Modal and Temporal Logics

Colin Stirling
School of Informatics
University of Edinburgh

July 25, 2003
Summary: Temporal Operators as Fixed Points

1. $E(\Phi U \Psi) \equiv \Psi \lor (\Phi \land \langle - \rangle E(\Phi U \Psi))$

2. $A(\Phi U \Psi) \equiv \Psi \lor (\Phi \land \langle - \rangle tt \land [-] A(\Phi U \Psi))$

Syntactically: property $X$ such that

1. $X \equiv \Psi \lor (\Phi \land \langle - \rangle X)$

2. $X \equiv \Psi \lor (\Phi \land \langle - \rangle tt \land [-] X)$
Summary: Temporal Operators as Fixed points

Semantically: set of states $S = f(S)$ where $f$ is

1. $\lambda x.\| \psi \lor (\phi \land \langle \neg \rangle x) \|

2. $\lambda x.\| \psi \lor (\phi \land \langle \neg \rangle tt \land [-] x) \|

If $S = f(S)$ then $S$ is a fixed point of $f$.

In both cases $f$ is monotonic: $S \subseteq S' \rightarrow f(S) \subseteq f(S')$

$f$ is essentially modal (using $\langle \neg \rangle$ and $[-]$).
Summary: Fixed points

$S$ is a **prefix fixed point** of $f$, if $f(S) \subseteq S$

$S$ is a **postfix fixed point** of $f$, if $S \subseteq f(S)$

**Proposition**  If $f$ is monotonic (w.r.t $\subseteq$) then $f$

1. has a **least** fixed point, $\bigcap\{S : f(S) \subseteq S\}$

2. has a **greatest** fixed point, $\bigcup\{S : S \subseteq f(S)\}$
Exercise

What property is defined by the following fixed points?

1. \( X \equiv \Phi \vee \langle \neg \rangle X \) least \hspace{1cm} \text{Answer: E F } \Phi

2. \( X \equiv \Phi \wedge \langle \neg \rangle X \) greatest

3. \( X \equiv \Phi \wedge [\neg][\neg]X \) greatest
A Scheduler

Problem: assume $n$ tasks when $n > 1$.

$a_i$ initiates the $i$th task and $b_i$ signals its completion

The scheduler plans the order of task initiation, ensuring

1. actions $a_1 \ldots a_n$ carried out cyclically and tasks may terminate in any order

2. but a task can not be restarted until its previous operation has finished. ($a_i$ and $b_i$ happen alternately for each $i$.)

More complex temporal properties. Not expressible in CTL* (“not first order” but are “regular”).

Expressible using fixed points
Modal Logic

$Z$ ranges over propositional variables

$$\Phi ::= Z \mid \top \mid \bot \mid \Phi_1 \land \Phi_2 \mid \Phi_1 \lor \Phi_2 \mid [K]\Phi \mid \langle K \rangle \Phi$$

- $\models$ refined to $\models_V$ where $V$ is a valuation that assigns a set of states $V(X)$ to each variable $X$

$$E \models_V X \text{ iff } E \in V(X)$$

- $\parallel \Phi \parallel$ refined too: $\parallel \Phi \parallel_V = \{E : E \models_V \Phi\}$

- $V[S/X]$ is valuation $V'$ like $V$ except $V'(X) = S$. 
Modal Logic + II

**Proposition** The function $\lambda x.\| \Phi \|_{V[x/X]}$ is monotonic for any modal $\Phi$.

- If $\neg$ explicitly in logic then above not true: $\neg X: \lambda x. \neg x$ not monotonic.

  However, define when $\Phi$ is **positive** in $X$: if $X$ occurs within an even number of negations in $\Phi$

**Proposition** If $\Phi$ is positive in $X$ then $\lambda x.\| \Phi \|_{V[x/X]}$ is monotonic.

1. Property given by **least** fixed point of $\lambda x.\| \Phi \|_{V[x/X]}$ is written $\mu X. \Phi$.

2. Property given by **greatest** fixed point of $\lambda x.\| \Phi \|_{V[x/X]}$ is written $\nu X. \Phi$.

Alternative basis for temporal logic: **modal logic + fixed points**
Modal $\mu$-calculus

Syntax

$\Phi ::= \text{tt} \mid \text{ff} \mid Z \mid \Phi_1 \land \Phi_2 \mid \Phi_1 \lor \Phi_2 \mid [K]\Phi \mid \langle K \rangle \Phi \mid \nu Z. \Phi \mid \mu Z. \Phi$

- let $\sigma$ range over the set \{\$\mu,\nu\}.

- An occurrence of $Z$ is free within $\Phi$ if it is not within the scope of an occurrence of $\sigma Z$. $\sigma Z$ in $\sigma Z. \Phi$ binds free occurrences of $Z$ in $\Phi$.

