The HOL Semantics of PSL

The semantics (Section 2) and theorems (Section 3) below are generated from the HOL sources using Keith Wansbrough's HOL-to-latex tool.

1 Syntax

If p ranges over the set P of atomic propositions, then the syntax of boolean expressions b is:

$$
\begin{array}{lcll}
b & ::= & p & \text{(Atomic proposition)} \\
 & \mid & \neg b & \text{(Negation)} \\
 & \mid & b_1 \wedge b_2 & \text{(Conjunction)}
\end{array}
$$

If r, r_1, r_2 etc. range over Sugar Extended Regular Expressions (SEREs) and b and c range over boolean expressions, then the syntax of SEREs is:

$$
\begin{array}{lcll}
r & ::= & b & \text{(Boolean formula)} \\
 & \mid & \{r_1\} \mid \{r_2\} & \text{(Disjunction)} \\
 & \mid & r_1 ; r_2 & \text{(Concatenation)} \\
 & \mid & r_1 : r_2 & \text{(Fusion: overlapping concatenation)} \\
 & \mid & \{r_1\}\&\&\{r_2\} & \text{(Length matching conjunction)} \\
 & \mid & r[*] & \text{(Repeat)} \\
 & \mid & r@c & \text{(Clocking)}
\end{array}
$$

The syntax of PSL Foundation Language Formulas (FL) is:

$$
\begin{array}{lcll}
f & ::= & p & \text{(Atomic formula)} \\
 & \mid & \neg f & \text{(Negation)} \\
 & \mid & f_1 \wedge f_2 & \text{(Conjunction)} \\
 & \mid & X!\ f & \text{(Successor)} \\
 & \mid & [f_1\ U\ f_2] & \text{(Until)} \\
 & \mid & \{r\}(f) & \text{(Suffix implication)} \\
 & \mid & \{r_1\} \mapsto \{r_2\}! & \text{(Strong suffix implication)} \\
 & \mid & \{r_1\} \mapsto \{r_2\} & \text{(Weak suffix implication)} \\
 & \mid & f\ \mathit{abort}\ b & \text{(Abort)} \\
 & \mid & f@c! & \text{(Clocking)}
\end{array}
$$

The syntax of the PSL Optional Branching Extension(OBE) is:

$$
\begin{array}{lcll}
f & ::= & p & \text{(Atom)} \\
 & \mid & \neg f & \text{(Negation)} \\
 & \mid & f_1\ \wedge\ f_2 & \text{(Conjunction)} \\
 & \mid & \mathbf{EX} f & \text{(Some successors)} \\
 & \mid & \mathbf{E}[f_1\ \mathbf{U}\ f_2] & \text{(Until -- along some path)} \\
 & \mid & \mathbf{EG} f & \text{(Always on some path)}
\end{array}
$$

2 Semantics

2.1 Boolean expressions

$(l \models p \;=\; p \in l)$
$\wedge$
$(l \models \neg b \;=\; \neg(l \models b))$
$\wedge$
$(l \models b_1 \wedge b_2 \;=\; l \models b_1 \wedge l \models b_2)$

2.2 Unclocked Semantics of SEREs

$(w \models b \;=\; (|w| = 1) \wedge w_0 \models b)$
$\wedge$
$(w \models r_1; r_2 \;=\; \exists w1\, w2.(w = w1\, w2) \wedge w1 \models r_1 \wedge w2 \models r_2)$
$\wedge$
$(w \models r_1 : r_2 \;=\; \exists w1\, w2\, l.(w = w1[l]w2) \wedge w1[l] \models r_1 \wedge [l]w2 \models r_2)$
$\wedge$
$(w \models \{r_1\} \mid \{r_2\} \;=\; w \models r_1 \vee w \models r_2)$
$\wedge$
$(w \models \{r_1\}\&\&\{r_2\} \;=\; w \models r_1 \wedge w \models r_2)$
$\wedge$
$(w \models r[*] \;=\; \exists wlist.(w = \mathsf{Concat}\, wlist) \wedge \mathsf{Every}(\lambda w.w \models r)\, wlist)$

