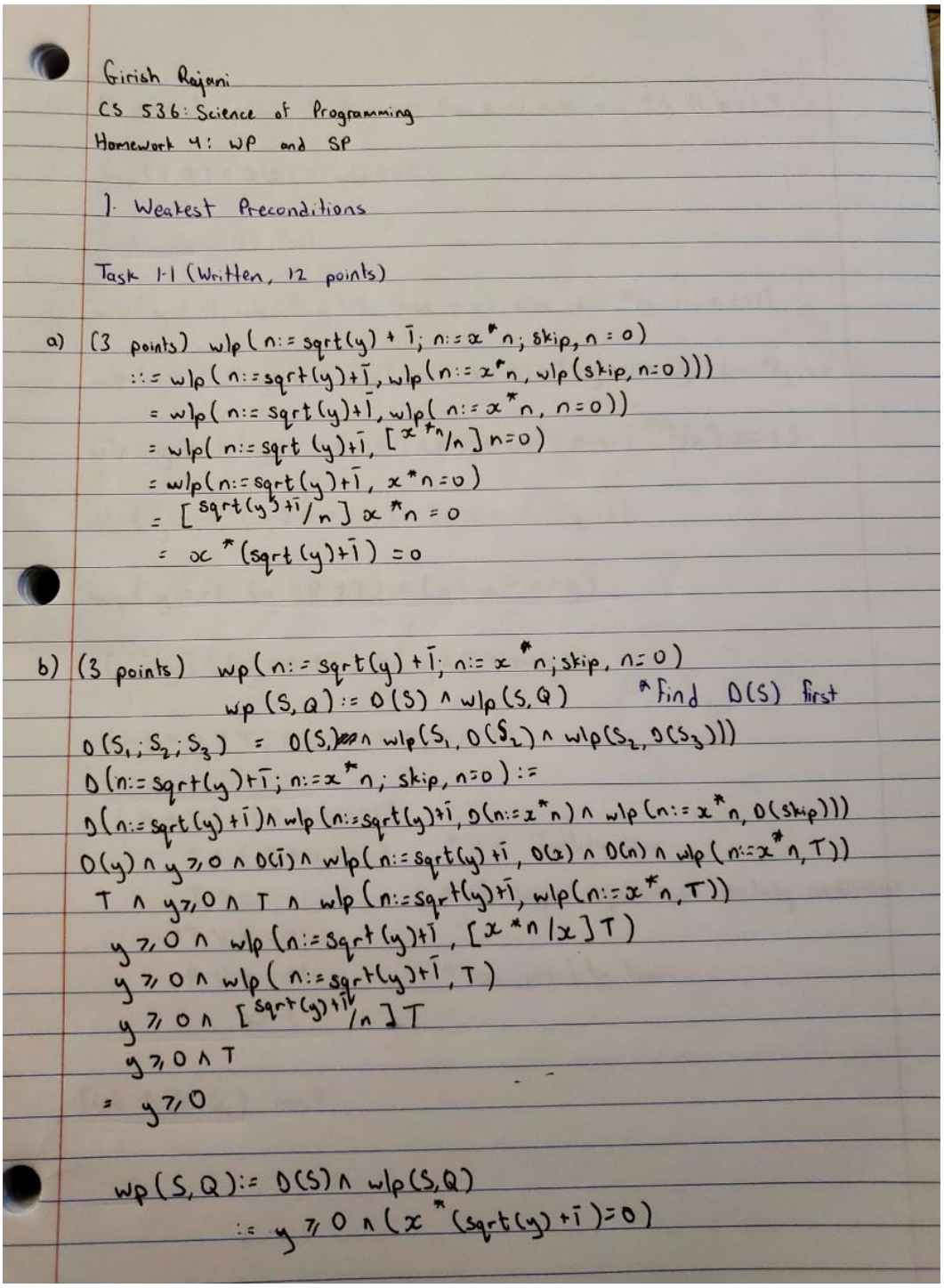
CS 536 – Science of Programming

Homework 4 – WP and SP

Girish Rajani

A20503736



Girish Rajani
CS 536: Science of Programming
Homework 4: WP and SP

1. Weakest Preconditions

Task 1.1 (Written, 12 points)

