Girish Rajani (A20503736)

CS 536: Science of Programming

Homework 7: Separation Logic, Nondeterminism, and Parallelism

1 Linked list and separation logic

Task 1.1 (Written, 10 points)

$$
\begin{aligned}
S ::= \ & head_1 := head; \\
& x_0 := !(head_1 + 1); \\
& x_1 := !(x_0 + 1); \\
& head_2 := !(x_1 + 1); \\
& !(x_1 + 1) := nil
\end{aligned}
$$

Task 1.2 (Written, 12 points)

$\{List(L, head, m+3)\}$

$\{List(L_1; L_2, head, 3+m)\}$

$\{List(a_1; a_2; a_3; L_2, head, 3+m)\}$

$\Rightarrow \{head \mapsto a_1, i_1 * i_1 \mapsto a_2, i_2 * i_2 \mapsto a_3, i_3 * List(L_2, i_3, m)\}$

$head_1 := head;$ $\{head_1 \mapsto a_1, i_1 * i_1 \mapsto a_2, i_2 * i_2 \mapsto a_3, i_3 * List(L_2, i_3, m)\}$

$x_0 := !(head_1 + 1);$ $\{x_0 = i_1 \wedge head_1 \mapsto a_1, x_0 * i_1 \mapsto a_2, i_2 * i_2 \mapsto a_3, i_3 * List(L_2, i_3, m)\}$

$\Rightarrow \{head_1 \mapsto a_1, x_0 * x_0 \mapsto a_2, i_2 * i_2 \mapsto a_3, i_3 * List(L_2, i_3, m)\}$

$x_1 := !(x_0 + 1);$ $\{x_1 = i_2 \wedge head_1 \mapsto a_1, x_0 * x_0 \mapsto a_2, x_1 * i_2 \mapsto a_3, i_3 * List(L_2, i_3, m)\}$

$\Rightarrow \{head_1 \mapsto a_1, x_0 * x_0 \mapsto a_2, x_1 * x_1 \mapsto a_3, i_3 * List(L_2, i_3, m)\}$

$head_2 := !(x_1 + 1);$ $\{head_2 = i_3 \wedge head_1 \mapsto a_1, x_0 * x_0 \mapsto a_2, x_1 * x_1 \mapsto a_3, i_3 * List(L_2, i_3, m)\}$

$\Rightarrow \{head_1 \mapsto a_1, x_0 * x_0 \mapsto a_2, x_1 * x_1 \mapsto a_3, head_2 * List(L_2, head_2, m)\}$

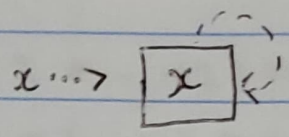
$!(x_1 + 1) := nil$ $\{head_1 \mapsto a_1, x_0 * x_0 \mapsto a_2, x_1 * x_1 \mapsto a_3, nil * List(L_2, head_2, m)\}$

$\Rightarrow \{List(a_1; a_2; a_3, head_1, 3) * List(L_2, head_2, m)\}$

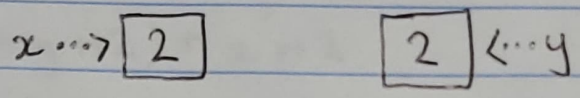
2 Resource Logic

Task 2.1 (Written, 10 points)

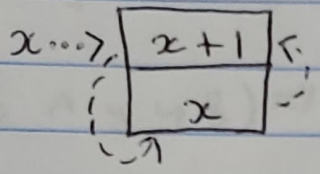
a)



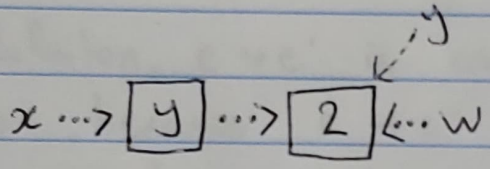
b)



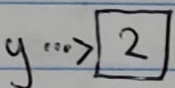
c)



d)



