CS 520
Theory of Programming Language

03/10 – 03/17, 2021

1. Reminder.

① Predicate logic ·· syntax, den. semantics, inf. rules

② Binding ···· local variable declaration. ....$[\![\underset{\uparrow}{\forall x}. p]\!] = [\![\forall y. p[x \to y]]\!]$

$y \notin FV(P) - \{x\}$.

③ Substitution in the presence of binding.

2. Substitution.

$\delta : \langle \text{var} \rangle \to \langle \text{intexp} \rangle$.

p/δ .... subst. all free variables in p using δ.

two typical errors. ① $(\forall x.\ x > y) / x \to y$. $= \left[\begin{array}{ll} \forall x.\ x > y. & \checkmark \\ \forall x.\ y > y & \times \end{array} \right.$

free variable

② $(\forall x.\ x > y) / y \to x+1 = \left[\begin{array}{ll} \forall x.\ x > x+1. & \times \\ \forall x_{new}.\ (x_{new} > y) / y \to x+1 & \\ = \forall x_{new}.\ x_{new} > x+1 & \bigcirc \end{array} \right.$

variable capturing

① defined in a syntax-directed way

$true/\delta = true.$

$false/\delta = false.$

$(e_1 \underset{?}{=} e_2 / \delta) = (e_1/\delta \underset{?}{=} e_2/\delta).$

$(p_1 \wedge p_2)/\delta = (p_1/\delta \wedge p_2/\delta).$

$\neg p/\delta = \neg(p/\delta).$

$(\forall x. p)/\delta = \forall x_{new}(p/[\delta \mid \underbrace{x : x_{new}}])$

allows us to avoid the first pb.

where $x_{new} \notin \bigcup FV(\delta(y))$
$\forall y \in FV(p) - \{x\}.$

$p = \ldots y_1 \ldots x \ldots y_2 \ldots$

$\delta(y_1) \qquad \delta(y_2).$

$x_{new}.$

1) $x_{new} \equiv x$
if x satisfies the cond.

2) pick the first variable satisfying the cond.

② [Correspondence]

<u>Lemma</u>

p ... assertion.

σ, σ' .... states. $\in \underset{\Sigma}{\overset{\Sigma \atop ||}{}}[\langle var \rangle \to \mathbb{Z}]$.

if $\sigma(x) = \sigma'(x)$ for all $x \in FV(p)$, then. $[\![p]\!]\sigma = [\![p]\!]\sigma'$. $\left([\![p]\!] \in [\Sigma \to \mathbb{B}] \right)$

Proof. By structural induction. (case analysis on p & proof using ind. hypo).

$p \equiv true$ ..... $[\![p]\!]\sigma \overset{?}{=} [\![p]\!]\sigma'$, $[\![p]\!]\sigma = tt$, $[\![p]\!]\sigma' = tt$.

$p \equiv p_1 \wedge p_2$ .... $FV(p_i) \subseteq FV(p)$. $\therefore$ σ, σ' satisfy the assumptions of the lemma for p_1 & p_2.

$\therefore$ By ind. hypo., $[\![p_1]\!]\sigma = [\![p_1]\!]\sigma'$, $[\![p_2]\!]\sigma = [\![p_2]\!]\sigma'$

$[\![p]\!]\sigma = [\![p_1]\!]\sigma \wedge [\![p_2]\!]\sigma$

logical $\wedge$ operator

$= [\![p_1]\!]\sigma' \wedge [\![p_2]\!]\sigma'$

$= [\![p_1 \wedge p_2]\!]\sigma' = [\![p]\!]\sigma'$

$p \equiv \forall x. p_1$ ......

ex: prove it.

Pick $n \in \mathbb{Z}$.

$[\sigma | x : n]$, $[\sigma' | x : n]$.

satisfy the assm. for p_1

$\therefore$ $[\![p_1]\!][\sigma | x : n] = [\![p_1]\!][\sigma' | x : n]$

by ind. hypo.

$$[\![p]\!]\sigma = (\forall n \in \mathbb{Z}.\ [\![p_1]\!][\sigma | x : n])$$
$$= (\forall n \in \mathbb{Z}.\ [\![p_1]\!][\sigma' | x : n])$$
$$= [\![p]\!]\sigma'.$$

$\square$

what we learnt.

Lemma [Substitution] ... correspondence bt syntactic subst. and semantic subst.

p ... assertion.

σ, σ' ... states.

δ ... substitution.

$\sigma'(x) = [\![\delta(x)]\!]\sigma$ for all $x \in FV(p)$.

" $\sigma' = \sigma/\delta$ " informal.

$\Rightarrow$ $[\![p/\delta]\!]\sigma = [\![p]\!]\sigma'$

(informal description ... $[\![p/\delta]\!]\sigma = [\![p]\!](\overset{\text{informal}}{\sigma/\delta})$).

Recall. $S \equiv x_1 \to e_1, x_2 \to e_2, \dots, x_n \to e_n.$

$$[\sigma \mid x : n](y) = \begin{cases} n & \text{if } x \equiv y \\ \sigma(y) & \text{otherwise.} \end{cases}$$

weakest precondition

Cor. $$[\![p / x_1 \to e_1, \dots, x_n \to e_n]\!]\sigma = [\![p]\!] [\sigma \mid x_1 : [\![e_1]\!]\sigma, x_2 : [\![e_2]\!]\sigma, \dots \mid x_n : [\![e_n]\!]\sigma].$$

($x_1, \dots, x_n$ are distinct).

Cor $\llbracket \underbrace{\forall x. p}_{|} \rrbracket \sigma = \llbracket \forall y. p/x \to y \rrbracket \sigma$. as long as. $y \notin FV(p) - \{x\}$.

Proof. ex: prove it.

$\delta = \phi$ .... identity substitution.

By Cor. above, $* \;\; \underbrace{\llbracket (\forall x. p)/\phi}_{\shortparallel} \rrbracket \sigma = \llbracket \forall x. p \rrbracket [\underbrace{\sigma | \phi}_{\sigma}] = \llbracket \forall x. p \rrbracket \sigma$.

$\shortparallel$

$\llbracket \forall x. p/x \to x_{new} \rrbracket \sigma$. $\forall x_{new}. (\underbrace{p/[\phi | x : x_{new}]}_{p/x \to x_{new}})$

$$\left[\frac{x_{new} \notin \bigcup_{y \in FV(p) - \{x\}} FV(\phi(y))}{x_{new} \notin FV(p) - \{x\}.} \right]$$

D.