E *sp*'s proofs

E.1 $x := E$

$$
\begin{array}{rlll}
sp_o(\gamma(P), x := E) & = \{s', h' \mid \exists s, h.\ s, h \models & P \wedge\ h' = h \wedge\ s' = [s \mid x \to [\![E]\!]s]\} \\
& = \{s', h' \mid \exists s. & s, h' \models\ P \wedge\ s' = [s \mid x \to [\![E]\!]s]\} \\
\gamma(sp(P, x := E)) & = \{s', h' \mid & s', h' \models \exists x'.\ P[x'/x] \wedge\ x = E\{x'/x\}\} \\
& = \{s', h' \mid & \exists v. \quad [s' \mid x' \to v], h' \models P[x'/x]\ \wedge\ [s' \mid x' \to v](x) = [\![E\{x'/x\}]\!][s' \mid x' \to v]\} \\
& = \{s', h' \mid & \exists v. \quad [s \mid x' \to v \mid x \to v], h' \models P\ \wedge\ s'(x) = [\![E]\!][s' \mid x' \to v \mid x \to v]\} \\
& = \{s', h' \mid & \exists v. \quad [s' \mid x' \to v \mid x \to v], h' \models P\ \wedge\ s'(x) = [\![E]\!][s' \mid x \to v]\} \\
& = \{s', h' \mid & \exists v. \quad [s' \mid v \mid x \to v], h' \models P\ \wedge\ s'(x) = [\![E]\!][s' \mid x \to v]\}
\end{array}
$$

The last equality is because $x' \notin Var(P)$.

We can prove the inclusion by taking $v = s(x)$ if $x \in dom(s)$ and any value otherwise.

We could also prove the inclusion in the other way by taking $s = [s' \mid x \to v]$.

So we have $sp_o(\gamma(P), x := E)\ =\ \gamma(sp(P, x := E))$.

E.2 $x := E.i$

$$
\begin{array}{rlll}
sp_o(\gamma(P), x := E.i) & = \{s', h' \mid \exists s, h.\ s, h \models & P \wedge\ h' = h \wedge\ [\![E]\!]s \in Loc\ \wedge\ (\exists v.\ v = \pi_i(h([\![E]\!]s)) \wedge\ s' = [s \mid x \to v])\} \\
& = \{s', h' \mid \exists s. & s, h' \models\ P \wedge\ (\exists v.\ v = \pi_i(h'([\![E]\!]s)) \wedge\ s' = [s \mid x \to v])\} \\
& = \{s', h' \mid \exists s. & s, h' \models\ P \wedge\ s' = [s \mid x \to \pi_i(h'([\![E]\!]s))])\} \\
\gamma(sp(P, x := E.i)) & = \{s', h' \mid & s', h' \models \exists x'.\ P[x'/x] \wedge\ x = (E\{x'/x\}).i\} \\
& = \{s', h' \mid & \exists v. \quad [s' \mid x' \to v], h' \models P[x'/x]\ \wedge\ [s' \mid x' \to v](x) = \pi_i(h([\![E\{x'/x\}]\!][s' \mid x' \\
& = \{s', h' \mid & \exists v. \quad [s \mid x' \to v \mid x \to v], h' \models P\ \wedge\ s'(x) = \pi_i(h([\![E]\!][s' \mid x' \to v \mid x \to v]))\} \\
& = \{s', h' \mid & \exists v. \quad [s' \mid x' \to v \mid x \to v], h' \models P\ \wedge\ s'(x) = \pi_i(h([\![E]\!][s' \mid x \to v]))\} \\
& = \{s', h' \mid & \exists v. \quad [s' \mid x \to v], h' \models P\ \wedge\ s'(x) = \pi_i(h([\![E]\!][s' \mid x \to v]))\}
\end{array}
$$

The last equality is because $x' \notin Var(P)$.

We can prove the inclusion by taking $v = s(x)$ if $x \in dom(s)$ and any value otherwise.

We could also prove the inclusion in the other way by taking $s = [s' \mid x \to v]$.

So we have $sp_o(\gamma(P), x := E.i)\ =\ \gamma(sp(P, x := E.i))$.

