The μ-calculus and model checking

[J. Bradfield and I. Walukiewicz, Handbook of MC]

<u>So far</u>: Linear-time properties

<u>Now</u>: Branching-time.

Syntax and Semantics:

<u>Transition systems</u> are potentially infinite graphs whose transitions are labeled by actions from $Act = \{a, b, c, \ldots\}$ and whose states are labeled by propositions from $Prop = \{p_1, p_2, \ldots\}$.

Formally,

$$M = (S, \{R_a\}_{a \in Act}, \{P_i\}_{i \in \mathbb{N}})$$

with $R_a \subseteq S \times S$ and $P_i \subseteq S$.

<u>Syntax</u>:

Let $Var = \{X, Y, Z, \ldots\}$ be a countable set of variables that will denote sets of states.

The set Fmc of μ-calculus formulas α is defined by

$$\alpha ::= p \mid \neg p \mid X \mid \alpha_1 \wedge \alpha_2 \mid \alpha_1 \vee \alpha_2$$
$$\mid \langle a \rangle \alpha \mid [a]\alpha \mid \mu X. \alpha \mid \nu X. \alpha$$

<u>Convention</u>: $\langle a \rangle$ and $[a]$ bind stronger than Boolean connectives.

<u>Example</u>: Infinitely often p on some path:

$$\nu Y. (\mu X. ((p \wedge \langle a \rangle Y) \vee \langle a \rangle X))$$

We write this as

$$\nu Y. \mu X. (p \wedge \langle a \rangle Y) \vee \langle a \rangle X.$$

We write · $\sigma X.\alpha$ for $\mu X.\alpha$ or $\nu X.\alpha$

· tt for $p_1 \vee \neg p_1$

· ff for $p_1 \wedge \neg p_1$.

Semantics:

The meaning of a formula in a transition system is the set of states satisfying the formula.

Definition:

Given a transition system $\mathcal{M} = (S, \{R_a\}_{a \in Act}, \{P_i\}_{i \in PV})$ and a valuation $v : Vars \longrightarrow \mathbb{P}(S)$, the meaning of formulas $\llbracket \alpha \rrbracket_v^{\mathcal{M}}$ is defined by induction:

$$\llbracket X \rrbracket_v^{\mathcal{M}} := v(X)$$

$$\llbracket p_i \rrbracket_v^{\mathcal{M}} := P_i \qquad \llbracket \neg P_i \rrbracket_v^{\mathcal{M}} := S \setminus P_i$$

$$\llbracket \alpha_1 \underset{\vee}{\wedge} \alpha_2 \rrbracket_v^{\mathcal{M}} := \llbracket \alpha_1 \rrbracket_v^{\mathcal{M}} \underset{\cup}{\cap} \llbracket \alpha_2 \rrbracket_v^{\mathcal{M}}$$

// there is an a-transition $\quad \llbracket \langle a \rangle \alpha \rrbracket_v^{\mathcal{M}} := \{ s \in S \mid \exists s'.\ R_a(s,s') \wedge s' \in \llbracket \alpha \rrbracket_v^{\mathcal{M}} \}$

$$\llbracket [a] \alpha \rrbracket_v^{\mathcal{M}} := \{ s \in S \mid \forall s'.\ R_a(s,s') \Rightarrow s' \in \llbracket \alpha \rrbracket_v^{\mathcal{M}} \}.$$

To define the semantics of fixed point operators, we understand a formula $\alpha(X)$ with free variable X as an operator

$$\alpha(X) : \mathbb{P}(X) \longrightarrow \mathbb{P}(X)$$
$$S' \longmapsto \llbracket \alpha \rrbracket_{v[X \mapsto S']}^{\mathcal{M}}.$$

This operator is monotonic, so we can rely on Knaster-Tarski.

$$[\![\mu X.\alpha]\!]^M_v := \bigcap \{ S' \subseteq S \mid [\![\alpha]\!]^M_{v[X\mapsto S']} \subseteq S' \}$$

// Meet over all prefix points,
so $\mu X.\alpha$ is the lfp of α.

$$[\![\nu X.\alpha]\!]^M_v := \bigcup \{ S' \subseteq S \mid S' \subseteq [\![\alpha]\!]^M_{v[X\mapsto S']} \}.$$

We also write $M, s, v \models \alpha$ for $s \in [\![\alpha]\!]^M_v$.

Examples:

(1) There is an a-labeled transition: $\langle a \rangle tt$.

(2) Termination, all sequences of a-transitions are finite: $\mu X.[a]X$.

(3) Non-termination, there is an infinite sequence of a-transitions: $\nu X.\langle a \rangle X$.

Note that (2) and (3) only need one fixed point.

(4) There is an infinite sequence of a-transitions and all states on the sequence satisfy p: $\nu Y.\ p \wedge \langle a \rangle Y$.

(5) $\mu X.\langle a \rangle X$ is false.
Why? The empty set is a prefix point:

$$[\![\langle a \rangle X]\!]^M_{[X\mapsto \emptyset]} = \{ s \in S \mid \exists s'.\ R_a(s,s') \wedge s' \in \emptyset \}$$
$$= \emptyset \subseteq \emptyset.$$

(6) There is a sequence of a-transitions to a state where p holds: $\mu X.\ p \vee \langle a \rangle X$.

(7) Two fixed points allow us to define fairness:
On some a-path there are infinitely many states where p holds: $\nu Y.\mu X.(p \wedge \langle a \rangle Y) \vee \langle a \rangle X$

(8) On some a-path, <u>almost</u> <u>always</u> p holds:

$$\mu X.\, \nu Y.\, (p \wedge \langle a \rangle Y) \vee \langle a \rangle X$$

// The fixed points are swapped between (7) and (8).

To see why $\mu X. [a] X$ holds
if all paths are finite, consider

$$M \qquad \begin{tikzcd}[row sep=small] & s_1 \\ s \arrow[ur, "a"] \arrow[dr, "a"'] & \\ & s_2 \end{tikzcd}$$

- We check whether $\emptyset$ can be a prefix point:

$$\llbracket [a] X \rrbracket^{M}_{[X \mapsto \emptyset]}$$
$$= \{ s \in S \mid \forall s'.\, R_a(s,s') \Rightarrow s' \in \emptyset \}$$
$$= \{ s_1, s_2 \} \not\subseteq \emptyset.$$

- We check $\{s_1, s_2\}$:

$$\llbracket [a] X \rrbracket^{M}_{[X \mapsto \{s_1, s_2\}]}$$
$$= \{ s \in S \mid \forall s'.\, R_a(s,s') \Rightarrow s' \in \{s_1, s_2\} \}$$
$$= \{ s, s_1, s_2 \} \not\subseteq \{ s_1, s_2 \}$$

- The least fixed point actually is $\{s, s_1, s_2\}$.

Why do formulas mean what they mean?
We will introduce alternative semantics to understand them.