Modal and Temporal Logics

Colin Stirling
School of Informatics
University of Edinburgh

July 25, 2003

Summary: Temporal Operators as Fixed points

1. $\mathsf{E}(\Phi \,\mathsf{U}\, \Psi) \equiv \Psi \vee (\Phi \wedge \langle - \rangle \mathrm{E}(\Phi \,\mathrm{U}\, \Psi))$

2. $\mathsf{A}(\Phi \,\mathsf{U}\, \Psi) \equiv \Psi \vee (\Phi \wedge \langle - \rangle \mathtt{tt} \wedge [-]\mathrm{A}(\Phi \,\mathrm{U}\, \Psi))$

Syntactically: property X such that

1. $X \equiv \Psi \vee (\Phi \wedge \langle - \rangle X)$

2. $X \equiv \Psi \vee (\Phi \wedge \langle - \rangle \mathtt{tt} \wedge [-] X)$

Summary: Temporal Operators as Fixed points

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

1. $\lambda x. \| \, \Psi \vee (\Phi \wedge \langle - \rangle x) \, \|$

2. $\lambda x. \| \, \Psi \vee (\Phi \wedge \langle - \rangle \mathtt{tt} \wedge [-] x) \, \|$

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 $\langle - \rangle$ and $[-]$).

Summary: Fixed points

S is a prefixed point of f, if $f(S) \subseteq S$

S is a postfixed 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. $X \;\equiv\; \Phi \vee \langle - \rangle X$ least   Answer: $\mathsf{E}\,\mathsf{F}\,\Phi$

2. $X \;\equiv\; \Phi \wedge \langle - \rangle X$ greatest

3. $X \;\equiv\; \Phi \wedge [-][-]X$ greatest

A Scheduler

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

a_i initiates the ith 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

$\Phi ::= Z \mid \texttt{tt} \mid \texttt{ff} \mid \Phi_1 \wedge \Phi_2 \mid \Phi_1 \vee \Phi_2 \mid [K]\Phi \mid \langle K \rangle \Phi$

- $\models$ refined to $\models_{\mathsf{V}}$ where V is a **valuation** that assigns a set of states $\mathsf{V}(X)$ to each variable X

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

- $\parallel \Phi \parallel$ refined too: $\parallel \Phi \parallel_{\mathsf{V}} \; = \{E : E \models_{\mathsf{V}} \Phi\}$

- $\mathsf{V}[S/X]$ is valuation V' like V except $\mathsf{V}'(X) = S$.

Modal Logic+ II

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

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

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

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

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

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

Alternative basis for temporal logic: **modal logic + fixed points**

Modal μ-calculus

Syntax

$\Phi ::= \mathtt{tt} \mid \mathtt{ff} \mid Z \mid \Phi_1 \wedge \Phi_2 \mid \Phi_1 \vee \Phi_2 \mid [K]\Phi \mid \langle K\rangle\Phi \mid \nu Z.\,\Phi \mid \mu Z.\,\Phi$

- let σ range over the set $\{\mu, \nu\}$.
- An occurrence of Z is free within Φ if it is not within the scope of an occurrence of σZ. σZ in $\sigma Z.\Phi$ binds free occurrences of Z in Φ.
- Formulas may have multiple fixed points: $\nu Z.\,\mu Y.\,([b]Y \wedge [K]Z)$
- σZ may bind more than one occurrence of Z: $\nu Z.\,\langle\mathtt{tick}\rangle Z \wedge \langle\mathtt{tock}\rangle Z$.