a) (3 points) $wlp(n := sqrt(y) + \bar{1};\ n := x * n;\ skip,\ n = 0)$

$:= wlp(n := sqrt(y)+\bar{1}, wlp(n := x*n, wlp(skip, n=0)))$

$= wlp(n := sqrt(y)+\bar{1}, wlp(n := x*n, n=0))$

$= wlp(n := sqrt(y)+\bar{1}, [x*n/n]\, n=0)$

$= wlp(n := sqrt(y)+\bar{1}, x*n=0)$

$= [sqrt(y)+\bar{1}/n]\, x*n = 0$

$= x * (sqrt(y)+\bar{1}) = 0$

b) (3 points) $wp(n := sqrt(y) + \bar{1};\ n := x * n;\ skip,\ n = 0)$

$wp(S, Q) := D(S) \wedge wlp(S, Q)$ *Find D(S) first

$D(S_1; S_2; S_3) = D(S_1) \wedge wlp(S_1, D(S_2) \wedge wlp(S_2, D(S_3)))$

$D(n := sqrt(y)+\bar{1};\ n := x*n;\ skip,\ n=0) :=$

$D(n := sqrt(y)+\bar{1}) \wedge wlp(n := sqrt(y)+\bar{1}, D(n := x*n) \wedge wlp(n := x*n, D(skip)))$

$D(y) \wedge y \geq 0 \wedge D(\bar{1}) \wedge wlp(n := sqrt(y)+\bar{1}, D(x) \wedge D(n) \wedge wlp(n := x*n, T))$

$T \wedge y \geq 0 \wedge T \wedge wlp(n := sqrt(y)+\bar{1}, wlp(n := x*n, T))$

$y \geq 0 \wedge wlp(n := sqrt(y)+\bar{1}, [x*n/x]\, T)$

$y \geq 0 \wedge wlp(n := sqrt(y)+\bar{1}, T)$

$y \geq 0 \wedge [sqrt(y)+\bar{1}/n]\, T$

$y \geq 0 \wedge T$

$= y \geq 0$

$wp(S, Q) := D(S) \wedge wlp(S, Q)$

$:= y \geq 0 \wedge (x * (sqrt(y)+\bar{1}) = 0)$

c) (6 points) $wp(y := -1;$ if $y > 0$ then $z := 1$ else $z := x/y$ fi, $z = 1)$

$wp(S, Q) := D(S) \wedge wlp(S, Q)$

find $wlp(S, Q)$ first:

$wlp(y := -1, wlp($if $y > 0$ then $z := 1$ else $z := x/y$ fi, $z = 1))$

$wlp(y := -1, (y > 0 \rightarrow wlp(z := 1, z = 1)) \wedge (\neg y > 0 \rightarrow wlp(z := x/y, z = 1))$

$wlp(y := -1, (y > 0 \rightarrow [1/z]\, z = 1) \wedge (y \leq 0 \rightarrow [x/y/z]\, z = 1)$

$wlp(y := -1, (y > 0 \rightarrow 1 = 1) \wedge (y \leq 0 \rightarrow x/y = 1)$

$wlp(y := -1, (y > 0 \rightarrow T) \wedge (y \leq 0 \rightarrow x = y)$

$[-1/y]((y > 0 \rightarrow T) \wedge (y \leq 0 \rightarrow x = y))$

$(-1 > 0 \rightarrow T) \wedge (-1 \leq 0 \rightarrow x = -1)$

$(F \rightarrow T) \wedge (T \rightarrow x = -1)$

$T \wedge (T \rightarrow x = -1)$ * use identity law

$T \rightarrow x = -1$ * use logical equivalence involving conditional

$\neg T \vee x = -1$

$F \vee x = -1$ * use identity law

$x = -1$

Find $D(S_1; S_2)$ next:

$D(S_1; S_2)$:

$D(y := -1;$ if $y > 0$ then $z := \bar{1}$ else $z := x/y$ fi$)$

$D(y := -1) \wedge wlp(y := -1, D($if $y > 0$ then $z := \bar{1}$ else $z := x/y$ fi$))$

$D(y := -1) \wedge wlp(y := -1, D(y > 0) \wedge (y > 0 \to D(z := \bar{1})) \wedge (y \leq 0 \to D(z := x/y)))$

$D(-1) \wedge wlp(y := -1, D(y) \wedge D(0) \wedge (y > 0 \to D(1)) \wedge (y \leq 0 \to D(x/y)))$

$T \wedge wlp(y := -1, T \wedge T \wedge (y > 0 \to T) \wedge (y \leq 0 \to D(x) \wedge D(y) \wedge y \neq 0))$

