Model Checking, SS2011: Exercise Sheet 2

May 11, 2011

Exercise 2.1 Apply the following substitutions.

1. $(y > 0 \wedge \forall x.y = x)[x/y]$
2. $(y > 0 \wedge \forall x.y = x)[y/x]$
3. $(\exists x.y = x)[x + 1/y]$

Exercise 2.2 Prove or refute the following propositions.

1. $(\forall x.x = y + 1) \equiv \forall z.z = y + 1$
2. $(\forall x.x = y + 1)[x/w] \equiv \forall z.(z = y + 1)[x/w]$
3. $(\forall x.x = y + 1)[w/y] \equiv \forall x.(x = y + 1)[w/y]$
4. $((\forall x.x = 1)[x + 1/x]) \equiv \forall x.x = 1$

Exercise 2.3 Let t, s, s' denote terms. Let x and y denote variables. Prove or refute $(t[s/x])[s'/y] = t[s/x, s'/y]$.

Exercise 2.4 Let F and G be formulas. Prove or refute the validity of the following formulas. Note: We enumerate the free variables $x_1, \ldots, x_n$ of F by $\mathrm{F}(x_1, \ldots, x_n)$.

1. $pc = 2 \vee pc = 3 \rightarrow pc = 2 \vee pc = 1$
2. $\exists x''.x = x''$
3. $(y' \geq z' \wedge y = y' \wedge z = z') \equiv y \geq z$
4. $\top \wedge \mathrm{F} \equiv \mathrm{F}$
5. $(\exists x''.y \geq z \wedge x = x'') \equiv (y \geq z \wedge \exists x''.x = x'')$
6. $(y' \geq z' \wedge y = y' \wedge z = z') \equiv (y \geq z \wedge y = y' \wedge z = z')$
7. $(\exists x.\mathrm{F}(x) \wedge \mathrm{G}(x)) \equiv (\exists x.\mathrm{F}(x)) \wedge (\exists x.\mathrm{G}(x))$

8. $(\exists x.\mathrm{F}(x) \vee \mathrm{G}(x)) \equiv (\exists x.\mathrm{F}(x)) \vee (\exists x.\mathrm{G}(x))$
9. $(\exists x \exists y.\mathrm{F}(x) \wedge \mathrm{G}(y)) \equiv (\exists x.\mathrm{F}(x)) \wedge (\exists y.\mathrm{G}(y))$
10. $(\exists x.\mathrm{F}(x)) \equiv (\exists x \exists x.\mathrm{F}(x))$
11. $\exists x.x = 1 \wedge x = 2$

Exercise 2.5 Give an equivalent quantifier-free formula for each of following formulas. Note 1: we denote $\exists x \exists y \exists z.\mathrm{F}$ by $\exists x, y, z.\mathrm{F}$. Note 2: Keep in mind that $\mathrm{F} \wedge \mathrm{G} \vee \mathrm{E} = (\mathrm{F} \wedge \mathrm{G}) \vee \mathrm{E}$.

1. $\exists pc', x', y', z'.pc' = 1 \wedge pc = 2 \wedge y' \geq z' \wedge x = x' \wedge y = y' \wedge z = z'$
2. $\exists pc', x', y', z'.pc' = 1 \wedge pc' = 2 \wedge pc = 2 \wedge y' < z' \wedge x = x' + 1 \wedge y = y' \wedge z = z'$
3. $\exists pc', x', y', z'.(pc' = 2 \wedge y' \geq z' \vee pc' = 1) \wedge pc' = 1 \wedge pc = 2 \wedge y' \geq z' \wedge x = x' \wedge y = y' \wedge z = z'$
4. $\exists pc', x', y', z'.(pc' = 2 \wedge y' \geq z' \vee pc' = 3 \wedge y' \geq z' \wedge x' \geq y' \vee pc' = 1) \wedge pc' = 1 \wedge pc = 2 \wedge y' \geq z' \wedge x = x' \wedge y = y' \wedge z = z'$
5. $\exists pc', x', y', z'.(pc' = 2 \wedge y' \geq z' \vee pc' = 3 \wedge y' \geq z' \wedge x' \geq y' \vee pc' = 1) \wedge pc' = 3 \wedge pc = 4 \wedge x' \geq z' \wedge x = x' \wedge y = y' \wedge z = z'$
6. $\exists pc', x', y', z'.(pc' = 2 \wedge y' \geq z' \vee pc' = 3 \wedge y' \geq z' \wedge x' \geq y' \vee pc' = 1) \wedge pc' = 3 \wedge pc = 5 \wedge x' + 1 \geq z' \wedge x = x' \wedge y = y' \wedge z = z'$

Exercise 2.6 Consider the program $P = (X,\ pc,\ T,\ \varphi_{init},\ \varphi_{err})$ where

- $X = \{x, y, z\}$
- $T = \{\rho_1, \ldots, \rho_5\}$
- $\varphi_{init} = \top$
- $\varphi_{err} = (pc = l_5)$
- $\rho_1 = (pc = l_1 \wedge pc' = l_2 \wedge y \geq z \wedge x' = x \wedge y' = y \wedge z' = z)$
- $\rho_2 = (pc = l_2 \wedge pc' = l_2 \wedge x < y \wedge x' = x + 1 \wedge y' = y \wedge z' = z)$
- $\rho_3 = (pc = l_2 \wedge pc' = l_3 \wedge x \geq y \wedge x' = x \wedge y' = y \wedge z' = z)$
- $\rho_4 = (pc = l_3 \wedge pc' = l_4 \wedge x \geq z \wedge x' = x \wedge y' = y \wedge z' = z)$
- $\rho_5 = (pc = l_3 \wedge pc' = l_5 \wedge x < z \wedge x' = x \wedge y' = y \wedge z' = z)$

Apply the Forward-Symbolic-Reachability (FSR) algorithm to decide whether the program is safe or not. Note: a program is safe if the formula C returned by FSR is such that $\neg \exists x, y, z, pc.C \wedge \varphi_{err}$.