2.3 Unclocked Semantics of FL formulas

$(w \models b \;=\; |w| > 0 \wedge w_0 \models b)$
$\wedge$
$(w \models \neg f \;=\; \neg(w \models f))$
$\wedge$
$(w \models f_1 \wedge f_2 \;=\; w \models f_1 \wedge w \models f_2)$
$\wedge$
$(w \models X!\, f \;=\; |w| > 1 \wedge w^1 \models f)$
$\wedge$
$(w \models [f_1\ U\ f_2] \;=\; \exists k \in (0 \,..\, |w|).w^k \models f_2 \wedge \forall j \in (0 \,..\, k).w^j \models f_1)$
$\wedge$
$(w \models \{r\}(f) \;=\; \forall j \in (0 \,..\, |w|).w^{0,j} \models r \Rightarrow w^j \models f)$
$\wedge$
$(w \models \{r_1\} \mapsto \{r_2\}! \;=\; \forall j \in (0 \,..\, |w|).w^{0,j} \models r_1 \Rightarrow \exists k \in (j \,..\, |w|).w^{j,k} \models r_2)$
$\wedge$
$(w \models \{r_1\} \mapsto \{r_2\} \;=$
$\forall j \in (0 \,..\, |w|).$
$w^{0,j} \models r_1 \Rightarrow ((\exists k \in (j \,..\, |w|).w^{j,k} \models r_2) \vee (\forall k \in (j \,..\, |w|).\exists w'.w^{j,k}w' \models r_2)))$
$\wedge$
$(w \models f\ abort\ b \;=\; w \models f \vee w \models b \vee \exists j \in (1 \,..\, |w|).\exists w'.w^j \models b \wedge w^{0,j-1}w' \models f)$

2.4 Semantics of OBE formulas

A Kripke Structure M is a quintuple $M = (S, S0, R, P, L)$. The transition relation component of M is $M.R$, the L component is $M.L$ etc. Define:

$\mathsf{Path}\ M\ p\ s\ =\ (|p| = \infty) \wedge (p_0 = s) \wedge (\forall n.M.R(p_n, p_{n+1}))$

then the semantics is:

$$
\begin{array}{l}
(M, s \models b\ =\ M.L\ s \models b) \\
\wedge \\
(M, s \models \neg f\ =\ \neg(M, s \models f)) \\
\wedge \\
(M, s \models f_1 \wedge f_2\ =\ M, s \models f_1 \wedge M, s \models f_2) \\
\wedge \\
(M, s \models EX\ f]\ =\ \exists p.\mathsf{Path}\ M\ p\ s \wedge M, p_1 \models f) \\
\wedge \\
(M, s \models [f_1\ U\ f_2]\ = \\
\quad \exists p.\mathsf{Path}\ M\ p\ s \wedge \exists k \in (0 .. |p|).M, p_k \models f_2 \wedge \forall j.j < k \Rightarrow M, p_j \models f_1) \\
\wedge \\
(M, s \models EG\ f]\ =\ \exists p.\mathsf{Path}\ M\ p\ s \wedge \forall j \in (0 .. |p|).M, p_j \models f)
\end{array}
$$