$T \wedge wlp(y := -1, T \wedge T \wedge (y > 0 \to T) \wedge (y \leq 0 \to T \wedge T \wedge y \neq 0))$

$wlp(y := -1, (y > 0 \to T) \wedge (y \leq 0 \to y \neq 0))$

$[-1/y]((y > 0 \to T) \wedge (y \leq 0 \to y \neq 0))$

$(-1 > 0 \to T) \wedge (-1 \leq 0 \to -1 \neq 0)$

$(F \to T) \wedge (T \to T)$

$T \wedge T$

$= T$

$\therefore wp(S, Q) = D(S) \wedge wlp(S, Q)$

$:= T \wedge x = -1$

$:= x = -1$

Task 1.2 (Written, 5 points)

$SP\text{-}state(S,P) = \{\sigma' \in states \mid \sigma' \models sp(S,P)\}$
$= \{\sigma \in states \mid \exists_\sigma.\ \sigma \models P \wedge M(S,\sigma) = \sigma'\}$

$wlp(S, sp(S,P)) = P$ can be defined as

1. For any state $\sigma \models P$ either
   a) $M(S,\sigma) = \sigma'$ and $\sigma' \models sp(S,P)$, or
   b) $M(S,\sigma) = \perp$, or
   c) $M(S,\sigma) = \{\}$

2. For any state $\sigma \not\models P$, we have $M(S,\sigma) = \sigma'$ and $\sigma' \not\models sp(S,P)$.

$sp(S,P)$ only holds in those final states for which there exists an execution of S that starts from an initial state satisfying P.

- By definition, $wlp(S,Q)$ gives weakest P under which S either doesn't terminate or satisfies Q.
- Similarly, by definition, $sp(S,P)$ gives strongest Q such that for any state satisfying P, Q is satisfied by σ' after S executes.
- Therefore, ~~sing~~ since $sp(S,P)$ satisfies P, from the definition above, we can also say that $wlp(S, sp(S,P))$ also satisfies P given any state.

Let's check this using an example:

$\{y > 0\}\ x := y + 2\ \{Q\}$

* $\{y > 0\}\ x := y + 2\ \{Q\}$

$sp(S, P)$

$sp(x := y+2, y>0) :=$

$\exists x_0 . ([^{x_0}/_x]\, y>0 \wedge x = [^{x_0}/_x]\, y+2)$

$= y>0 \wedge x = y+2$

$wlp(S, sp(S,P))$

$wlp(x := y+2, y>0 \wedge x = y+2)$

$[^{y+2}/_x]\, y>0 \wedge x = y+2$

$= y>0 \wedge y+2 = y+2$

$= y>0 \wedge T$

* $= y>0$

$wlp(S, sp(S,P)) \Rightarrow P$

$y>0 \Rightarrow y>0$

2 Strongest Postconditions

Task 2.1 (written, 6 points)

a) (3 points) $sp(x := -1;$ if $y > 0$ then $x := \bar{1}$ else $z := x/y$ fi, $y \geq 0) :=$

$sp($if $y>0$ then $x:=\bar{1}$ else $z:=x/y$ fi, $sp(x:=-1, y\geq 0))$

$sp($if $y>0$ then $x:=\bar{1}$ else $z:=x/y$ fi, $\exists x_0 . [x_0/x](y\geq 0) \wedge x = [x_0/x](-1))$

$sp($if $y>0$ then $x:=\bar{1}$ else $z:=x/y$ fi, $y\geq 0 \wedge x = -1)$

$sp(x:=\bar{1}, y\geq 0 \wedge x = -1 \wedge y > 0) \vee sp(z := x/y, y\geq 0 \wedge x = -1 \wedge \neg(y>0))$

$\exists x_0 .([x_0/x](y\geq 0 \wedge x = -1 \wedge y>0) \wedge x = [x_0/x]1) \vee$
$\exists z_0 .([z_0/z](y\geq 0 \wedge x = -1 \wedge \neg(y>0)) \wedge z = [z_0/z]\, x/y)$

