Topics in Concurrency

Lecture 7

Jonathan Hayman

29 January 2016

Fixed points and model checking

- 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:

$$X = \langle - \rangle T \wedge [-]X$$

Fixed points and model checking

- 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:

$$X = \langle - \rangle T \wedge [-] X$$

- A fixed point equation: $X = \varphi(X)$
- But such equations can have many solutions...

Fixed point equations

- 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.

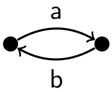
Theorem (1-dimensional Brouwer's fixed point theorem)

Any continuous function $f : [0,1] \to [0,1]$ *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 ⇝ Knaster-Tarski fixed point theorem and least and greatest fixed points

Least and greatest fixed points on transition systems: examples



In the above transition system, what are the least and greatest subsets of states X, Y and Z that satisfy:

$$X = X$$

$$Y = \langle - \rangle T \wedge [-] Y$$

$$Z = \neg Z$$

The powerset lattice

- Given a set $\mathcal{S}$, its powerset is

$$\mathcal{P}(\mathcal{S}) = \{S \mid S \subseteq \mathcal{S}\}$$

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

The powerset lattice

- Given a set $\mathcal{S}$, its powerset is

$$\mathcal{P}(\mathcal{S}) = \{S \mid S \subseteq \mathcal{S}\}$$

- 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

$$\varphi : \mathcal{P}(\mathcal{S}) \to \mathcal{P}(\mathcal{S})$$

- φ is monotonic if $S \subseteq S'$ implies $\varphi(S) \subseteq \varphi(S')$
- a prefixed point of φ is a set X satisfying $\varphi(X) \subseteq X$
- a postfixed point of φ is a set X satisfying $X \subseteq \varphi(X)$

Knaster-Tarski fixed point theorem for minimum fixed points

Theorem

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

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

Then m *is a fixed point of* φ *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 $\varphi : \mathcal{P}(\mathcal{S}) \to \mathcal{P}(\mathcal{S})$, *define*

$$M = \bigcup \{ X \subseteq \mathcal{S} \mid X \subseteq \varphi(X) \}.$$

Then M *is a fixed point of* φ *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 [§5.2 p68]

Bisimilarity can be viewed as a fixed point ⇝ model checking algorithms.

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

$$p \; \varphi(R) \; q$$

iff

1. $\forall \alpha, p'. \quad p \xrightarrow{\alpha} p' \quad \Longrightarrow$
   $\exists q'. \quad q \xrightarrow{\alpha} q' \quad \& \quad p' \; R \; q'$
2. $\forall \alpha, q'. \quad q \xrightarrow{\alpha} q' \quad \Longrightarrow$
   $\exists p'. \quad p \xrightarrow{\alpha} p' \quad \& \quad p' \; R \; q'$

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 φ.

Theorem

Bisimilarity is the greatest fixed point of φ.

Proof.

$$\begin{aligned} \sim \quad &= \quad \bigcup\{R \mid R \text{ is a bisimulation}\} && (1) \\ &= \quad \bigcup\{R \mid R \subseteq \varphi(R)\} && (2) \\ &= \quad \nu X.\varphi(X) && (3) \end{aligned}$$

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

$\square$

Theorem

Bisimilarity is the greatest fixed point of φ.

Proof.

$$
\begin{aligned}
\sim \quad &= \quad \bigcup\{R \mid R \text{ is a bisimulation}\} && (1)\\
&= \quad \bigcup\{R \mid R \subseteq \varphi(R)\} && (2)\\
&= \quad \nu X.\varphi(X) && (3)
\end{aligned}
$$

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

$\square$

Question: How is this different from the least fixed point of φ?

The modal μ-calculus [§4.2 p48]

$$A ::= T \mid F \mid A_0 \wedge A_1 \mid A_0 \vee A_1 \mid \neg A \mid \langle\lambda\rangle A \mid \langle - \rangle A \mid \nu X.A$$

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.

$$\begin{array}{lll} s \models \nu X.A & \text{iff} & s \in \nu X.A \\ & \text{i.e.} & s \in \bigcup\{S \subseteq \mathcal{P} \mid S \subseteq A[S/X]\} \\ & & \text{the maximum fixed point of the monotonic} \\ & & \text{function } S \mapsto A[S/X] \end{array}$$

The modal μ-calculus [§4.2 p48]

$$A ::= T \mid F \mid A_0 \wedge A_1 \mid A_0 \vee A_1 \mid \neg A \mid \langle \lambda \rangle A \mid \langle - \rangle A \mid \nu X.A$$

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.

$$\begin{array}{lll} s \models \nu X.A & \text{iff} & s \in \nu X.A \\ & \text{i.e.} & s \in \bigcup \{ S \subseteq \mathcal{P} \mid S \subseteq A[S/X] \} \\ & & \text{the maximum fixed point of the monotonic} \\ & & \text{function } S \mapsto A[S/X] \end{array}$$

As before, we take

$$[\lambda]A \equiv \neg \langle \lambda \rangle \neg A \qquad [-]A \equiv \neg \langle - \rangle \neg A$$

Now also take

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

Example

Consider the process

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

Which states satisfy

- $\mu X.\langle a\rangle X$
- $\nu X.\langle a\rangle X$
- $\mu X.[a]X$
- $\nu X[a]X$

Approximants

Let $\varphi : \mathcal{P}(\mathcal{S}) \to \mathcal{P}(\mathcal{S})$ be monotonic.
φ is $\bigcap$-continuous iff for all decreasing chains $X_0 \supseteq X_1 \supseteq \cdots \supseteq X_n \supseteq \cdots$

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

If the set of states $\mathcal{S}$ is finite, continuity certainly holds

Theorem

If $\varphi : \mathcal{P}(\mathcal{S}) \to \mathcal{P}(\mathcal{S})$ *is* $\bigcap$*-continuous:*

$$\nu X.\varphi(X) = \bigcap_{n \in \omega} \varphi^n(\mathcal{S})$$

Approximants

Let $\varphi : \mathcal{P}(\mathcal{S}) \to \mathcal{P}(\mathcal{S})$ be monotonic.
φ is $\bigcup$-continuous iff for all increasing chains $X_0 \subseteq X_1 \subseteq \cdots \subseteq X_n \subseteq \cdots$

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

If the set of states $\mathcal{S}$ is finite, continuity certainly holds

Theorem

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

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

Proving interpretations

Proposition

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

Bisimilarity and modal μ

For finite-state processes, modal-μ can be encoded in infinitary H-M logic

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

Bisimilarity and modal μ

For finite-state processes, modal-μ can be encoded in infinitary H-M logic

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

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