

# COMP6463: Temporal Logic and Model Checking

## 1. Modal Logic

Michael Norrish

Canberra Research Lab., NICTA

Semester 1, 2009



**NICTA**

# Outline

- 1 Introduction
- 2 Syntax and Semantics
- 3 Proof Rules
- 4 Properties of the Logics

# Introduction

Modal logic is a very big area for both pure logicians and computer scientists.

This part of COMP6463 will cover a smaller, focussed aspect of modal logic: **temporal logics**, and their application in **model checking**.

**Model checking** is a powerful automatic verification technology: it can be used to verify properties of, and find bugs in large formal systems, such as descriptions of

- hardware;
- protocols (security, bus-level, general communication)
- software

Properties that are checked are written in a **temporal logic**.

## But Today...

Modal logic generally.

A whirlwind tour of the important things every computer scientist should know about modal logic.

See, for example:

- *Modal Logic*, by Patrick Blackburn, Maarten de Rijke and Yde Venema. Cambridge University Press, 2001.
- the Wikipedia page is OK, and has lots of references to other resources.

# Historical Background

Modal logics are logics with added modalities.

A modality modifies a proposition  $p$ . For example:

- I know  $p$  is true (epistemic)
- I believe  $p$  is true (doxastic)
- $p$  is necessarily true (necessity)
- $p$  will be true (temporal)
- $p$  is provable (provability)
- One ought to  $p$  (deontic ??)

Arguing about what necessity means is something you can do for a good long time.

Indicate modal( $p$ ) as  $\Box p$ .

# Random Axiom Schemes

The problem with the early work on modal logics is that there were no **models**.

Investigation had to proceed thus:

- Postulate set of axioms and proof rules
- Explore consequences
- ...

One could show

- triviality (system proved everything)
- inclusion (system 1 proved everything system 2 proved)

But no possible notion of **completeness**.

# The Kripke Revolution

Two slogans from Blackburn *et al.*:

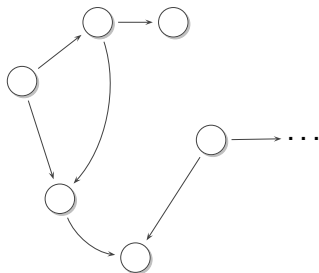
**Slogan 1** Modal languages are simple yet expressive languages for talking about relational structures

**Slogan 2** Modal languages provide an internal, local perspective on relational structures

What is a **relational structure**?

# Relational Structures

A relational structure



Also known as a graph.

Models, for example, transition systems.

In modal logic, each node is often known as a **world**.

## Modal Intuitions in Terms of Worlds

Something is *necessarily* true if it is true in all possible worlds.

Something is true *in the future* if it is true in a “later” world.

Not all worlds are necessarily *visible* from others:

- If action *a* is true at some point in the future, it may then be the case that *b* will never be true thereafter.
- But if *c* is true at some point, then *b* may be true at *all* later times

In this way, a relational structure's branching structure may impact formula truth.

# Syntax

A formula  $\phi$  of modal logic can be

- $p, q, r, \dots$  (a variable)
- $\neg\phi$  (a negation)
- $\phi_1 \Rightarrow \phi_2$  (an implication)
- $\Box\phi$  (a modality)

Add obvious (classical) definitions for  $\vee$ ,  $\wedge$  and  $\perp$  if you wish.

Also, define

$$\Diamond\phi = \neg\Box\neg\phi$$

## Semantic Intuition

A formula is true of a particular world within a relation.

- (Remember Slogan 2's: "modal languages provide a... local perspective")

The box is a form of **universal** quantifier:

$\Box p$

means  $p$  is true at all my neighbours.

# Semantic Intuition

A formula is true of a particular world within a relation.

- (Remember Slogan 2's: "modal languages provide a... local perspective")

The box is a form of **universal** quantifier:

$\Box p$

means  $p$  is true at all my neighbours.

Diamond is existential:

$$\begin{aligned}\neg\Box\neg p &= \text{it's not the case that } p \text{ is false at all my neighbours} \\ &= p \text{ is true at one of my neighbours} \\ &= \Diamond p\end{aligned}$$

## Example Formulas

$$p \Rightarrow \Box \Diamond p$$

If  $p$  is true in “my world”, then every world I can reach has a neighbour where  $p$  is true.