E.3 $E_1.i := E_2$

$$
\begin{array}{rll}
sp_o(\gamma(P), E_1.1 := E_2) & = \{s', h' \mid \exists h.\ s', h \in & \gamma(P) \wedge\ \exists v_1, v_2. h([\![E_1]\!]s') = \langle v_1, v_2\rangle \wedge h' = [h \mid [\![E_1]\!]s' \rightarrow \langle [\![E_2]\!]s', v_2\rangle]\} \\
\gamma(sp(P, E_1 := E_2.i)) & = \{s', h' \mid & s', h' \in \gamma(\exists x_1, x_2.\ (E \mapsto E_2, x_2) * ((E_1 \mapsto x_1, x_2) \mathrel{-\!\!*} P))\} \\
& = \{s', h' \mid & \exists v_1, v_2.\ \exists h'_0, h'_1. h'_0 \sharp h'_1. \\
& & \quad \wedge\ h' = h'_0 \cdot h'_1 \\
& & \quad \wedge\ [s \mid x_i \mapsto v_i], h'_0 \in \gamma(E_1 \mapsto E_2, x_2) \\
& & \quad \wedge\ [s \mid x_i \mapsto v_i], h'_1 \in \gamma((E_1 \mapsto x_1, x_2) \mathrel{-\!\!*} P)\} \\
& = \{s', h' \mid & \exists v_1, v_2.\ \exists h'_0, h'_1. h'_0 \sharp h'_1. \\
& & \quad \wedge\ h' = h'_0 \cdot h'_1 \\
& & \quad \wedge [\![E_1]\!]s' \in Loc \\
& & \quad \wedge h'_0 = [[\![E_1]\!]s' \mapsto \langle [\![E_2]\!]s', v_2\rangle] \text{ (using } x_i \notin Var(E_2)) \\
& & \quad \wedge \forall h_0. \text{If } h_0 \sharp h'_1 \text{ and } h_0 = [[\![E_1]\!]s' \mapsto \langle v_1, v_2\rangle] \\
& & \quad \text{ then } s', h_0 \cdot h'_1 \in \gamma(P) \\
& = \{s', h' \mid & \exists v_1, v_2.\ \exists h'_0, h'_1. h'_0 \sharp h'_1. \\
& & \quad \wedge\ h' = h'_0 \cdot h'_1 \\
& & \quad \wedge [\![E_1]\!]s' \in Loc \\
& & \quad \wedge h'_0 = [[\![E_1]\!]s' \mapsto \langle [\![E_2]\!]s', v_2\rangle] \text{ (using } x_i \notin Var(E_2)) \\
& & \quad \wedge \text{If } [\![E_1]\!]s' \notin dom(h'_1) \\
& & \quad \text{ then } s', [[\![E_1]\!]s' \mapsto \langle v_1, v_2\rangle] \cdot h'_1 \in \gamma(P) \\
& = \{s', h' \mid & \exists v_1, v_2.\ \exists h'_0, h'_1. h'_0 \sharp h'_1. \\
& & \quad \wedge\ h' = h'_0 \cdot h'_1 \\
& & \quad \wedge [\![E_1]\!]s' \in Loc \\
& & \quad \wedge h'_0 = [[\![E_1]\!]s' \mapsto \langle [\![E_2]\!]s', v_2\rangle] \text{ (using } x_i \notin Var(E_2)) \\
& & \quad \wedge s', [[\![E_1]\!]s' \mapsto \langle v_1, v_2\rangle] \cdot h'_1 \in \gamma(P)
\end{array}
$$

We can prove the inclusion by taking $h'_1 = h \mid_{dom(h) \setminus [\![E_1]\!]s'}$. We could also prove the inclusion in the other way by taking $h = [[\![E_1]\!]s' \mapsto \langle v_1, v_2\rangle] \cdot h'_1$.

So we have $sp_o(\gamma(P), E_1 := E_2.i) \ = \ \gamma(sp(P, E_1 := E_2.i))$.

E.4 $x :=$ `cons`(E_1, E_2)

Not typed yet.

E.5 `dispose`(E)

Not typed yet.

