Syntactic Substitution

CS 536: Science of Programming, Fall 2022

A. Why

- Syntactic substitution is used in the assignment rules to calculate the weakest precondition *(*and as we'll see, the strongest postcondition*)*.

B. Objectives

At the end of this activity you should

- Be able to calculate a syntactic substitution on an expression or predicate.

C. Questions

1. Calculate $(x+i*b+c = 0)[i+1/i][b+c/c]$.
2. Let p be $\exists x.x < y \wedge x^2 \geq y+k$
   a. What is $p[5/x]$?
   b. What is $p[5/y]$?
   c. What is $p[5/z]$?
   d. What is $p[y*2/y]$?
   e. What is $p[y*k/y]$?
   f. What is $p[(x + y) \div 2/y]$?
3. Give an example where $(v * w)[e/v][e'/w]$ and $(v * w)[e'/w][e/v]$ are
   a. Syntactically equal $(\equiv)$
   b. Syntactically unequal $(\not\equiv)$.
4. In the predicate $(\exists x\ .\ x < y \wedge x^2 \geq y+k)$, x is bound, but in $(x < y \wedge x^2 \geq y+k)$, x is free — is this a contradiction?
5. For substitution into a quantified predicate $(Qx.p)[e/v]$, we could just say "always rename x to something fresh." Why do you think we didn't do that?
6. Let $p \equiv (\forall\, x.\exists\, y.R(x, y, z)) \wedge (\exists\, z.R(x, y, z))$ where R is a boolean function over three arguments.
   a. What is $p[17/w]$?
   b. What is $p[17/x]$?
   c. What is $p[y*2/y]$?
   d. What is $p[y*2/z]$?
   e. What is $p[a*z/y][a+b/z]$?

Solution to Practice 12 (Syntactic Substitution)

1. $(x+i*b+c = 0)[i+1/i][b+c/c] \equiv (\ x + (i+1)*b + c = 0\ )[b+c/c]$
   $\equiv x+(i+1)*b+(b+c) = 0$
2. Let $p \equiv \exists\, x\,.\, x < y \wedge x^2 \geq y+k$
   2a. $p[5/x] \equiv p$ unchanged
   2b. $p[5/y] \equiv (\exists\, x\,.\, x < y \wedge x^2 \geq y+k)[5/y] \equiv \exists\, x\,.\, x < 5 \wedge x^2 \geq 5+k$
   2c. $p[5/z] \equiv p$ unchanged because z doesn't occur in p
   2d. $p[y*2/y] \equiv (\exists\, x\,.\, x < y \wedge x^2 \geq y+k)[y*2/y] \equiv \exists\, x\,.\, x < y*2 \wedge x^2 \geq y*2+k$
   2e. $p[y*k/y] \equiv (\exists\, x\,.\, x < y \wedge x^2 \geq y+k)[y*k/y] \equiv \exists\, x\,.\, x < y*k \wedge x^2 \geq y*k+k$
   2f. $p[(x + y) \div 2/y] \equiv (\exists\, x\,.\, x < y \wedge x^2 \geq y+k)[(x + y) \div 2/y]$
   $\equiv \exists\, v.(x < y \wedge x^2 \geq y+k)[v/x][(x + y) \div 2/y]$ (note renaming of x to v)
   $\equiv \exists\, v\,.(v < y \wedge v^2 \geq y+k)[(x + y) \div 2/y]$
   $\equiv \exists\, v\,.\, v < (x + y) \div 2 \wedge v^2 \geq (x + y) \div 2 + k$
3. (Cases where $(v * w)[e/v][e'/w]$ and $(v * w)[e'/w][e/v]$ are $\equiv$ and $\not\equiv$.)
   3a. One case is when v doesn't occur in e' and w doesn't occur in e.
   Example: $(v * w)[v*2/v][a*w/w] \equiv (v*2 * w)[a*w/w]$
   $\equiv v*2 *(a*w) \equiv (v *(a*w))[v*2/v]$
   $\equiv (v * w)[a*w/w][v*2/v]$
   3b. One case is when w appears in e and v appears in e', at least, for certain e and e'.
   Example: $(v * w)[w-3/v][a*v/w] \equiv ((w-3) * w)[a*v/w] \equiv (w-3) * (a * v)$
   but $(v * w)[a*v/w][w-3/v] \equiv (v *(a*v))[w-3/v] \equiv (w-3) *(a* (w-3))$
4. No, this is exactly what a quantifier does: It captures the x's that are free in its body and makes them bound with respect to any context that includes the quantified predicate.
5. Because it's confusing/annoying to have to come up with fresh variables if we don't really need them.
6. Substitutions with $p \equiv (\forall\, x.\exists\, y.R(x, y, z)) \wedge \exists\, z.R(x, y, z)$:
   6a. $p[17/w] \equiv p$ (because w doesn't occur in p)
   6b. $p[17/x] \equiv (\forall\, x.\exists\, y.R(x, y, z)) \wedge \exists\, z.R(17, y, z)\ )$
   6c. $p[y*2/y] \equiv (\forall\, x.\exists\, y.R(x, y, z)) \wedge \exists\, z.R(x, y*2, z)\ )$
   6d. $p[y*2/z] \equiv (\forall\, x.\exists\, v.R(x, y, z)[v/y][y*2/z]) \wedge \exists\, z.R(x, y, z)\ )$ (using v as a fresh variable)
   $\equiv (\forall\, x.\exists\, v.R(x, v, y*2)) \wedge \exists\, z.R(x, y, z)\ )$
   6e. $p[a*z/y][a+b/z]$
   $\equiv (\forall\, x.\exists\, y.R(x, y, z)) \wedge \exists\, v.R(x, y, z)[v/z][a*z/y])[a+b/z]$ (using v as a fresh variable)
   $\equiv (\ (\forall\, x.\exists\, y.R(x, y, z)) \wedge \exists\, v.R(x, y, v)\ [a*z/y]\ )[a+b/z]$ (only the first y is quantified)
   $\equiv ((\forall\, x.\exists\, y.R(x, y, z)) \wedge \exists\, v.R(x, a*z, v))\ [a+b/z]$
   $\equiv ((\forall\, x.\exists\, y.R(x, y, a+b)) \wedge \exists\, v.R(x, a*(a+b), v))$ (parens around $a+b$ are required)
   (No renaming necessary because we have no quantification of a or b.)