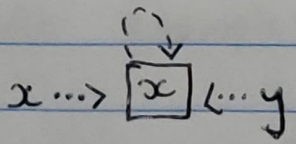
e)

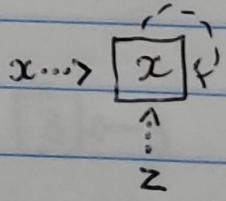


where $x = 2$

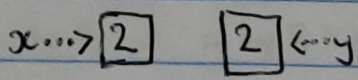
Task 2.2 (Written, 6 points)

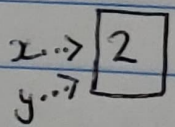
a)



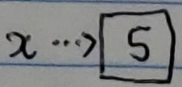


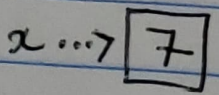
b)





c)





Task 2.3 (Written, 8 points)

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

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

$\Leftrightarrow$ $x \mapsto 2 * (y \mapsto 2 * z \mapsto 2)$ Rule 2

$\Leftrightarrow$ $x \mapsto 2 * (z \mapsto 2 * y \mapsto 2)$ Rule 1

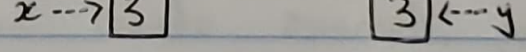
$\Leftrightarrow$ $(z \mapsto 2 * y \mapsto 2) * x \mapsto 2$ Rule 1

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

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

By definition, $e \hookrightarrow e'$ is considered imprecise assertion because $e \mapsto e'$ just needs to appear somewhere in the heap. Therefore we cannot say for sure that $x = y$ since $x \hookrightarrow 3$ may appear in one place and $y \hookrightarrow 3$ may appear somewhere else.

Counter example:



Here we have $x \hookrightarrow 3 \wedge y \hookrightarrow 3$ but $x \neq y$.

Hence $(x \hookrightarrow 3 \wedge y \hookrightarrow 3) \not\Rightarrow x = y$

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

$emp * ((\exists x.\ y \mapsto x) * w \mapsto 2)$

$\Leftrightarrow$ $((\exists x.\ y \mapsto x) * w \mapsto 2) * emp$ Rule 1

$\Leftrightarrow$ $((\exists x.\ y \mapsto x) * w \mapsto 2)$ Rule 3

$\Leftrightarrow$ $\exists x.(y \mapsto x * w \mapsto 2)$ Rule 6

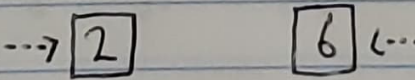
Hence $emp * ((\exists x.\ y \mapsto x) * w \mapsto 2) \Rightarrow \exists x.(y \mapsto x * w \mapsto 2)$

d) $(\exists x.\ y \mapsto x) * x \mapsto 2 \not\Rightarrow \exists x.(y \mapsto x * x \mapsto 2)$

As per rule 6, if x is not free in P_2, then only can we apply rule 6.

However, in this example, x is free since it is not bound to the x in $\exists x.$

Counter example :



where $x = 6$

In the above counter example, we have $(\exists x.\ y \mapsto x) * x \mapsto 2$ but not $\exists x.(y \mapsto x * x \mapsto 2)$.

Hence $(\exists x.\ y \mapsto x) * x \mapsto 2 \not\Rightarrow \exists x.(y \mapsto x * x \mapsto 2)$

3 Nondeterminism

Task 3.1 (Written, 10 points)

a) $S_1 \triangleq$ while $\{ x \geq 0 \to y := x/y \;\square\; x \leq 0 \to y := y * x \}$

$\sigma \triangleq \{x=0, y=1\}$

$\langle S_1, \{x=0, y=1\} \rangle$
$\to \langle y := x/y ; S_1, \{x=0, y=1\} \rangle$
$\to^2 \langle S_1, \{x=0, y=0\} \rangle$
$\to \langle y := y * x ; S_1, \{x=0, y=0\} \rangle$
$\to^2 \langle S_1, \{x=0, y=0\} \rangle$
$\to \langle y := y * x ; S_1, \{x=0, y=0\} \rangle$
$\to^2 \langle S_1, \{x=0, y=0\} \rangle$
...