E.6 $C_1; C_2$

We prove that $sp_o(\gamma(P), C_1; C_2) = \gamma(sp(P, C_1; C_2))$ by induction on the size of the command.

$$
\begin{array}{rll}
sp_o(\gamma(P), C_1; C_2) & = sp_o(sp_o(\gamma(P), C_1), C_2) & definition \\
& = sp_o(\gamma(sp(P, C_1)), C_2) & induction\ hypothesis \\
& = \gamma(sp((sp(P, C_1)), C_2)) & induction\ hypothesis \\
& = \gamma(sp(P, C_1; C_2)) & definition
\end{array}
$$

E.7 *if E then C_1 else C_2*

$C = if\ \ E\ \ then\ \ C_1\ \ else\ \ C_2$

$$
\begin{array}{rrll}
sp_o(\gamma(P), C) = & \{s', h' \mid \exists s, h. & s, h \models P & \wedge ((\llbracket E \rrbracket s = True\ \wedge\ s', h' \in sp_o(\{s, h\}, C_1)) \\
 & & & \vee (\llbracket E \rrbracket s = False\ \wedge\ s', h' \in sp_o(\{s, h\}, C_2)))\} \\
= & \{s', h' \mid \exists s, h. & ((s, h \models P & \wedge E = \texttt{true}\ \wedge\ s', h' \in sp_o(\{s, h\}, C_1)) \\
 & & \vee (s, h \models P & \wedge E = \texttt{false}\ \wedge\ s', h' \in sp_o(\{s, h\}, C_2)))\} \\
= & sp_o(\gamma(P \wedge E = \texttt{true}), C_1) \cup & & sp_o(\gamma(P \wedge E = \texttt{false}), C_2) \\
\gamma(sp(P, C)) = & \{s', h' \mid & s', h' \models & (sp(P \wedge E = \texttt{true}, C_1) \\
 & & & \vee sp(P \wedge E = \texttt{false}, C_2))\} \\
= & \{s', h' \mid & s', h' \models & sp(P \wedge E = \texttt{true}, C_1)\} \\
 & \cup \{s', h' \mid & s', h' \models & sp(P \wedge E = \texttt{false}, C_2)\} \\
= & \gamma(sp(P \wedge E = \texttt{true}, C_1)) \cup & & \gamma(sp(P \wedge E = \texttt{false}, C_2))
\end{array}
$$

We prove by induction in the size of the command.

E.8 `skip`

$$
\begin{aligned}
sp_o(\gamma(P), \texttt{skip}) &= \gamma(P) \\
\gamma(sp(P, \texttt{skip})) &= \gamma(P)
\end{aligned}
$$

So we have $sp_o(\gamma(P), \texttt{skip}) = \gamma(sp(P, \texttt{skip}))$.

E.9 *while E do C_1*

We define $F_o = \lambda X.\ \gamma(P) \cup sp_o(X \cap \gamma(E = \texttt{true}), C_1)$
and $F = \lambda X.\ \Gamma_{[X_v \mapsto X]}(sp(X_v \wedge E = \texttt{true}, C_1) \vee P)$.

Lemma 7. $\forall n \geq 0. F_o^n(\emptyset) = F^n(\emptyset)$

Proof (Lemma 7). We prove by recurrence that the $F_o^n(\emptyset) = F^n(\emptyset)$ and that $\exists Y.\ F^n(\emptyset) = \gamma(Y)$:

- Case n=0 :
  $F_o^0(\emptyset) = \gamma(P) \cup \emptyset$
  $= \gamma(P \vee \texttt{false})$
  $F^0(\emptyset) = \Gamma_{[X_v \mapsto \emptyset]}(sp(X_v \wedge E = \texttt{true}, C_1) \vee P)$
  $= \Gamma_{[X_v \mapsto \gamma(\texttt{false})]}(sp(X_v \wedge E = \texttt{true}, C_1) \vee P)$
  $= \gamma(sp(\texttt{false} \wedge E = \texttt{true}, C_1) \vee P)$ (by Th. 4)
  $= \gamma(\texttt{false} \vee P)$
- Case n+1. : $F_o^{n+1}(\emptyset) = F_o(F_o^n(\emptyset))$
  $= F_o(F^n(\emptyset))$
  $= \gamma(P) \cup sp_o(F^n(\emptyset) \cap \gamma(E = \texttt{true}), C_1)$
  by induction hyp $\exists Y.\ F^n(\emptyset) = \gamma(Y)$
  so $= \gamma(P) \cup sp_o(\gamma(Y) \cap \gamma(E = \texttt{true}), C_1)$
  $= \gamma(P) \cup sp_o(\gamma(Y \vee E = \texttt{true}), C_1)$
  $= \gamma(P) \cup \gamma(sp(Y \vee E = \texttt{true}, C_1))$, by the global ind. hyp
  $= \gamma(sp(Y \wedge E = \texttt{true}, C_1) \vee P)$
  $= \Gamma_{[X_v \mapsto \gamma(Y)]}(sp(X_v \wedge E = \texttt{true}, C_1) \vee P)$, by Th. 4+ lemma 9+ X_v not free in P
  $= \Gamma_{[X_v \mapsto F^n]}(sp(X_v \wedge E = \texttt{true}, C_1) \vee P)$
  $= F^{n+1}(\emptyset)$