## Example Formulas

$$p \Rightarrow \Box \Diamond p$$

If  $p$  is true in “my world”, then every world I can reach has a neighbour where  $p$  is true.

$$\Box p \wedge \Diamond q \Rightarrow \Diamond p$$

If  $p$  is true of every neighbour, and I have a neighbour where  $q$  is true, then I also have a neighbour where  $p$  is true.

The latter is true of every possible relation, regardless of  $p$  and  $q$ .

## Semantic Details

Semantics is with respect to a relation  $R$  connecting worlds  $W$ , a world  $w \in W$  and a valuation  $V : W \rightarrow \mathcal{P}(\text{Var})$ . (Compare propositional valuations, which give values to just one set of variables.)

The triple  $(W, R, V)$  is a **model**, call it  $\mathfrak{M}$ .

Write  $\mathfrak{M}, w \models \phi$  to mean “ $\phi$  is true at world  $w$  in model  $\mathfrak{M}$ ”.

$\mathfrak{M}, w \models p$                     if  $p \in V(w)$

$\mathfrak{M}, w \models \neg\phi$                 if  $\mathfrak{M}, w \not\models \phi$

$\mathfrak{M}, w \models \phi_1 \Rightarrow \phi_2$     if  $\mathfrak{M}, w \not\models \phi_1$  or  $\mathfrak{M}, w \models \phi_2$

$\mathfrak{M}, w \models \Box\phi$                 if at every  $v$  such that  $w R v$ , have  $\mathfrak{M}, v \models \phi$

## Formula Examples



At left world,

$\diamond q$

is true

# Formula Examples



At left world,

$\diamond q$   
 $\square \neg q$

is true

is false

# Formula Examples



At left world,

$\diamond q$	is true
$\square \neg q$	is false
$\diamond \square r$	is true

# Formula Examples



At left world,

$\diamond q$	is true
$\square \neg q$	is false
$\diamond \square r$	is true
$p \Rightarrow \square \diamond p$	is false

# Formula Examples



At left world,

$\diamond q$	is true
$\square \neg q$	is false
$\diamond \square r$	is true
$p \Rightarrow \square \diamond p$	is false
$\neg p \Rightarrow \square \diamond \neg p$	is true

# Validity

In **first order logic**, we define truth of a formula with respect to

- an interpretation (interpreting function and predicate symbols), and
- a valuation (interpreting variables)

These two are sometimes lumped together.

A formula can then be **true** (sometimes **valid**) in an interpretation, if it is true in all possible variable interpretations. For example,

$$x + 2 > x$$

is true in the interpretation corresponding to natural number arithmetic.

# Validity

A formula can also be **logically valid**, if it is true for all possible interpretations. E.g.,

$$(\forall x. P(x) \wedge Q(x)) \equiv (\forall x.P(x)) \wedge (\forall x.Q(x))$$

Such formulas can even have free variables:

$$P(x) \Rightarrow P(x)$$

is logically valid.

# Validity for Modal Logic

Call a relation  $R$  and its worlds  $W$ , a **frame**  $\mathfrak{F}$ .

Can now talk about ascending chain of “validities”.

- $\phi$  valid for a world  $w$  and frame  $\mathfrak{F}$ , if  $(\mathfrak{F}, V), w \models \phi$  for all  $V$
- $\phi$  valid for a frame  $\mathfrak{F}$ , if  $(\mathfrak{F}, V), w \models \phi$  for all  $V$  and  $w \in W$
- $\phi$  valid for a class of frames  $F$ , if  $(\mathfrak{F}, V), w \models \phi$  for all  $V$ ,  $w \in W$  and  $\mathfrak{F} \in F$
- $\phi$  valid for all frames, if  $(\mathfrak{F}, V), w \models \phi$  for all  $V$ ,  $w \in W$  and  $\mathfrak{F}$

Only the last two are likely to be of any interest.

Write **valid for a frame** as  $\mathfrak{F} \models \phi$

Write **valid for all frames** as  $\models \phi$

# Valid Formulas

Some examples:

- Propositional tautologies ( $p \Rightarrow p$ , etc) are always valid.
- $\Box p \wedge \Diamond q \Rightarrow \Diamond p$  is valid on all frames.
- $p \Rightarrow \Diamond p$  is valid on all reflexive frames.
- $p \Rightarrow \Box \Diamond p$  is valid on all symmetric frames.
- $\Diamond \Diamond p \Rightarrow \Diamond p$  is valid on all transitive frames.