- Formulas may have multiple fixed points: $\nu Z. \mu Y. ([b] Y \land [K] Z)$

- $\sigma Z$ may bind more than one occurrence of $Z$: $\nu Z. \langle \text{tick} \rangle Z \land \langle \text{tock} \rangle Z$. 
### Semantics

\[ E \models_\Gamma \top \]  
\[ E \not\models_\Gamma \bot \]  
\[ E \models_\Gamma \land \Psi \quad \text{iff} \quad E \models_\Gamma \Phi \text{ and } E \models_\Gamma \Psi \]  
\[ E \models_\Gamma \lor \Psi \quad \text{iff} \quad E \models_\Gamma \Phi \text{ or } E \models_\Gamma \Psi \]  
\[ E \models_\Gamma [K] \Phi \quad \text{iff} \quad \forall F \in \{ E' : E \stackrel{a}{\to} E' \text{ and } a \in K \}. F \models_\Gamma \Phi \]  
\[ E \models_\Gamma \langle K \rangle \Phi \quad \text{iff} \quad \exists F \in \{ E' : E \stackrel{a}{\to} E' \text{ and } a \in K \}. F \models_\Gamma \Phi \]  
\[ E \models_\Gamma \nu Z. \Phi \quad \text{iff} \quad E \in \bigcup \{ S : S \subseteq \| \Phi \|_{\Gamma[S/Z]} \} \]  
\[ E \models_\Gamma \mu Z. \Phi \quad \text{iff} \quad E \in \bigcap \{ S : \| \Phi \|_{\Gamma[S/Z]} \subseteq S \} \]

If \( f \) is monotonic (w.r.t \( \subseteq \)) then \( \bigcap \{ S : f(S) \subseteq S \} \) is **least** fixed point and \( \bigcup \{ S : S \subseteq f(S) \} \) is **greatest** fixed point of \( f \).
Semantics II

A slightly different presentation of the clauses for the fixed points dispenses with explicit use of sets $\| \Phi \|_\nu$.

$$
E \models \nu Z. \Phi \quad \text{iff} \quad \exists S. \; E \in S \; \text{and} \; \forall F \in S. \; F \models_{\nu[S/Z]} \Phi \\
E \models \mu Z. \Phi \quad \text{iff} \quad \forall S. \; \text{if} \; E \not\in S \; \text{then} \; \exists F \not\in S. \; F \models_{\nu[S/Z]} \Phi
$$

Looks second-order because of quantification over sets. Better: $1\frac{1}{2}$-order

If $\Phi$ does not contain free variables omit index $V$: $E \models \Phi$
Variant

Define modal $\mu$-calculus on Kripke models

Syntax

$\Phi ::= p \mid \neg p \mid Z \mid \Phi_1 \land \Phi_2 \mid \Phi_1 \lor \Phi_2 \mid [\neg] \Phi \mid \langle \neg \rangle \Phi \mid \nu Z. \Phi \mid \mu Z. \Phi$

$$
E \models \neg p \quad \text{iff} \quad E \notin L(p)
$$

$$
E \models \land p \quad \text{iff} \quad E \in L(p)
$$
Unfolding

- An unfolding of $\sigma Z. \Phi$ is $\Phi\{\sigma Z.\Phi/Z\}$
- Unfolding of $\nu Z. (-)Z$ is $(-)(\nu Z. (-)Z)$.
- Proposition $E \models_{\nu} \sigma Z.\Phi$ iff $E \models_{\nu} \Phi\{\sigma Z.\Phi/Z\}$. 
Expressiveness I

Modal $\mu$-calculus contains LTL, CTL, CTL$^*$

It also contains Propositional Dynamic Logic (PDL). PDL is modal logic when there is some structure on labels $A$: closed under operations $+$, $;$ and $^*$

\[
E \xrightarrow{w+v} F \iff E \xrightarrow{w} F \text{ or } E \xrightarrow{v} F \\
E \xrightarrow{w;v} F \iff E \xrightarrow{w} E_1 \xrightarrow{v} F \text{ for some } E_1 \\
E \xrightarrow{w^*} F \iff E = F \text{ or } E \xrightarrow{w} E_1 \xrightarrow{w} \ldots \xrightarrow{w} E_n \xrightarrow{w} F \text{ for some } n \geq 0 \text{ and } E_1, \ldots, E_n
\]
Exercise

What properties are expressed by the following formulas?

1. $\mu Z. [-]Z$

2. $\nu Z. [-](\text{tick})Z$

3. $\nu Z. (\text{tick})Z \land (\text{tock})Z$

4. $\mu Z. \nu Y. [a]Z \land [-a]Y$

5. $\nu Z. (\mu X. [b](\nu Y. [c](\nu Y_1. X \land [-a]Y_1) \land [-a]Y) \land [-]Z)$
Bisimulation Invariance

\[ E \equiv F \text{ if for all closed modal } \mu\text{-calculus formulas } \Phi, \ E \models \Phi \text{ iff } F \models \Phi. \]

**Proposition** if \( E \sim F \) then \( E \equiv F \)
Exercise

Express the following properties in modal $\mu$-calculus

1. Eventually either tick happens or $\Phi$ becomes true

2. In some run $\Phi$ is always true

3. tick happens until $\Phi$

4. tick happens until tock happens

5. In exactly three runs, $\Phi$ is true
Expressiveness II

**Proposition** Modal $\mu$-calculus equals bisimulation invariant properties expressible in monadic 2nd-order logic of transition graphs/Kripke models.

