Topics in Concurrency
Lectures 5

Glynn Winskel

30 January 2020
Logics for specifying correctness properties. We’ll look at:

- Basic logics and bisimilarity
- Fixed points and logic
- CTL
- Model checking
Finitary Hennessy-Milner Logic

Assertions:

\[ A ::= T \mid F \mid A_0 \land A_1 \mid A_0 \lor A_1 \mid \neg A \mid \langle \lambda \rangle A \mid \langle - \rangle A \mid [\lambda]A \mid [-]A \]

Satisfaction: \( s \models A \)

- \( s \models T \) always
- \( s \models F \) never
- \( s \models A_0 \land A_1 \) if \( s \models A_0 \) and \( s \models A_1 \)
- \( s \models A_0 \lor A_1 \) if \( s \models A_0 \) or \( s \models A_1 \)
- \( s \models \neg A \) if not \( s \models A \)
- \( s \models \langle \lambda \rangle A \) if there exists \( s' \) s.t. \( s \xrightarrow{\lambda} s' \) and \( s' \models A \)
- \( s \models \langle - \rangle A \) if there exist \( s', \lambda \) s.t. \( s \xrightarrow{\lambda} s' \) and \( s' \models A \)
- \( s \models [\lambda]A \) iff for all \( s' \) s.t. \( s \xrightarrow{\lambda} s' \) have \( s' \models A \)
- \( s \models [-]A \) iff for all \( s', \lambda \) s.t. \( s \xrightarrow{\lambda} s' \) have \( s' \models A \)

Alternatively, derived assertions

\[ [\lambda]A \equiv -\langle \lambda \rangle \neg A \quad [-]A \equiv -\langle - \rangle \neg A \]
Examples

? s ⊨ ⟨a⟩T ?
? s ⊨ [a]T ?
? u ⊨ [−]F ?
? s ⊨ ⟨a⟩⟨b⟩T ?
? s ⊨ [a]⟨b⟩T ?
Examples

Generally:

- $\langle a \rangle T$
- $[a] F$
- $\langle \neg \rangle F$
- $\langle \neg \rangle T$
- $[\neg] T$
- $[\neg] F$
A non-finitary Hennessy-Milner logic allows an infinite conjunction

\[ A ::= \bigwedge_{i \in I} A_i \mid \neg A \mid (\lambda)A \]

with semantics

\[ s \models \bigwedge_{i \in A} A_i \text{ iff } s \models A_i \text{ for all } i \in I \]

Define

\[ p \preceq q \text{ iff for all assertions } A \text{ of H-M logic} \]
\[ p \models A \text{ iff } q \models A \]

**Theorem**

\[ \preceq = \sim \]

This gives a way to demonstrate non-bisimilarity of states
The finitary H-M logic doesn’t allow properties such as the process never deadlocks.

We can add particular extensions (such as always, never) to the logic (CTL).

Alternatively, what about defining sets of states ‘recursively’? The set of states $X$ that can always do some action satisfies:

$$X = \langle-\rangle \top \land \lbrack -\rbrack X$$

A fixed point equation: $X = \varphi(X)$

But such equations can have many solutions...
In general, an equation of the form $X = \varphi(X)$ can have many solutions for $X$.

Fixed points are important: they represent steady or consistent states.

Range of different fixed point theorems applicable in different contexts e.g.

**Theorem (1-dimensional Brouwer’s fixed point theorem)**

*Any continuous function $f : [0, 1] \rightarrow [0, 1]$ has at least one fixed point*

(used e.g. in proof of existence of Nash equilibria)

We’ll be interested in fixed points of functions on the powerset lattice $\rightarrow$ Knaster-Tarski fixed point theorem and least and greatest fixed points
In the above transition system, what are the least and greatest subsets of states $X$, $Y$ and $Z$ that satisfy:

\[
X = X
\]

\[
Y = (\neg T \land \neg Y)
\]

\[
Z = \neg Z
\]
The powerset lattice

- Given a set $S$, its powerset is
  \[ \mathcal{P}(S) = \{ S \mid S \subseteq S \} \]

- Taking the order on its elements to be inclusion, $\subseteq$, this forms a complete lattice

We are interested in fixed points of functions of the form

\[ \varphi : \mathcal{P}(S) \to \mathcal{P}(S) \]

- \( \varphi \) is monotonic if $S \subseteq S'$ implies $\varphi(S) \subseteq \varphi(S')$
- a prefixed point of $\varphi$ is a set $X$ satisfying $\varphi(X) \subseteq X$
- a postfixed point of $\varphi$ is a set $X$ satisfying $X \subseteq \varphi(X)$
Knaster-Tarski fixed point theorem for minimum fixed points

**Theorem**

For monotonic $\varphi : \mathcal{P}(S) \to \mathcal{P}(S)$, define

$$m = \bigcap \{X \subseteq S \mid \varphi(X) \subseteq X\}.$$

Then $m$ is a fixed point of $\varphi$ and, furthermore, is the least prefixed point:

1. $m = \varphi(m)$
2. $\varphi(X) \subseteq X$ implies $m \subseteq X$

$m$ is conventionally written

$$\mu X. \varphi(X)$$

Used for inductive definitions: syntax, operational semantics, rule-based programs, model checking
Knaster-Tarski fixed point theorem for maximum fixed points

Theorem

For monotonic \( \varphi : \mathcal{P}(S) \to \mathcal{P}(S) \), define

\[
M = \bigcup \{ X \subseteq S \mid X \subseteq \varphi(X) \}.
\]

Then \( M \) is a fixed point of \( \varphi \) and, furthermore, is the greatest postfixed point.

