2 Prove that under group axioms, every element has only one inverse.

Use the group axioms in lecture notes. Consult the worked out example in the notes as well as Section 6.5.3 which works out the above theorems partially.

Problem 2. Consider the following quantifier-free formula written over a combination of two theories— theory of natural numbers with + and theory of uninterpreted functions (including the uninterpreted function symbol f).

$$\varphi : y \leq x \wedge x \leq y \wedge f(y) = f(7) \wedge x \leq 5$$

(a) Using the Nelson-Oppen method (nondeterministic), reduce the satisfiability of φ to satisfiability of formulas over the two distinct theories— theory of natural numbers and theory of uninterpreted functions.

(b) Give an arrangement of your variables such that the formula is satisfiable, and give a satisfying model for your formula, and hence derive a satisfying model for φ (your model for φ should be derived from the individual models and satisfy the chosen arrangement).

Problem 3.

(a) Let $f : 2^{\mathbb{N}} \longrightarrow 2^{\mathbb{N}}$ be defined as $f(S) = \{2\} \cup \{y \mid y = 2x, x \in S\}$.

What is the least fixpoint of f? (i.e., describe which elements belong to this least fixpoint set)

(b) Let $X = \{0, \ldots, 100\}$ (natural numbers from 0 through 100).
Let $f : 2^X \longrightarrow 2^X$ be defined as: $f(S) = \{100\} \cup \{y \in X \mid \exists z \in \mathbb{N}, z \textit{ is prime }, yz \in S\}$.

Argue why f is monotonic. Then compute, using the iterative method, the least fixpoint of f. You need to show all the sets $X_0, X_1, \ldots$ that you use to reach the lfp.

(c) Let $f : 2^{\mathbb{N}} \longrightarrow 2^{\mathbb{N}}$ be defined as Let $f(S) = S \cup \{0\} \setminus \{1\}$.

Is f monotonic? If you think it is, argue why it is, and also give the least fixpoint of f. If not, precisely argue why it is not using the definition of monotonicity.

(d) Let $f : 2^{\mathbb{N}} \longrightarrow 2^{\mathbb{N}}$ be defined as $f(S) = S \cup \{1\} \cup \{2x \mid x \in S\} \setminus \{x \mid x \in S, x \textit{ is odd}\}$.

Is f monotonic? If you think it is, argue why it is, and also give the least fixpoint of f. If not, precisely argue why it is not using the definition of monotonicity.