2.5 Clocked semantics of SEREs

$$
\begin{array}{l}
(w \overset{c}{\models} b\ =\ |w| \geq 1 \wedge (\forall i \in (0 .. (|w| - 1)).w_i \models \neg c) \wedge w_{|w|-1} \models c \wedge b) \\
\wedge \\
(w \overset{c}{\models} r_1; r_2\ =\ \exists w1\, w2.(w = w1\, w2) \wedge w1 \overset{c}{\models} r_1 \wedge w2 \overset{c}{\models} r_2) \\
\wedge \\
(w \overset{c}{\models} r_1 : r_2\ =\ \exists w1\, w2\, l.(w = w1[l]w2) \wedge w1[l] \overset{c}{\models} r_1 \wedge [l]w2 \overset{c}{\models} r_2) \\
\wedge \\
(w \overset{c}{\models} \{r_1\} \mid \{r_2\}\ =\ w \overset{c}{\models} r_1 \vee w \overset{c}{\models} r_2) \\
\wedge \\
(w \overset{c}{\models} \{r_1\}\&\&\{r_2\}\ =\ w \overset{c}{\models} r_1 \wedge w \overset{c}{\models} r_2) \\
\wedge \\
(w \overset{c}{\models} r[*]\ =\ \exists wlist.(w = \mathsf{Concat}\, wlist) \wedge \mathsf{Every}(\lambda w.w \overset{c}{\models} r)wlist) \\
\wedge \\
(w \overset{c}{\models} r@c_1\ =\ \exists i \in (0 .. |w|).w^{0,i} \models \neg c_1[*]; c_1 \wedge w^i \overset{c_1}{\models} r)
\end{array}
$$

2.6 Clocked semantics of FL formulas

$$
\begin{array}{l}
(w \overset{c}{\models} b\ =\ |w| > 0 \wedge w_0 \models b) \\
\wedge \\
(w \overset{c}{\models} \neg f\ =\ \neg(w \overset{c}{\models} f)) \\
\wedge \\
(w \overset{c}{\models} f_1 \wedge f_2\ =\ w \overset{c}{\models} f_1 \wedge w \overset{c}{\models} f_2) \\
\wedge \\
(w \overset{c}{\models} X!\, f\ =\ \exists i \in (1 .. |w|).w^{1,i} \overset{\mathbf{T}}{\models} \neg c[*]; c \wedge w^i \overset{c}{\models} f) \\
\wedge
\end{array}
$$

$(w \overset{c}{\models} [f_1\ U\ f_2]\ =$
$\quad \exists k \in (0\,..\,|w|).w^k \overset{\mathbf{T}}{\models}\ c \wedge w^k \overset{c}{\models} f_2 \wedge \forall j \in (0\,..\,k).w^j \overset{\mathbf{T}}{\models}\ c \Rightarrow w^j \overset{c}{\models} f_1)$
$\wedge$
$(w \overset{c}{\models} \{r\}(f)\ =$
$\quad \forall i \in (0\,..\,|w|).w^{0,i} \overset{c}{\models} r \Rightarrow \exists j \in (i\,..\,|w|).w^{i,j} \overset{\mathbf{T}}{\models} \neg c[*]; c \wedge w^j \overset{c}{\models} f)$
$\wedge$
$(w \overset{c}{\models} \{r_1\} \mapsto \{r_2\}!\ =$
$\quad \forall i \in (0\,..\,|w|).w^{0,i} \overset{c}{\models} r_1 \Rightarrow \exists j \in (i\,..\,|w|).w^{i,j} \overset{c}{\models} r_2)$
$\wedge$
$(w \overset{c}{\models} \{r_1\} \mapsto \{r_2\}\ =$
$\quad \forall i \in (0\,..\,|w|).$
$\qquad w^{0,i} \overset{c}{\models} r_1$
$\qquad \Rightarrow$
$\qquad ((\exists j \in (i\,..\,|w|).w^{i,j} \overset{c}{\models} r_2) \vee (\forall j \in (i\,..\,|w|).\exists w'.w^{i,j}w' \overset{c}{\models} r_2)))$
$\wedge$
$(w \overset{c}{\models} f\ abort\ b\ =$
$\quad w \overset{c}{\models} f$
$\quad \vee$
$\quad w \overset{c}{\models} b$
$\quad \vee$
$\quad \exists i \in (1\,..\,|w|).\exists w'.w^i \overset{\mathbf{T}}{\models}\ (c \wedge b) \wedge w^{0,i-1}w' \overset{c}{\models} f)$
$\wedge$
$(w \overset{c}{\models} f@c_1!\ =\ \exists i \in (0\,..\,|w|).w^{0,i} \overset{\mathbf{T}}{\models} \neg c_1[*]; c_1 \wedge w^i \overset{c_1}{\models}\ f)$

