15-812 Programming Language Semantics ________ Spring 2018

Homework 2: Substituting program reasoning ________ Feb 20

Name: ________

Andrew ID: ________

1 The Sound of Axioms and Proof Rules (20 points)

Axioms and proof rules are more useful if they are actually also sound. Recall that an axiom is sound iff all its instances are valid. A proof rule is sound iff the validity of each of its premises implies the validity of the conclusion. Your job in this task is to find out which suggested axiom or proof rule is sound and which one is unsound. Clearly mark which case it is. If it is sound, also give a semantic soundness proof or prove it's derived. If it is unsound, also give a counterexample, so a formula that can be proved with the unsound axiom/proof rule and about which you explain why it is not valid.

Here's an example of an axiom:

$$\text{R1} \quad \theta \geq 0 \leftrightarrow -\theta < 0$$

ⓤ R1 is unsound since the following instance is not valid (left side is true but right false):

$$\text{R1}\,\frac{}{0 \geq 0 \leftrightarrow -0 < 0}$$

And here's an example of a rule:

$$\text{R2} \quad \frac{\Gamma, \phi, \psi \vdash \Delta}{\Gamma, \phi \lor \psi \vdash \Delta}$$

ⓤ R2 is unsound as shown by the following counterexample with valid premises (integer arithmetic) but invalid conclusion:

$$\text{R2}\,\frac{x \geq 0, x \leq 0 \vdash x = 0}{x \geq 0 \lor x \leq 0 \vdash x = 0}$$

5 **Task 1**

$$\text{R3} \quad \frac{\Gamma, \phi \vdash \Delta \quad \Gamma \vdash \neg\psi, \Delta}{\Gamma, \phi \lor \psi \vdash \Delta}$$

5 **Task 2**

$$\text{R4} \quad \frac{\Gamma \vdash J, \Delta \quad J, Q \vdash [\alpha]J \quad J, \neg Q \vdash P, \boldsymbol{\Delta}}{\Gamma \vdash [\mathsf{while}(Q)\,\alpha]P, \Delta}$$

5 **Task 3**

$$\text{R5} \quad [\alpha;\beta]\phi \leftrightarrow [\beta;\alpha]\phi$$

5 **Task 4**

$$\text{R6} \quad \langle\alpha;\beta\rangle\phi \leftrightarrow \langle\alpha\rangle\neg[\beta]\neg\phi$$

2 Uniform Substitutions (20 points)

5 **Task 1** Add the case of $\mathsf{while}(Q)\,\alpha$ loops to the uniform substitution definition.

5 **Task 2** Prove that your added case of the uniform substitution mechanism is sound.

Which uniform substitution applied to which axiom proves the following formulas? Or justify why no such uniform substitution exists.

1 **Task 3** $[x := 7 + y]y < x \leftrightarrow y < 7 + y$

3 **Task 4** $[x := x + 1][\mathsf{while}(x > y)\, y := y + 1]x \geq y \leftrightarrow [\mathsf{while}(x + 1 > y)\, y := y + 1]x + 1 \geq y$

3 **Task 5** $[x := x + 1][\mathsf{while}(x > y)\, x := x + 1]x \geq y \leftrightarrow [\mathsf{while}(x + 1 > y)\, x := x + 1 + 1]x + 1 \geq y$

3 **Task 6** $[\mathsf{while}(x > y)\, x := x + 1]x \geq y \leftrightarrow [\mathsf{if}(x > y)\, (x := x + 1; \mathsf{while}(x > y)\, x := x + 1)]x \geq y$

3 Totally Correct Diamonds (10 points)

Consider a fixed interpretation in which gcd is interpreted to be the standard greatest common divisor function. What exactly do you need to prove to show that the following formula is valid?

$$0 < a \land 0 < b \rightarrow \langle x := a; y := b; \mathsf{while}(x \neq y)\, \{\mathsf{if}(x > y)\, x := x - y \;\mathsf{else}\; y := y - x\rangle(x = gcd(a, b))$$

List the resulting proof branches and explain where they come from. You do not need to conduct an entire sequent calculus proof but can settle for justifying informally but precisely why each of the resulting proof branches will close.