1: Nondeterministic while programs α

Program	Operation	Effect
$x \leftarrow e$	assignment	assigns value of term e to variable x
$?Q$	test	check truth of first-order formula Q in current state
$\alpha\ ;\ \beta$	sequential composition	β starts after α finishes
$\alpha \cup \beta$	nondeterministic choice	run either α or β
α^*	nondeterministic repetition	repeats α n-times for any $n \in \mathbb{N}$

2: Semantics of while programs α as a relation $\omega[\![\alpha]\!]\nu$ between prestates ω and poststates ν

$\omega[\![x \leftarrow e]\!]\nu$ iff $\omega[x \mapsto a] = \nu$ where $a = \omega[\![e]\!]$
$\omega[\![?Q]\!]\nu$ iff $\omega \models Q$ and $\omega = \nu$
$\omega[\![\alpha\ ;\ \beta]\!]\nu$ iff $\omega[\![\alpha]\!]\mu$ and $\mu[\![\beta]\!]\nu$ for some μ
$\omega[\![\alpha \cup \beta]\!]\nu$ iff $\omega[\![\alpha]\!]\nu$ or $\omega[\![\beta]\!]\nu$
$\omega[\![\alpha^*]\!]\nu$ iff $\omega[\![\alpha]\!]^n\nu$ for some $n \geq 0$

$\omega[\![\alpha]\!]^0\nu$ iff $\omega = \nu$
$\omega[\![\alpha]\!]^{n+1}\nu$ iff $\omega[\![\alpha]\!]\mu$ and $\mu[\![\alpha]\!]^n\nu$ for some μ

3: Semantics of Dynamic Logic formulas P in state ω

$\omega \models e_1 \geq e_2$ iff $\omega[\![e_1]\!] \geq \omega[\![e_2]\!]$
$\omega \models \neg P$ iff $\omega \not\models P$ that is, it is not the case that $\omega \models P$
$\omega \models P \wedge Q$ iff $\omega \models P$ and $\omega \models Q$
$\omega \models P \rightarrow Q$ iff $\omega \models P$ implies $\omega \models Q$
$\omega \models \exists x\, P$ iff $\omega[x \mapsto a] \models P$ for some integer a
$\omega \models \forall x\, P$ iff $\omega[x \mapsto a] \models P$ for all integers a
$\omega \models \langle\alpha\rangle P$ iff $\nu \models P$ for some state ν such that $\omega[\![\alpha]\!]\nu$
$\omega \models [\alpha]P$ iff $\nu \models P$ for all states ν such that $\omega[\![\alpha]\!]\nu$
$\omega \models \Box P$ iff $\nu \models P$ for all states ν

4: Selected dynamic logic axioms

$\langle\cdot\rangle$ $\boldsymbol{\langle\alpha\rangle P} \leftrightarrow \neg[\alpha]\neg P$

$[\leftarrow]$ $\boldsymbol{[x \leftarrow e]P(x)} \leftrightarrow (\forall x'.\, x' = e \rightarrow P(x'))$ (x' not in e or $P(x)$)

$[?]$ $\boldsymbol{[?Q]P} \leftrightarrow (Q \rightarrow P)$

$[\cup]$ $\boldsymbol{[\alpha \cup \beta]P} \leftrightarrow [\alpha]P \wedge [\beta]P$

$[;]$ $\boldsymbol{[\alpha;\beta]P} \leftrightarrow [\alpha][\beta]P$

I $\boldsymbol{[\alpha^*]P} \leftrightarrow P \wedge [\alpha^*](P \rightarrow [\alpha]P)$

5: Weakest Preconditions

$$
\begin{aligned}
wp(\alpha\ ;\ \beta)Q &= wp(\alpha)(wp(\beta)Q) \\
wp(\alpha \cup \beta)Q &= wp(\alpha)Q \wedge wp(\beta)Q \\
wp(?P)Q &= P \rightarrow Q \\
wp(\alpha^*)Q &= Q \wedge wp(\alpha)(wp(\alpha^*)Q) \\
wp(x \leftarrow e)Q(x) &= \forall x'.\, x' = e \rightarrow Q(x') \qquad (x' \notin e, Q(x))
\end{aligned}
$$