□

Lemma 8. *F is upper-continuous.*

Proof (Lemma 8). The proof come directly from lemma 13 and theorem 6 □

$$
\begin{aligned}
sp_o(\gamma(P), w\ E\ d\ C_1) &= (\mathrm{lfp}^{\subseteq}_{\emptyset} \lambda X.\ \{s', h' \mid \exists s, h.\ s, h \in X \wedge \begin{pmatrix} ([\![E]\!]s = True\ \wedge s', h' \in sp_o(\{s, h\}, C_1)) \\ \vee (s', h' \in \gamma(P))\}) \end{pmatrix} \\
&\quad \cap \{s', h' \mid [\![E]\!]s' = \texttt{false}\} \\
&= (\mathrm{lfp}^{\subseteq}_{\emptyset} \lambda X.\ \begin{matrix} \{s', h' \mid \exists s, h.\ s, h \in X \wedge\ [\![E]\!]s = True\ \wedge s', h' \in sp_o(\{s, h\}, C_1)\} \\ \cup \gamma(P) \end{matrix}) \\
&\quad \cap \gamma(E = \texttt{false}) \\
&= (\mathrm{lfp}^{\subseteq}_{\emptyset} \lambda X.\ \gamma(P) \cup\ sp_o(X \cap \gamma(E = \texttt{true}), C_1)) \\
&\quad \cap \gamma(E = \texttt{false}) \\
&= (\mathrm{lfp}^{\subseteq}_{\emptyset} F_o) \\
&\quad \cap \gamma(E = \texttt{false}) \\
(F_o\ u.c. + Tarski) \quad &= \bigcup_{n \geq 0} F_o^n(\emptyset) \\
&\quad \cap \gamma(E = \texttt{false}) \\
(Lem. 7) \quad &= \bigcup_{n \geq 0} F^n(\emptyset) \\
&\quad \cap \gamma(E = \texttt{false})
\end{aligned}
$$

$$
\begin{aligned}
\gamma(sp(P, w\ E\ d\ C_1)) &= \gamma(\mu X_v.\ (P \vee sp(X_v \wedge E = \texttt{true}, C_1)) \\
&\qquad \wedge (E = \texttt{false})) \\
&= \gamma(\mu X_v.\ (P \vee sp(X_v \wedge E = \texttt{true}, C_1))) \\
&\quad \cap\ \gamma(E = \texttt{false}) \\
&= \Gamma(\mu X_v.\ (P \vee sp(X_v \wedge E = \texttt{true}, C_1))) \\
&\quad \cap\ \gamma(E = \texttt{false}) \\
&= (\mathrm{lfp}^{\subseteq}_{\emptyset}\, \lambda X.\ \Gamma_{[X_v \mapsto X]}(sp(X_v \wedge E = \texttt{true}, C_1) \vee P)) \\
&\quad \cap\ \gamma(E = \texttt{false}) \\
&= (\mathrm{lfp}^{\subseteq}_{\emptyset}\, F) \\
&\quad \cap\ \gamma(E = \texttt{false}) \\
(Lem.8 + Tarski) &= \bigcup_{n \geq 0} F^n(\emptyset) \\
&\quad \cap\ \gamma(E = \texttt{false})
\end{aligned}
$$

So we have that
$sp_o(\gamma(P), while\ \ E\ \ do\ \ C_1) = \gamma(sp(P, while\ \ E\ \ do\ \ C_1))$.