1. \( M = \varphi(M) \)
2. \( X \subseteq \varphi(X) \) implies \( X \subseteq M \)

\( M \) is conventionally written

\[
\nu X. \varphi(X)
\]

Used for co-inductive definitions, bisimulation, model checking
(Strong) bisimilarity as a maximum fixed point \[\S 5.2 \text{ p}68\]

Bisimilarity can be viewed as a fixed point \(\sim\) model checking algorithms.

Given a relation \(R\) (on CCS processes or states of transition systems) define:

\[
p \varphi(R) q
\]

iff

1. \(\forall \alpha, p'.\quad p \xrightarrow{\alpha} p' \implies \exists q'.\quad q \xrightarrow{\alpha} q' \land p' R q'

2. \(\forall \alpha, q'.\quad q \xrightarrow{\alpha} q' \implies \exists p'.\quad p \xrightarrow{\alpha} p' \land p' R q'

**Lemma**

\(R \subseteq \varphi(R)\) iff \(R\) is a (strong) bisimulation.

Hence, by Knaster-Tarski fixed point theorem for maximum fixed points:

**Theorem**

Bisimilarity is the greatest fixed point of \(\varphi\).
Theorem

Bisimilarity is the greatest fixed point of $\varphi$.

Proof.

\[ \sim = \bigcup \{ R \mid R \text{ is a bisimulation} \} \tag{1} \]
\[ = \bigcup \{ R \mid R \subseteq \varphi(R) \} \tag{2} \]
\[ = \nu X. \varphi(X) \tag{3} \]

(1) is by definition of $\sim$
(2) is by Lemma
(3) is by Knaster-Tarski for maximum fixed points: note that $\varphi$ is monotonic

Question: How is this different from the least fixed point of $\varphi$?
The modal $\mu$-calculus [§4.2 p48]

$$A ::= T \mid F \mid A_0 \land A_1 \mid A_0 \lor A_1 \mid \neg A \mid (\lambda)A \mid (\neg)A \mid X \mid \nu X.A$$

To guarantee monotonicity (and therefore the existence of the fixed point), require the variable $X$ to occur only positively in $A$ in $\nu X.A$. That is, $X$ occurs only under an even number of $\neg$s.

$s \models \nu X.A$ \iff $s \in \nu X.A$

\[s \in \bigcup \{ S \subseteq \mathcal{P} \mid S \subseteq A[S/X]\}\]

the maximum fixed point of the monotonic function $S \mapsto A[S/X]$

As before, we take

$$[\lambda]A \equiv \neg(\lambda)\neg A \quad [-]A \equiv \neg(\neg)\neg A$$

Now also take

$$\mu X.A \equiv \neg \nu X.(\neg A[\neg X/X])$$
Example

Consider the process

\[ P \overset{\text{def}}{=} a.(a.P + b.c.\text{nil}) \]

Which states satisfy

- \( \mu X.(a)X \)
- \( \nu X.(a)X \)
- \( \mu X.[a]X \)
- \( \nu X[a]X \)
Approximants

Let $\varphi : \mathcal{P}(S) \rightarrow \mathcal{P}(S)$ be monotonic. $\varphi$ is $\cap$-continuous iff for all decreasing chains $X_0 \supseteq X_1 \supseteq \ldots \supseteq X_n \supseteq \ldots$

$$\bigcap_{n \in \omega} \varphi(X_n) = \varphi\left(\bigcap_{n \in \omega} X_n\right)$$

If the set of states $S$ is finite, continuity certainly holds.

Theorem

If $\varphi : \mathcal{P}(S) \rightarrow \mathcal{P}(S)$ is $\cap$-continuous:

$$\nu X. \varphi(X) = \bigcap_{n \in \omega} \varphi^n(S)$$
Let $\phi : \mathcal{P}(S) \to \mathcal{P}(S)$ be monotonic. $\phi$ is $\bigcup$-continuous iff for all increasing chains $X_0 \subseteq X_1 \subseteq \ldots \subseteq X_n \subseteq \ldots$

$$\bigcup_{n \in \omega} \phi(X_n) = \phi \left( \bigcup_{n \in \omega} X_n \right)$$

If the set of states $S$ is finite, continuity certainly holds

**Theorem**

If $\phi : \mathcal{P}(S) \to \mathcal{P}(S)$ is $\bigcup$-continuous:

$$\mu X. \phi(X) = \bigcup_{n \in \omega} \phi^n(\emptyset)$$
Proposition

\[ s \models \mu X.\langle a\rangle T \lor \langle \neg \rangle X \] in any transition system iff there exists a sequence of transitions from \( s \) to a state \( t \) where an \( a \)-action can occur.
Proposition

$s \models \nu X.\langle a \rangle X$ in a finite-state transition system iff there exists an infinite sequence of $a$-transitions from $s$.

There are infinite-state transition systems where $\varphi(X) = \langle a \rangle X$ is not \cap-continuous.
For finite-state processes, modal-$\mu$ can be encoded in infinitary H-M logic

if finite-state processes $p$ and $q$ are bisimilar then they satisfy the same modal-$\mu$ assertions

Note that logical equivalence in modal-$\mu$ does not generally imply bisimilarity (due to the lack of infinitary conjunction)