IIT CS536: Science of Programming

Homework 7: Separation Logic, Nondeterminism, and Parallelism

Prof. Stefan Muller

Out: Monday, Nov. 20
Due: Thursday, Nov. 30, 11:59pm CST

This assignment contains 8 written task(s) for a total of 66 points.

Logistics

Submission Instructions

Please read and follow these instructions carefully.

- Submit your homework on Blackboard under the correct assignment by the deadline (or the extended deadline if taking late days).
- You may submit multiple times, but we will only look at your last submission. Make sure your last submission contains all necessary files.
- Email the instructor and TAs ASAP if
  - You submit before the deadline but then decide to take (more) late days.
  - You accidentally resubmit after the deadline, but did not intend to take late days.

  Otherwise, you do not need to let us know if you're using late days; we'll count them based on the date of your last submission.
- Submit your written answers in a single PDF or Word document. Typed answers are preferred (You can use any program as long as you can export a .pdf, .doc or .docx; LaTeX is especially good for typesetting logic and math, and well worth the time to learn it), but *legible* handwritten and scanned answers are acceptable as well.
- Your Blackboard submission should contain only the file with your written answers. Do not compress or put any files in folders.

Collaboration and Academic Honesty

Read the policy on the website and be sure you understand it.

1 Linked list and separation logic

Task 1.1 (Written, 10 points).

In class, we wrote a program that appends a list of length three to a list of length m. Now, write a program that operates on a list L with a length of $m + 3$ and starting head variable *head*. This program should create two lists L_1 and L_2, where L_1 contains the first three elements of L with the head variable $head_1$ and L_2 contains the remaining elements of the list L with the head variable $head_2$.

Task 1.2 (Written, 12 points).

Write a precondition and a postcondition for your program in Task 1.1 that specifies its intended behavior. Using a proof outline, prove that your program adheres to the specification. Use the $list(L, i, n)$ predicate in your specifications and the separation logic rules in the proof outline.

Write a full proof outline. You do not, however, need to separately justify the proof obligations (but they must be correct).

2 Resource logic

Task 2.1 (Written, 10 points).

For each resource logic formula, draw *one heap* (in the style of the diagrams of Figures 1, 2, and 3 of the Lecture 21 notes) that satisfies it.

a) $x \mapsto x$

b) $x \mapsto 2 * y \mapsto 2$

c) $x \mapsto x + 1, x$

d) $w \mapsto 2 * (x \mapsto y \wedge y = w)$

e) $(\exists x.y \mapsto x) \wedge y \mapsto 2$

Task 2.2 (Written, 6 points).

For each resource logic formula, draw *two heaps* that satisfy it.

a) $x \hookrightarrow x$

b) $x \hookrightarrow 2 \wedge y \hookrightarrow 2$

c) $x \mapsto -$

Task 2.3 (Written, 8 points).

For each implication, either prove it using the axioms and rules of resource logic or provide a counterexample. Specify which rule you are using by referring to its line number in Section 2 of the separation logic lecture.

a) $(x \mapsto 2 * y \mapsto 2) * z \mapsto 2 \Rightarrow (z \mapsto 2 * y \mapsto 2) * x \mapsto 2$

b) $(x \hookrightarrow 3 \wedge y \hookrightarrow 3) \Rightarrow x = y$

c) $\mathbf{emp} * ((\exists x.y \mapsto x) * w \mapsto 2) \Rightarrow \exists x.(y \mapsto x * w \mapsto 2)$

d) $(\exists x.y \mapsto x) * x \mapsto 2 \Rightarrow \exists x.(y \mapsto x * x \mapsto 2)$

3 Nondeterminism

Task 3.1 (Written, 10 points).

a) Using the small step semantics write one (nondeterministic) execution of the program

$$S_1 \triangleq \mathsf{while}\ \{x \geq 0 \to y := x/y \,\square\, x \leq 0 \to y := y * x\}$$

on the state $\sigma \triangleq \{x = 0, y = 1\}$. If the execution does not terminate, write at least three iterations of the loop.

b) What is $M(S, \sigma)$?

4 Parallel programs

Task 4.1 (Written, 10 points).

Consider the program

$$S_2 \triangleq [\ x := y; y := y + \overline{1} \parallel y := y + \overline{3}\ ]$$

and the initial state $\sigma \triangleq \{x = 3, y = 2\}$ and a heap h. Draw the evaluation graph for this program describing the possible behaviors of S_2.

5 One more wrap-up question

Task 5.1 (Written, 0 points).

How long (approximately) did you spend on this homework, in total hours of actual working time? Your honest feedback will help us with future homeworks.