Semantics

$$
\begin{array}{lll}
E \models_{\mathsf{V}} \mathtt{tt} & & \\
E \not\models_{\mathsf{V}} \mathtt{ff} & & \\
E \models_{\mathsf{V}} Z & \text{iff} & E \in \mathsf{V}(Z) \\
E \models_{\mathsf{V}} \Phi \wedge \Psi & \text{iff} & E \models_{\mathsf{V}} \Phi \text{ and } E \models_{\mathsf{V}} \Psi \\
E \models_{\mathsf{V}} \Phi \vee \Psi & \text{iff} & E \models_{\mathsf{V}} \Phi \text{ or } E \models_{\mathsf{V}} \Psi \\
E \models_{\mathsf{V}} [K]\Phi & \text{iff} & \forall F \in \{E' : E \xrightarrow{a} E' \text{ and } a \in K\}.\ F \models_{\mathsf{V}} \Phi \\
E \models_{\mathsf{V}} \langle K\rangle\Phi & \text{iff} & \exists F \in \{E' : E \xrightarrow{a} E' \text{ and } a \in K\}.\ F \models_{\mathsf{V}} \Phi \\
E \models_{\mathsf{V}} \nu Z.\,\Phi & \text{iff} & E \in \bigcup\{S \ : \ S \subseteq \|\,\Phi\,\|_{\mathsf{V}[S/Z]}\} \\
E \models_{\mathsf{V}} \mu Z.\,\Phi & \text{iff} & E \in \bigcap\{S \ : \ \|\,\Phi\,\|_{\mathsf{V}[S/Z]} \subseteq S\}
\end{array}
$$

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 $\parallel \Phi \parallel_{\mathsf{V}}$.

$$
\begin{array}{lll}
E \models_{\mathsf{V}} \nu Z.\,\Phi & \text{iff} & \exists S.\, E \in S \text{ and } \forall F \in S.\, F \models_{\mathsf{V}[S/Z]} \Phi \\
E \models_{\mathsf{V}} \mu Z.\,\Phi & \text{iff} & \forall S.\ \text{if } E \notin S \text{ then } \exists F \notin S.\, F \models_{\mathsf{V}[S/Z]} \Phi
\end{array}
$$

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

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

Variant

Define modal μ-calculus on Kripke models

Syntax

$\Phi ::= p \mid \neg p \mid Z \mid \Phi_1 \wedge \Phi_2 \mid \Phi_1 \vee \Phi_2 \mid [-]\Phi \mid \langle - \rangle \Phi \mid \nu Z.\, \Phi \mid \mu Z.\, \Phi$

$$
\begin{array}{lll}
E \models_{\mathsf{V}} p & \text{iff} & E \in L(p) \\
E \models_{\mathsf{V}} \neg p & \text{iff} & E \notin L(p)
\end{array}
$$

Unfolding

- An unfolding of $\sigma Z.\,\Phi$ is $\Phi\{\sigma Z.\Phi/Z\}$

  Unfolding of $\nu Z.\,\langle - \rangle Z$ is $\langle - \rangle(\nu Z.\,\langle - \rangle Z)$.

- **Proposition** $E \models_{\mathsf{V}} \sigma Z.\Phi$ iff $E \models_{\mathsf{V}} \Phi\{\sigma Z.\Phi/Z\}$.

Expressiveness I

Modal μ-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 *

$$
\begin{array}{lll}
E \xrightarrow{w+v} F & \text{iff} & E \xrightarrow{w} F \text{ or } E \xrightarrow{v} F \\
E \xrightarrow{w;v} F & \text{iff} & E \xrightarrow{w} E_1 \xrightarrow{v} F \text{ for some } E_1 \\
E \xrightarrow{w^*} F & \text{iff} & E = F \text{ or } E \xrightarrow{w} E_1 \xrightarrow{w} \ldots \xrightarrow{w} E_n \xrightarrow{w} F \text{ for some} \\
 & & n \geq 0 \text{ and } E_1, \ldots, E_n
\end{array}
$$

Exercise

What properties are expressed by the following formulas?

1. $\mu Z.\, [-]Z$
2. $\nu Z.\, [-]\langle \texttt{tick} \rangle Z$
3. $\nu Z.\, \langle \texttt{tick} \rangle Z \wedge \langle \texttt{tock} \rangle Z$
4. $\mu Z.\, \nu Y.\, [a]Z \wedge [-a]Y$
5. $\nu Z.\, (\mu X.\, [b](\nu Y.\, [c](\nu Y_1.\, X \wedge [-a]Y_1) \wedge [-a]Y) \wedge [-]Z)$

Bisimulation Invariance

$E \equiv F$ if for all closed modal μ-calculus formulas Φ, $E \models \Phi$ iff $F \models \Phi$.