b) $\Sigma_0 = \{\{x=0, y=1\}\}$

$\Sigma_1 = m(y := x/y, \{x=0, y=1\}) \cup m(y := y*x, \{x=0, y=1\})$

$= \{\{x=0, y=0\}\} \cup \{\{x=0, y=0\}\}$

$= \{\{x=0, y=0\}\}$

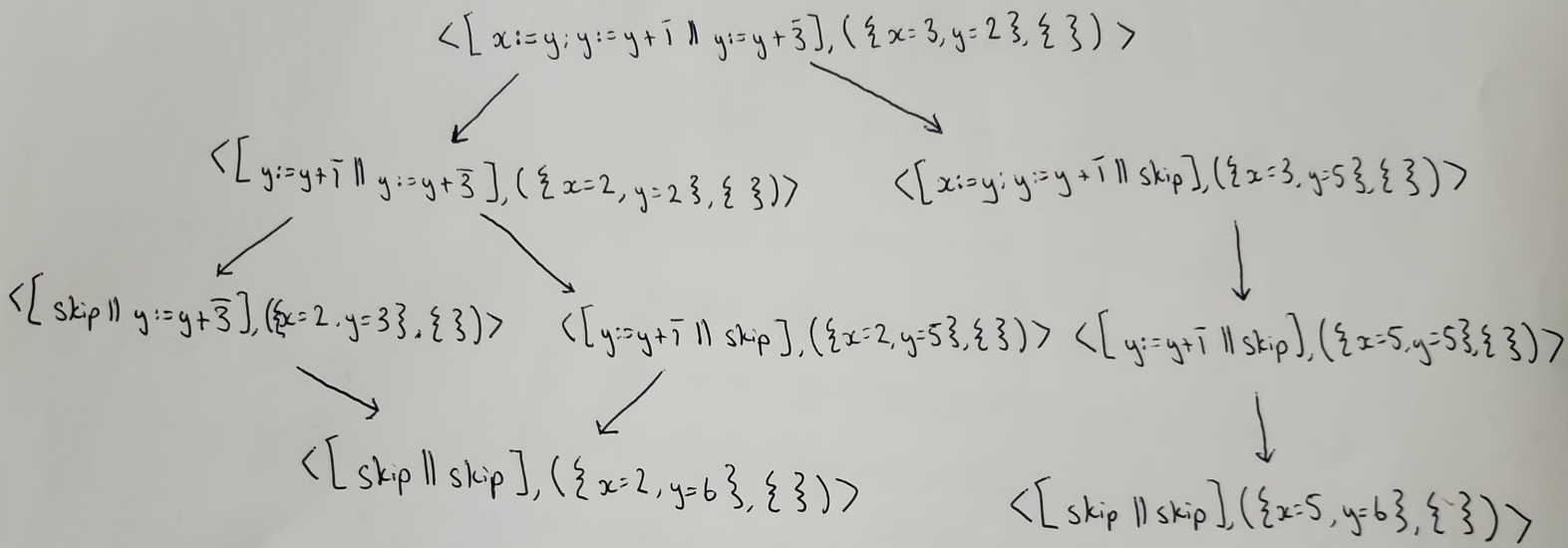
$\Sigma_2 = m(y := x/y, \{x=0, y=0\}) \cup m(y := y*x, \{x=0, y=0\})$

$= \{\bot\} \cup \{\{x=0, y=0\}\}$

$= \{\bot, \{x=0, y=0\}\}$

4 Parallel programs

Task 4.1 (Written, 10 points)



$$m(S_2, (\{x = 3, y = 2\}, \{\})) = \{ (\{x = 2, y = 6\}, \{\}), (\{x = 5, y = 6\}, \{\}) \}$$

5 One more wrap-up question

Task 5.1 (Written, 0 points).

15 hours