2.7 Clock removal rewrites

$(\mathcal{T}^c(b)\ =\ (\neg c[*]; c \wedge b))$
$\wedge$
$(\mathcal{T}^c(r_1; r_2)\ =\ \mathcal{T}^c(r_1); \mathcal{T}^c(r_2))$
$\wedge$
$(\mathcal{T}^c(r_1 : r_2)\ =\ \mathcal{T}^c(r_1) : \mathcal{T}^c(r_2))$
$\wedge$
$(\mathcal{T}^c(\{r_1\} \mid \{r_2\})\ =\ \{\mathcal{T}^c(r_1)\} \mid \{\mathcal{T}^c(r_2)\})$
$\wedge$
$(\mathcal{T}^c(\{r_1\}\&\&\{r_2\})\ =\ \{\mathcal{T}^c(r_1)\}\&\&\{\mathcal{T}^c(r_2)\})$
$\wedge$
$(\mathcal{T}^c(r[*])\ =\ \mathcal{T}^c(r)[*])$
$\wedge$
$(\mathcal{T}^c(r@c_1)\ =\ (\neg c_1[*]; c_1 : \mathcal{T}^{c_1}(r)))$

Define

$f_1 \vee f_2\ =\ \neg(\neg f_1 \wedge \neg f_2)$

$f_1 \Rightarrow f_2\ =\ \neg f_1 \vee f_2$

then:

$$(\mathcal{T}^c(b) \;=\; b)$$
$$\wedge$$
$$(\mathcal{T}^c(\neg f) \;=\; \neg(\mathcal{T}^c(f)))$$
$$\wedge$$
$$(\mathcal{T}^c(f_1 \wedge f_2) \;=\; \mathcal{T}^c(f_1) \wedge \mathcal{T}^c(f_2))$$
$$\wedge$$
$$(\mathcal{T}^c(X!\, f) \;=\; X!\, ([\neg c\; U\; (c \wedge \mathcal{T}^c(f))]))$$
$$\wedge$$
$$(\mathcal{T}^c([f_1\; U\; f_2]) \;=\; [c \Rightarrow \mathcal{T}^c(f_1)\; U\; c \wedge \mathcal{T}^c(f_2)])$$
$$\wedge$$
$$(\mathcal{T}^c(\{r\}(f)) \;=\; \{\mathcal{T}^c(r)\}([\neg c\; U\; (c \wedge \mathcal{T}^c(f))]))$$
$$\wedge$$
$$(\mathcal{T}^c(\{r_1\} \mapsto \{r_2\}!) \;=\; \{\mathcal{T}^c(r_1)\} \mapsto \{\mathcal{T}^c(r_2)\}!)$$
$$\wedge$$
$$(\mathcal{T}^c(\{r_1\} \mapsto \{r_2\}) \;=\; \{\mathcal{T}^c(r_1)\} \mapsto \{\mathcal{T}^c(r_2)\})$$
$$\wedge$$
$$(\mathcal{T}^c(f\; abort\; b) \;=\; \mathcal{T}^c(f)\; abort\; c \wedge b)$$
$$\wedge$$
$$(\mathcal{T}^c(f@c_1!) \;=\; [\neg c_1\; U\; (c_1 \wedge \mathcal{T}^{c_1}(f))])$$

3 Main properties proved

Define $\mathsf{ClockFree}(r)$ and $\mathsf{ClockFree}(f)$ by:

