Assignment 5: Uniform Substitution and Other Fun Topics
15-424/15-624/15-824 Logical Foundations of Cyber-Physical Systems
TA: Katherine Cordwell (kcordwel@cs.cmu.edu)

Due Date: Thursday, November 14th, 11:59PM (no late days), worth 60 points
Edited 11/12 to add a missing parentheses in 3(d).

1. **Sound axioms v.s. sound proof rules.** You should have lots of experience proving *axioms* sound by now: an axiom is sound iff all of its instances are valid.

   In contrast, we say that a *proof rule*:

$$\frac{\Gamma_1 \vdash \Delta_1 \qquad \dots \qquad \Gamma_n \vdash \Delta_n}{\Gamma \vdash \Delta}$$

   is sound iff for all instances of the rule, validity of all of the premises $\Gamma_i \vdash \Delta_i$ (for $i = 1, \dots, n$) implies validity of its conclusion $\Gamma \vdash \Delta$.

   The two notions look similar and can be easily confused. For each of the following pairs of similar-looking axioms (on the left) and proof rules (on the right), state whether the axiom and/or proof rule is sound and briefly explain your answer.

   (a) Gödel Generalization.

$$P \to [\alpha]P \qquad\qquad \frac{\vdash P}{\Gamma \vdash [\alpha]P, \Delta}$$

   (b) Hoare Sequencing.

$$[\alpha]E \wedge (E \to [\beta]B) \to [\alpha;\beta]B \qquad\qquad \frac{\Gamma \vdash [\alpha]E \qquad E \vdash [\beta]B}{\Gamma \vdash [\alpha;\beta]B, \Delta}$$

   (c) Differential Weakening.

$$(\forall x\, (Q \to P)) \to [\{x' = f(x) \,\&\, Q\}]P \qquad\qquad \frac{\Gamma, Q \vdash P, \Delta}{\Gamma \vdash [\{x' = f(x) \,\&\, Q\}]P, \Delta}$$

2. **Convergence.** The following formula is valid:

$$x \geq 1 \wedge v > 0 \to \langle (x := x - 1; \{x' = v\})^* \rangle x > 10$$

   One way of proving this is to use the *loop convergence* rule:

$$\text{(con)} \quad \frac{\Gamma \vdash \exists \tau\, p(\tau), \Delta \qquad \vdash \forall \tau{>}0\, (p(\tau) \to \langle\alpha\rangle p(\tau - 1)) \qquad \exists \tau{\leq}0\, p(\tau) \vdash Q}{\Gamma \vdash \langle \alpha^* \rangle Q, \Delta} \quad (\tau \notin \alpha)$$

State a *loop variant* $p(v)$ that can be used to prove the formula, and briefly explain why all 3 resulting premises of the rule are valid.

Hint: Convergence properties have been covered in less detail in the lectures. You may wish to read LFCPS Chapter 17.4 for a more in depth discussion. You may also find it useful to think carefully about the ODE and to check your answer in KeYmaera X.

3. **FV, BV, MBV.** For each of the following formulas and hybrid programs, identify the free variables, bound variables, and must-bound variables (when they exist). Show your work.

   (a) $a := b; b := c + a$

   (b) $[w := 5y; ?(k = 2); \{x' = 2k + 5 \ \&\ k \geq z\}]w = y + 2x$

   (c) $(\{x' = 2y + k\} \cup x := 2w + 5z)^*; (z := x + y \cup z := x)$

   (d) $((x := z; ?(z = 4) \cup x := x + z; y := x + 2); y := x + y; \{x' = 1, y' = 1\})^*$

4. **Applying Uniform Substitution.** Give the result of applying uniform substitution US with substitution $\sigma = \{c() \mapsto x \cdot y^2 + 1, p(\cdot) \mapsto (y + \cdot \geq z)\}$ on the following formulas, or explain why and how US clashes. Show your work.

   (a) $[u := c()]p(u) \leftrightarrow p(c())$

   (b) $[x := c()]p(x) \leftrightarrow p(c())$

   (c) $[z := c()]\forall z(z = c() \rightarrow p(z))$

5. **Identifying Uniform Substitution.** For each of the following formulas, identify a corresponding dL axiom from LFCPS Figure 18.2 that matches the shape of the formula. If possible, also give a uniform substitution σ that can be used to prove the formula. If no such substitution exists, briefly explain why a clash would occur for your chosen dL axiom.

   (a) $[x := y^2][y := y^2]x + y \geq 0 \leftrightarrow [y := y^2]y^2 + y \geq 0$

   (b) $[x := z^2][y := x + y]x + y \geq 0 \leftrightarrow [y := z^2 + y]z^2 + y \geq 0$

   (c) $[x := 1][\{x' = x\}]x > 0 \leftrightarrow [\{x' = 1\}]x > 0$

6. **Reassignment fallacy.** The following proof contains an error. Explain what the error is and how to fix it.

Proposition 1 *The following axiom is sound:*

$$\text{(R2)} \quad [x := e]P \leftrightarrow [x := e][x := e]P$$

Proof. To prove soundness show that the set of all states ω in which the left-hand side is true is equal to the set of all states in which the right-hand side is.

$$\begin{aligned}
[\![[x := e]P]\!] &= \{\omega \ : \ \nu \in [\![P]\!] \text{ for the state } \nu \text{ defined as } \omega_x^e\} \\
[\![[x := e][x := e]P]\!] &= \{\omega \ : \ \nu \in [\![[x := e]P]\!] \text{ for the state } \nu \text{ defined as } \omega_x^e\} \\
&= \{\omega \ : \ \nu \in [\![P]\!] \text{ for the state } \nu \text{ defined as } \omega_{xx}^{ee} \text{ which is } \omega_x^e\}
\end{aligned}$$

□

7. **Taylor series, bonus edition (not required—5 points extra credit).** On the last assignment you proved a lower bound for e^t, whose Taylor series is given by:

$$e^t = 1 + t + \frac{t^2}{2!} + \frac{t^3}{3!} + \dots$$

.

In fact, we can make the lower bound on e^t arbitrarily tight by truncating its Taylor series at the t^k term for higher values of k:

$$\sum_{i=0}^{k} \frac{t^i}{i!} \leq e^t$$

For fun and five points of extra credit, give an expression involving powers of t up to t^k that is an **upper bound** on e^t on $0 \leq t \leq 1$ and that can be made arbitrarily tight by increasing k. The expression should also be invariant for the ODE, i.e., the following formula should be valid for your expansion for any $k \geq 2$, where $\theta(k)$ is your expression involving the first k powers of t:

$$x \leq \theta(k) \rightarrow [\{x' = x, t' = 1 \,\&\, 0 \leq t \leq 1\}]x \leq \theta(k)$$

Hint: There are multiple possible answers. You may wish to check your answer (for some values of k) in KeYmaera X using the `dbx` tactic discussed in recitation.