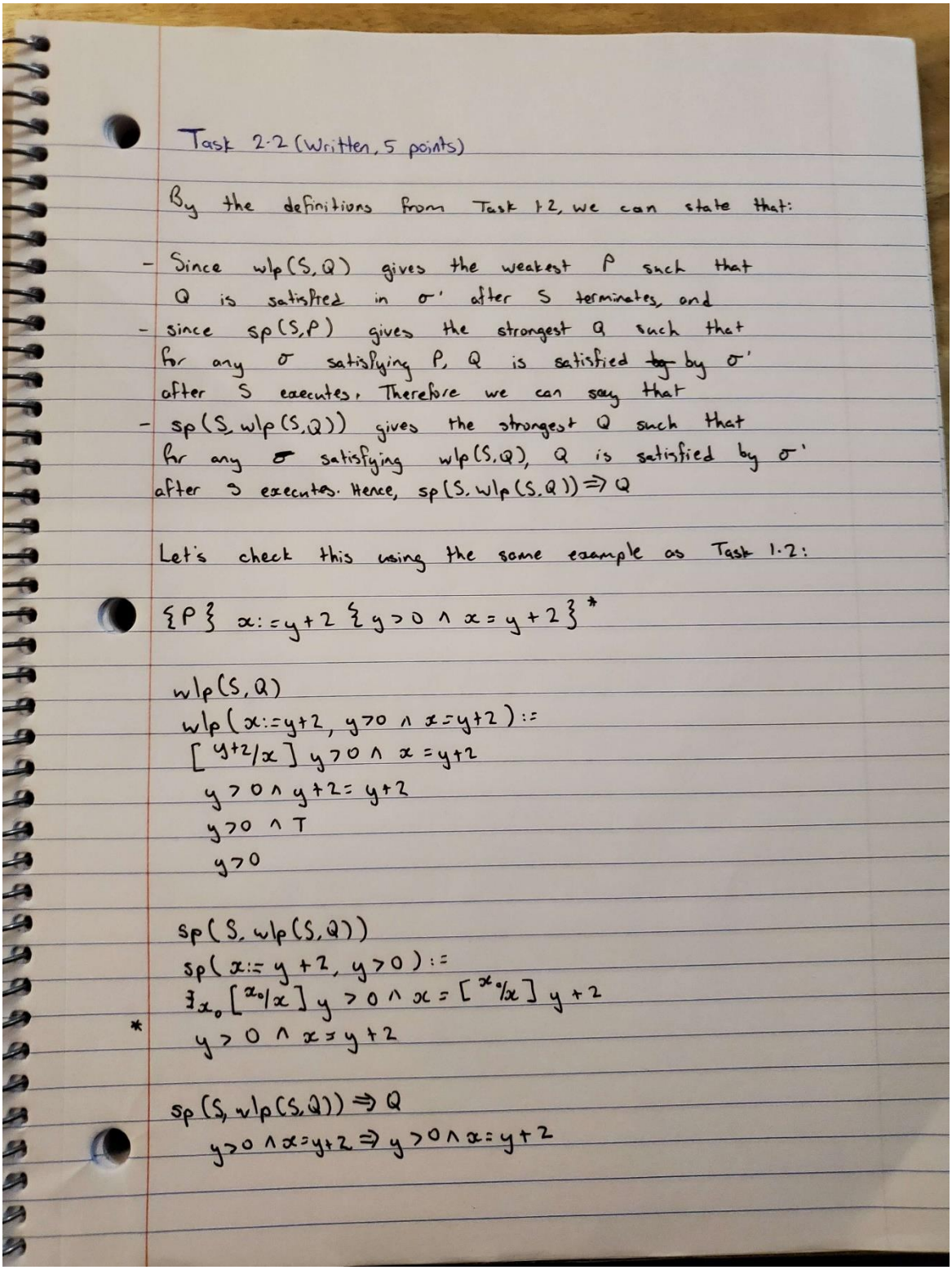
$= \exists x_0 .((y\geq 0 \wedge x_0 = -1 \wedge y = 0) \wedge x = 1) \vee \exists z_0 .((y\geq 0 \wedge x = -1 \wedge \neg(y>0)) \wedge z = x/y)$

b) (3 points) $sp($if $y = 0$ then $x := x * \bar{5}$ else skip fi, $x = 10) :=$

$sp(x := x * \bar{5}, x = 10 \wedge y = 0) \vee sp($skip, $x = 10 \wedge \neg(y=0))$

$\exists x_0 .([x_0/x](x = 10 \wedge y = 0) \wedge x = [x_0/x]\, x * \bar{5}) \vee (x = 10 \wedge \neg(y=0))$

$= \exists x_0 .((x_0 = 10 \wedge y = 0) \wedge x = x_0 * \bar{5}) \vee (x = 10 \wedge \neg(y=0))$



Task 3.1

8 hours