$(\mathsf{ClockFree}(b) \;=\; \mathbf{T}) \;\; \wedge$
$(\mathsf{ClockFree}(r_1; r_2) \;=\; \mathsf{ClockFree}(r_1) \wedge \mathsf{ClockFree}(r_2)) \;\; \wedge$
$(\mathsf{ClockFree}(r_1 : r_2) \;=\; \mathsf{ClockFree}(r_1) \wedge \mathsf{ClockFree}(r_2)) \;\; \wedge$
$(\mathsf{ClockFree}(\{r_1\} \mid \{r_2\}) \;=\; \mathsf{ClockFree}(r_1) \wedge \mathsf{ClockFree}(r_2)) \;\; \wedge$
$(\mathsf{ClockFree}(\{r_1\}\&\&\{r_2\}) \;=\; \mathsf{ClockFree}(r_1) \wedge \mathsf{ClockFree}(r_2)) \;\; \wedge$
$(\mathsf{ClockFree}(r[*]) \;=\; \mathsf{ClockFree}(r)) \;\; \wedge$
$(\mathsf{ClockFree}(r@c) \;=\; \mathbf{F})$

$(\mathsf{ClockFree}(b) \;=\; \mathbf{T}) \;\; \wedge$
$(\mathsf{ClockFree}(\neg f) \;=\; \mathsf{ClockFree}(f)) \;\; \wedge$
$(\mathsf{ClockFree}(f_1 \wedge f_2) \;=\; \mathsf{ClockFree}(f_1) \wedge \mathsf{ClockFree}(f_2)) \;\; \wedge$
$(\mathsf{ClockFree}(X!\, f) \;=\; \mathsf{ClockFree}(f)) \;\; \wedge$
$(\mathsf{ClockFree}([f_1\; U\; f_2]) \;=\; \mathsf{ClockFree}(f_1) \wedge \mathsf{ClockFree}(f_2)) \;\; \wedge$
$(\mathsf{ClockFree}(\{r\}(f)) \;=\; \mathsf{ClockFree}(f) \wedge \mathsf{ClockFree}(r)) \;\; \wedge$
$(\mathsf{ClockFree}(\{r_1\} \mapsto \{r_2\}!) \;=\; \mathsf{ClockFree}(r_1) \wedge \mathsf{ClockFree}(r_2)) \;\; \wedge$
$(\mathsf{ClockFree}(\{r_1\} \mapsto \{r_2\}) \;=\; \mathsf{ClockFree}(r_1) \wedge \mathsf{ClockFree}(r_2)) \;\; \wedge$
$(\mathsf{ClockFree}(f\; abort\; b) \;=\; \mathsf{ClockFree}(f)) \;\; \wedge$
$(\mathsf{ClockFree}(f@c!) \;=\; \mathbf{F})$

Then we have proved:

$\vdash \;\; \forall r.\ \mathsf{ClockFree}(r) \Rightarrow \forall w.\ w \models^{\mathbf{T}} r = w \models r$

$\vdash \;\; \forall f.\ \mathsf{ClockFree}(f) \Rightarrow \forall w.\ w \models^{\mathbf{T}} f = w \models f$

Other properties proved include:

$\vdash \;\; \forall r\ w\ c.\ w \models^{c} r \;=\; w \models \mathcal{T}^{c}(r)$

$\vdash \;\; \forall f\ w\ c.\ w_0 \models c \Rightarrow (w \models^{c} f = w \models \mathcal{T}^{c}(f))$

$\vdash \;\; \forall f\ w.\ w \models^{\mathbf{T}} f = w \models \mathcal{T}^{\mathbf{T}}(f)$

$\vdash \;\; \forall w\ f.\ w \models X!\, f \;=\; w \models \neg(\{\mathbf{T};\mathbf{T}\}(\mathbf{F})) \wedge \{\mathbf{T};\mathbf{T}\}(f)$

$\vdash \;\; \forall w\ r_1\ r_2.\ w \models \{r_1\} \mapsto \{r_2\}! \;=\; w \models \{r_1\}(\neg(\{r_2\}(\mathbf{F})))$

$\vdash \;\; w \models [f_1\ U\ f_2] \;=\; |w| > 0 \wedge (w \models f_2 \vee (w \models f_1 \wedge w^1 \models [f_1\ U\ f_2]))$

MJCG April 10, 2003