**Bisimulation invariant property:** if $E$ has property and $E \sim F$ then $F$ has the property
Fixed points

Assume $g$ is monotonic

least fixed point  $\mu g = \bigcap \{S : g(S) \subseteq S\}$
greatest fixed point $\nu g = \bigcup \{S : S \subseteq g(S)\}$
Approximants I

Let $\nu^i g$ for $i \geq 0$ be defined as follows where $S'$ is the set of states of the transition system $\nu^0 g = S'$ and $\nu^{i+1} g = g(\nu^i g)$.

- $\nu^{i+1} g \subseteq \nu^i g$ for all $i$

- Moreover, $\nu g \subseteq \nu^i g$ for all $i$

\[
\begin{align*}
\nu^0 g & \supseteq \nu^1 g \supseteq \ldots \supseteq \nu^i g \supseteq \ldots \\
\nu g & \cup \nu g \cup \ldots \cup \nu g \cup \ldots
\end{align*}
\]

- If $\nu^i g = \nu^{i+1} g$, then $\nu g$ is $\nu^i g$
Approximants II

- If $S'$ is not a finite set, then use ordinals $0, 1, \ldots, \omega, \omega + 1, \ldots, \omega + \omega, \omega + \omega + 1, \ldots$

- $\omega$ is the initial limit ordinal

- $\nu^0 g = S'$ and $\nu^{\alpha+1} g = g(\nu^\alpha g)$ and if $\lambda$ is a limit ordinal

\[
\nu^\lambda g = \bigcap \{\nu^\alpha g : \alpha < \lambda\}
\]
Approximants III

\[\nu^0 g \supseteq \ldots \supseteq \nu^\omega g \supseteq \nu^{\omega+1} g \supseteq \ldots\]

\[\nu g \ldots \nu g \ldots \]

The fixed point \(\nu g\) appears somewhere in the sequence, at the first point when \(\nu^\alpha g = \nu^{\alpha+1} g\)
Approximants IV

- $\mu^0 g = \emptyset$ and $\mu^{\alpha+1} g = g(\mu^\alpha g)$ and $\mu^\lambda g = \bigcup \{\mu^\alpha g : \alpha < \lambda\}$

- There is the following possibly increasing sequence of sets.

\[
\begin{align*}
\mu^g & \quad \cdots \quad \mu^g & \quad \mu^g & \quad \cdots \\
\cup & \quad \cup & \quad \cup & \quad \cup \\
\mu^0 g & \subseteq \cdots \subseteq \mu^\omega g & \subseteq \mu^{\omega+1} g & \subseteq \cdots
\end{align*}
\]

- The first time $\mu^\alpha g = \mu^{\alpha+1} g$ is $\mu^g$
Syntactic Approximants

\( \nu Z^0 . \Phi \ = \ \text{tt} \)
\( \nu Z^{\alpha + 1} . \Phi \ = \ \Phi\{\nu Z^\alpha . \Phi \mid Z\} \)
\( \nu Z^\lambda . \Phi \ = \ \bigwedge \{\nu Z^\alpha . \Phi : \alpha < \lambda\} \)
\( \mu Z^0 . \Phi \ = \ \text{ff} \)
\( \mu Z^{\alpha + 1} . \Phi \ = \ \Phi\{\mu Z^\alpha . \Phi \mid Z\} \)
\( \mu Z^\lambda . \Phi \ = \ \bigvee \{\mu Z^\alpha . \Phi : \alpha < \lambda\} \)

**Proposition**

1. If \( E \models^V \mu Z . \Phi \), then there is a least ordinal \( \alpha \) such that \( E \models^V \mu Z^\alpha . \Phi \) and for all \( \beta < \alpha \), \( E \not\models^V \mu Z^\beta . \Phi \)

2. If \( E \not\models^V \nu Z . \Phi \), then there is a least ordinal \( \alpha \) such that \( E \not\models^V \nu Z^\alpha . \Phi \) and for all \( \beta < \alpha \), \( E \models^V \nu Z^\beta . \Phi \)
Computational Properties

- **Satisfiability Problem**: “Given a modal $\mu$-calculus formula $\Phi$, is $\Phi$ satisfiable?” is **EXPTIME**-complete.

- **Tree Model Property** If $\Phi$ is satisfiable then $\Phi$ is satisfiable in a transition system/Kripke model that is a (regular) infinite tree.

- **Finite Model Property** If $\Phi$ is satisfiable then $\Phi$ is satisfiable in a finite transition system/Kripke model.

- **Model Checking Problem** “Given a finite model, a state $E$ and closed $\Phi$, does $E \models \Phi$?” Its exact complexity is a long standing **OPEN** problem. Best known upper bound is $\text{NP} \cap \text{co-NP}$.