Can take contrapositives (and substitution instances):

- $\Box p \Rightarrow \Diamond p \vee \Box q$  is valid on all frames
- $\Box p \Rightarrow p$  is valid on all reflexive frames.
- ...

# A Proof System

Take your favourite Hilbert presentation of propositional calculus (axioms plus Modus Ponens).

Add the **K axiom** (an axiom scheme):

$$\vdash \Box(p \Rightarrow q) \Rightarrow (\Box p \Rightarrow \Box q)$$

Add the rule of **necessitation** or **generalisation**:

$$\frac{\vdash p}{\vdash \Box p}$$

# What Does the Proof System Prove?

The proof system generates statements valid for all frames.

Thus, the soundness argument for

$$\frac{\vdash p}{\vdash \Box p}$$

- 1 If  $p$  is valid for all frames, then it is true for all worlds in all frames.
- 2 At any given world  $w$ , all of  $w$ 's neighbours must also have  $p$  true.
- 3 So  $\Box p$  is true at all worlds in all frames.
- 4 So  $\Box p$  is valid.

## The Error to Avoid

In first order logic, have

$$\frac{\vdash P(x)}{\vdash \forall x.P(x)} \text{ GEN}$$

This does **not** imply

$$\vdash P(x) \Rightarrow \forall x.P(x)$$

Similarly, modal generalisation does **not** imply

$$\vdash p \Rightarrow \Box p$$

# The Coolest Thing About Modal Logic

Classes of frames can be characterised by modal axioms.

If a frame is reflexive, then

$$\vdash \Box p \Rightarrow p$$

(alternatively)

$$\vdash p \Rightarrow \Diamond p$$

# The Coolest Thing About Modal Logic

Classes of frames can be characterised by modal axioms.

If a frame is reflexive, then

$$\vdash \Box p \Rightarrow p$$

(alternatively)

$$\vdash p \Rightarrow \Diamond p$$

Conversely, if  $p \Rightarrow \Diamond p$  holds of a frame, then it is reflexive.

## Interlude: Translation to Quantified Formulas

For a particular model, a modal formula denotes a set of worlds where it is true.

Define  $\llbracket - \rrbracket_w : \text{formula} \rightarrow 2$ , where  $w \in W$ .

Using the definitions of truth in a model

$$\begin{aligned}\llbracket p \rrbracket_w &= p^*(w) \\ \llbracket \neg \phi \rrbracket_w &= \neg \llbracket \phi \rrbracket_w \\ \llbracket \phi_1 \Rightarrow \phi_2 \rrbracket_w &= \llbracket \phi_1 \rrbracket_w \Rightarrow \llbracket \phi_2 \rrbracket_w \\ \llbracket \Box \phi \rrbracket_w &= \forall v. w R v \Rightarrow \llbracket \phi \rrbracket_v \\ \llbracket \Diamond \phi \rrbracket_w &= \exists v. w R v \wedge \llbracket \phi \rrbracket_v\end{aligned}$$

where  $p^*(w) = w \in V(p)$

## Quantified Version of Reflexivity Formula

So

$$p \Rightarrow \Diamond p$$

becomes (for a particular  $w$ ,  $R$  and  $V$ )

$$p^*(w) \Rightarrow \exists v. w R v \wedge p^*(v)$$

If this formula is true for all possible  $V$  and  $w$ , it becomes

$$\forall P w. P(w) \Rightarrow \exists v. w R v \wedge P(v)$$

(observe how there is a quantification over the predicate/set  $P$ )

## Quantified Version Implies Reflexivity

Have  $\forall P w. P(w) \Rightarrow \exists v. w R v \wedge P(v)$

Want  $x R x$  for an arbitrary  $x$

Pick  $P(y) = (y = x)$ , and  $w = x$

Obtaining  $(x = x) \Rightarrow \exists v. x R v \wedge (v = x)$

Other direction, that

$$(\forall x. x R x) \Rightarrow \forall P w. P(w) \Rightarrow \exists v. w R v \wedge P(v)$$

is easy.