Proposition if $E \sim F$ then $E \equiv F$

Exercise

Express the following properties in modal μ-calculus

1. Eventually either `tick` happens or Φ becomes true

2. In some run Φ is always true

3. `tick` happens until Φ

4. `tick` happens until `tock` happens

5. In exactly three runs, Φ is true

Expressiveness II

Proposition Modal μ-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

$$\begin{array}{lccl} \text{least fixed point} & \mu g & = & \bigcap\{S : g(S) \subseteq S\} \\ \text{greatest fixed point} & \nu g & = & \bigcup\{S : S \subseteq g(S)\} \end{array}$$

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

$$\begin{array}{ccccccccc} \nu^0 g & \supseteq & \nu^1 g & \supseteq & \ldots & \supseteq & \nu^i g & \supseteq & \ldots \\ \cup & & \cup & & & & \cup & & \\ \nu g & & \nu g & & \ldots & & \nu g & & \ldots \end{array}$$

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

Approximants II

- If S' is not a finite set, then use ordinals

$$0, 1, \ldots, \omega, \omega + 1, \ldots, \omega + \omega, \omega + \omega + 1, \ldots$$

- ω is the initial limit ordinal

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

$$\nu^\lambda g \quad = \quad \bigcap \{\nu^\alpha g \,:\, \alpha < \lambda\}$$

Approximants III

$$\begin{array}{ccccccccc} \nu^0 g & \supseteq & \ldots & \supseteq & \nu^\omega g & \supseteq & \nu^{\omega+1} g & \supseteq & \ldots \\ \cup & & & & \cup & & \cup & & \\ \nu g & & \ldots & & \nu g & & \nu g & & \ldots \end{array}$$

The fixed point νg 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 $\mu^\lambda g \quad = \quad \bigcup\{\mu^\alpha g : \alpha < \lambda\}$

- There is the following possibly increasing sequence of sets.

$$
\begin{array}{ccccccccc}
\mu g & & \dots & & \mu g & & \mu g & & \dots \\
\cup & & & & \cup & & \cup & & \\
\mu^0 g & \subseteq & \dots & \subseteq & \mu^\omega g & \subseteq & \mu^{\omega+1} g & \subseteq & \dots
\end{array}
$$

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

Syntactic Approximants

$$
\begin{array}{lclllcl}
\nu Z^0.\,\Phi & = & \mathtt{tt} & & \mu Z^0.\,\Phi & = & \mathtt{ff} \\
\nu Z^{\alpha+1}.\,\Phi & = & \Phi\{\nu Z^\alpha.\,\Phi/Z\} & & \mu Z^{\alpha+1}.\,\Phi & = & \Phi\{\mu Z^\alpha.\,\Phi/Z\} \\
\nu Z^\lambda.\,\Phi & = & \bigwedge\{\nu Z^\alpha.\,\Phi \,:\, \alpha < \lambda\} & & \mu Z^\lambda.\,\Phi & = & \bigvee\{\mu Z^\alpha.\,\Phi \,:\, \alpha < \lambda\}
\end{array}
$$

Proposition

1. If $E \models_{\mathsf{V}} \mu Z.\,\Phi$, then there is a least ordinal α such that $E \models_{\mathsf{V}} \mu Z^\alpha.\,\Phi$ and for all $\beta < \alpha$, $E \not\models_{\mathsf{V}} \mu Z^\beta.\,\Phi$

2. If $E \not\models_{\mathsf{V}} \nu Z.\,\Phi$, then there is a least ordinal α such that $E \not\models_{\mathsf{V}} \nu Z^\alpha.\,\Phi$ and for all $\beta < \alpha$, $E \models_{\mathsf{V}} \nu Z^\beta.\,\Phi$

Computational Properties

- **Satisfiability Problem:** "Given a modal μ-calculus formula Φ, is Φ satisfiable?" is **EXPTIME**-complete.

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

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

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