6: Strongest Postconditions

$$\begin{aligned}
sp(\alpha\,;\,\beta)P &= sp(\beta)(sp(\alpha)P)\\
sp(\alpha\cup\beta)P &= sp(\alpha)P \lor sp(\beta)P\\
sp(?Q)P &= Q \land P\\
sp(\alpha^*)P &= P \lor sp(\alpha^*)(sp(\alpha)P)\\
sp(x \leftarrow e(x))(P(x)) &= \exists x'.x = e(x') \land P(x') \quad (x' \notin e(x), P(x))
\end{aligned}$$

7: Sequent Calculus

$$\frac{}{\Gamma, P \vdash P, \Delta}\ id \qquad \frac{\Gamma \vdash P, \Delta \quad \Gamma, P \vdash \Delta}{\Gamma \vdash \Delta}\ cut$$

$$\frac{\Gamma, P \vdash \Delta}{\Gamma \vdash \neg P, \Delta}\ \neg R \qquad \frac{\Gamma \vdash P, \Delta}{\Gamma, \neg P \vdash \Delta}\ \neg L$$

$$\frac{\Gamma \vdash P, \Delta \quad \Gamma \vdash Q, \Delta}{\Gamma \vdash P \land Q, \Delta}\ \land R \qquad \frac{\Gamma, P, Q \vdash \Delta}{\Gamma, P \land Q \vdash \Delta}\ \land L$$

$$\frac{\Gamma \vdash P, Q, \Delta}{\Gamma \vdash P \lor Q, \Delta}\ \lor R \qquad \frac{\Gamma, P \vdash \Delta \quad \Gamma, Q \vdash \Delta}{\Gamma, P \lor Q \vdash \Delta}\ \lor L$$

$$\frac{\Gamma, P \vdash Q, \Delta}{\Gamma \vdash P \to Q, \Delta}\ {\to}R \qquad \frac{\Gamma \vdash P, \Delta \quad \Gamma, Q \vdash \Delta}{\Gamma, P \to Q \vdash \Delta}\ {\to}L$$

$$\frac{\Gamma \vdash P, P, \Delta}{\Gamma \vdash P, \Delta}\ contractionR \qquad \frac{\Gamma, P, P \vdash \Delta}{\Gamma, P \vdash \Delta}\ contractionL$$

$$\frac{\Gamma \vdash P(a), \Delta}{\Gamma \vdash \forall x.\, P(x), \Delta}\ \forall R^a \qquad \frac{\Gamma, P(e) \vdash \Delta}{\Gamma, \forall x.\, P(x) \vdash \Delta}\ \forall L$$

$$\frac{\Gamma \vdash P(e), \Delta}{\Gamma \vdash \exists x.\, P(x), \Delta}\ \exists R \qquad \frac{\Gamma, P(a) \vdash \Delta}{\Gamma, \exists x.\, P(x) \vdash \Delta}\ \exists L^a$$

8: Resolution

$$\frac{p \lor C \quad \neg p \lor D}{C \lor D}\ resolution$$

9: Equality Logic with Uninterpreted Functions

The theory of equality with uninterpreted functions has a signature that consists of a single binary predicate $=$, and all possible constant $(a, b, c, \ldots)$ and function $(f, g, h, \ldots)$ symbols:

$$\Sigma_{\mathsf{E}} : \{=, a, b, c, \ldots, f, g, h, \ldots\}$$

Axioms:

$$\begin{aligned}
&\forall x.x = x\\
&\forall x, y.x = y \to y = x\\
&\forall x, y, z.x = y \land y = z \to x = z\\
&\forall x, y.x = y \to f(\bar{x}) = f(\bar{y}) \text{ (congruence axiom)}
\end{aligned}$$

10: Semantics of Linear Temporal Logic (LTL)

The suffix of a trace σ starting at step $k \in \mathbb{N}$ is denoted σ^k and only defined if the trace has at least length k. That is

$$(\sigma_0, \sigma_1, \sigma_2, \dots, \sigma_{k-1}, \sigma_k, \sigma_{k+1}, \sigma_{k+2}, \dots)^k = (\sigma_k, \sigma_{k+1}, \sigma_{k+2}, \dots)$$

The truth of LTL formulas in a trace σ is defined inductively as follows:

(1) $\sigma \models F$ iff $\sigma_0 \models F$ for a state formula F provided that $\sigma_0 \neq \Lambda$
(2) $\sigma \models \neg P$ iff $\sigma \not\models P$, i.e. it is not the case that $\sigma \models P$
(3) $\sigma \models P \land Q$ iff $\sigma \models P$ and $\sigma \models Q$
(4) $\sigma \models \mathbf{X}P$ iff $\sigma^1 \models P$
(5) $\sigma \models \Box P$ iff $\sigma^i \models P$ for all $i \geq 0$
(6) $\sigma \models \Diamond P$ iff $\sigma^i \models P$ for some $i \geq 0$
(7) $\sigma \models P\,\mathbf{U}\,Q$ iff there is an $i \geq 0$ such that $\sigma^i \models Q$ and $\sigma^j \models P$ for all $0 \leq j < i$

In all cases, the truth-value of a formula is, of course, only defined if the respective suffixes of the traces are defined.

11: Kripke structure

A *Kripke frame* $(W, \curvearrowright)$ consists of:

- a set W of states;
- a transition relation $\curvearrowright \subseteq W \times W$ where $s \curvearrowright t$ indicates that there is a direct transition from s to t in the Kripke frame $(W, \curvearrowright)$.

A *Kripke structure* $K = (W, \curvearrowright, v, I)$ is:

- a Kripke frame $(W, \curvearrowright)$ with a mapping $v : W \to 2^V$, where 2^V is the powerset of V assigning truth-values to all the propositional atoms in all states;
- a Kripke structure has a set of initial states $I \subseteq W$.

12: Computation structure

A Kripke structure $K = (W, \curvearrowright, v, I)$ is called a *computation structure* if:

- W is a finite set of states;
- every element $s \in W$ has at least one direct successor $t \in W$ with $s \curvearrowright t$.

A (computation) *path* is an infinite sequence $s_0, s_1, s_2, s_3, \dots$ of states $s_i \in W$ such that $s_i \curvearrowright s_{i+1}$ for all i. We will always assume that the structures used in model checking are computation structures, unless otherwise noted.

13: Semantics of Computation Tree Logic (CTL)

In a fixed Kripke structure $K = (W, \curvearrowright, v)$, the truth of CTL formulas in state s is defined as follows:

(1) $s \models p$ iff $v(s)(p) = \mathit{true}$ for atomic propositions p
(2) $s \models \neg P$ iff $s \not\models P$, i.e. it is not the case that $s \models P$
(3) $s \models P \land Q$ iff $s \models P$ and $s \models Q$
(4) $s \models \mathbf{AX}P$ iff all successors t with $s \curvearrowright t$ satisfy $t \models P$
(5) $s \models \mathbf{EX}P$ iff at least one successor t with $s \curvearrowright t$ satisfies $t \models P$
(6) $s \models \mathbf{AG}P$ iff all paths $s_0, s_1, s_2, \dots$ starting in $s_0 = s$ satisfy $s_i \models P$ for all $i \geq 0$
(7) $s \models \mathbf{AF}P$ iff all paths $s_0, s_1, s_2, \dots$ starting in $s_0 = s$ satisfy $s_i \models P$ for some $i \geq 0$
(8) $s \models \mathbf{EG}P$ iff some path $s_0, s_1, s_2, \dots$ starting in $s_0 = s$ satisfies $s_i \models P$ for all $i \geq 0$
(9) $s \models \mathbf{EF}P$ iff some path $s_0, s_1, s_2, \dots$ starting in $s_0 = s$ satisfies $s_i \models P$ for some $i \geq 0$
(10) $s \models \mathbf{A}[P\,\mathbf{U}\,Q]$ iff all paths $s_0, s_1, s_2, \dots$ starting in $s_0 = s$ have some $i \geq 0$ such that $s_i \models Q$ and $s_j \models P$ for all $0 \leq j < i$
(11) $s \models \mathbf{E}[P\,\mathbf{U}\,Q]$ iff some path $s_0, s_1, s_2, \dots$ starting in $s_0 = s$ has some $i \geq 0$ such that $s_i \models Q$ and $s_j \models P$ for all $0 \leq j < i$

Given a Kripke structure K, we say that K satisfies P iff for all initial states s_0 of K, $s_0 \models P$.