## Cool Fact Applied

If we want to reason in/about the class of reflexive frames, we add the axiom

$$p \Rightarrow \Diamond p$$

to our system.

If we want to reason about the class of symmetric frames, we add the axiom

$$p \Rightarrow \Box \Diamond p$$

## Axioms and Their Wacky Names

$p \Rightarrow \Diamond p$	reflexive	T
$p \Rightarrow \Box \Diamond p$	symmetric	B
$\Diamond \Diamond p \Rightarrow \Diamond p$	transitive	4
$\Box p \Rightarrow \Diamond p$	“right-unbounded”	D
$\Box(\Box p \Rightarrow p) \Rightarrow \Box p$	SN and transitive	L (or G or W)

Name systems by concatenating axioms (starting with K).

E.g., KT (also T), KB (also B), KT4 (S4), KT4B (S5).

Thus, S4 is a logic of pre-orders, and S5 is a logic of equivalence relations.

## Exercise

Prove that axiom L is true for all worlds in a frame  $\mathcal{R}$  iff  $\mathcal{R}$  is transitive and strongly-normalising.

### Strong Normalisation:

A relation  $\mathcal{R}$  is strongly normalising if there are no infinite  $\mathcal{R}$ -chains:

$$w_0 \rightarrow_{\mathcal{R}} w_1 \rightarrow_{\mathcal{R}} w_2 \rightarrow_{\mathcal{R}} \dots$$

Alternatively, all non-empty sets have  $\mathcal{R}$ -maximal elements:

$$S \text{ not empty} \Rightarrow \exists x \in S. \forall y. \mathcal{R}(x, y) \Rightarrow y \notin S$$

Also,  $SN(\mathcal{R}) \equiv WF(\mathcal{R}^{-1})$

## Better Yet: Completeness

These axioms give **complete** systems for frames of the given shape.

- If  $\phi$  is true on all reflexive frames, then  $\phi$  is provable in KT.
- If  $\phi$  is true of all pre-orders, then  $\phi$  is provable in S4.

Of course, the desired property has to be something that can be expressed in the modal language!

# Varieties of Completeness

Weak Completeness: if  $\models \phi$ , then  $\vdash \phi$ .

Strong Completeness: if  $\Gamma \models \phi$ , then  $\Gamma \vdash \phi$ .

The  $\Gamma$  is a set of assumptions being made.

Curiously, all the previous examples, **except for KL**, are strongly complete.

- KL is *weak complete*

# Axiom Expressivity

Some axioms have first-order equivalents (reflexivity, etc).

Others, like L ( $\Box(\Box p \Rightarrow p) \Rightarrow \Box p$ ) do not.

Worse, lots of first-order properties (irreflexivity, anti-symmetry), don't have modal equivalents.

## Adding Modalities

The  $\diamond$  and  $\square$  link up with one underlying relation  $R$ .

It is trivial to add new modalities,  $\square^*$  and  $\diamond^*$  say, so that underlying frames with two relations can be reasoned about:

$$\mathfrak{M}, w \models \square\phi = \forall v. R_1(w, v) \Rightarrow \mathfrak{M}, v \models \phi$$

$$\mathfrak{M}, w \models \square^*\phi = \forall v. R_2(w, v) \Rightarrow \mathfrak{M}, v \models \phi$$

where  $\mathfrak{M}$  will be a 4-tuple  $(W, R_1, R_2, V)$ .

Generalising to  $n$  underlying relations is easy of course.

Two modalities is good enough for a simple temporal logic. . .

# A Temporal Logic

## Existential Modalities

$F \phi$   $\phi$  will be true at some point in the **F**uture

$P \phi$   $\phi$  was true at some point in the **P**ast

## Universal Duals:

$G \phi$   $\phi$  is **G**oing to be true at all points in the future

$H \phi$   $\phi$  **H**as been true at all points in the past

Relate the two underlying relations with two axioms:

$$p \Rightarrow HF p$$

$$p \Rightarrow GP p$$

# Summary

- Modal logics talk about **relational structures**
- Modal logics extend propositional logic with simple, restricted form of quantification ( $\diamond$ ,  $\Box$ )
- Semantics is with respect to **frames** and valuations
- Proof systems derive truths with respect to all possible frames in a class
- Classes of frame are characterised by various modal **axioms**
  
- (One exercise!)