LFCPS Exercise Class 7
Comprehensive CPS Correctness

Uniform substitution

Exercise 1. *Determine the free variables in the following formulas:*

1. $[x := 1 \cup y := 2]\, x \geq 1$
2. $[z := y; \{x := 1 \cup y := 2\}]\, x \geq z$

Determine the free variables in the following substitutions:

1. $\sigma = \{a \mapsto x' := 1,\ p(\cdot) \mapsto \cdot \geq 1\}$
2. $\sigma = \{q \mapsto \forall x(x \leq 1),\ p(\cdot) \mapsto \cdot + y \geq 3, a \mapsto \{?z = 0\}\}$

Exercise 2. *Find a uniform substitution σ that causes a clash in the formula:*

$$p \to [a]p.$$

Explain why the clash occurs.

Exercise 3. *A uniform substitution σ is called U-admissible for a formula φ if:*

$$U \cap \mathrm{FV}(\sigma|_{\Sigma(\varphi)}) = \emptyset.$$

Consider the following uniform substitution in the context of the bouncing ball model:

$$\sigma = \left\{a \mapsto \{x' = v, v' = -g \,\&\, x \geq 0\},\quad b \mapsto \{?x = 0; v := -cv\},\quad p(\bar{x}) \mapsto 2gx \leq 2gH - v^2\right\}.$$

Recall the slogan: "If you bind a free variable, you go to logic jail." Apply the substitution σ to the following formulas and determine whether any variable clashes occur:

1. $[a \cup b]p(\bar{x}) \leftrightarrow [a]p(\bar{x}) \wedge [b]p(\bar{x})$
2. $[a; b]p(\bar{x}) \leftrightarrow [a][b]p(\bar{x})$

Does the slogan accurately capture the formal definition of clashes in uniform substitutions? Why or why not?

Exercise 4. *Prove the following statement using uniform substitutions:*

$$(x = x_0 \wedge y = y_0) \to [x := x + y][y := x - y][x := x - y](x = y_0 \wedge y = x_0).$$

ModelPlex

Exercise 5. *Derive a runtime monitor for the hybrid program:*

$$\{u := *;\ ?(0 < u \leq 1);\ \{x' = v,\ v' = u,\ t' = 1\}\}.$$

How can you formally prove the correctness of this monitor?

Exercise 6. *Consider the following model of a water tank system:*

$$f := *;\ ?(-1 \leq f \leq (m - x)/\epsilon);\ t := 0;\ \{x' = f,\ t' = 1 \,\&\, x \geq 0 \wedge t \leq \epsilon\},$$

where:

- *x represents the water level,*
- *m is the maximum water level, and*
- *ϵ is the time trigger constant.*

Assuming $\epsilon \neq 0$:

1. *Prove that the water level never exceeds the maximum m.*
2. *Derive a runtime monitor for this model.*

Virtual substitution

Exercise 7. *Normalize the following formulas*

1. $\exists x x^2 = a \vee b > 0$
2. $\exists x x^2 = a \vee x^2 > b$
3. $\exists x((\exists y x^5 > y^4) \wedge \forall z(z + a \leq b \rightarrow z^5 \geq a))$

Exercise 8. *Substitute the square root expression ε into the formula F, i.e. compute F_x^ε. Then find an equivalent formula in the language of real arithmetic.*

1. $F \equiv 3x^2 > 2x \wedge x \neq 3$ *and* $\varepsilon \equiv \sqrt{2}/2$
2. $F \equiv 4x^3 < a \wedge ax \neq 0$ *and* $\varepsilon = a + \sqrt{a}$

Exercise 9. *Consider polynomials $p = ax^2 + bx + c$ and $q = dx + e$. When do $p = 0$ and $q = 0$ have simultaneous solutions?*

Exercise 10. *Let p, q be as before. When does the system $p = 0, q > 0$ have a solution?*

Exercise 11. *Use Virtual substitution to eliminate the quantifier in*

$$\exists x(ax + b \leq 0 \wedge cx - d < 0)$$