An Introduction to Modal Logic

2009 Formosan Summer School on Logic, Language, and Computation

29 June-10 July, 2009

廖純中

中央研究院

資訊科學研究所　資訊科技創新研究中心

The Agenda

- Introduction
- Basic Modal Logic
- Normal Systems of Modal Logic
- Meta-theorems of Normal Systems
- Variants of Modal Logic
- Conclusion

Introduction

Let me tell you the story

Introduction

- Historical overview
- Conceptual overview
- Further readings

Historical Overview

- Pre-history
- The syntactic era (1918-1959)
- The classical era (1959-1972)
- The modern era (1972-present)

Pre-history: How It Starts

The Battle of Salamis, 20 September, 480 B.C

Pre-history: Aristotle's De Interpretatione 9

- the problem of future contingents: a logical paradox by Diodorus Cronus, Megarian school of philosophy
- what happens was necessarily going to happen
- what does not happen was necessarily going to not happen
- Aristotle: statements about the future are neither true nor false

Pre-history: Aristotle's De Interpretatione 9

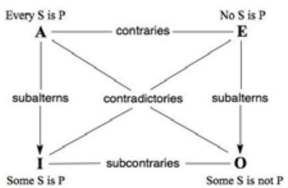
> . . . if a thing is white now, it was true before to say that it would be white, so that of anything that has taken place, it was always true to say 'it is' or 'it will be'. But if it was always true to say that a thing is or will be, it is not possible that it should not be or not come to be, and when a thing cannot not come to be, it is impossible that it should not come to be, and when it is impossible that it should not come to be, it must come to be. *All then, that is about to be must of necessity take place*. It results from this that nothing is uncertain or fortuitous, for if it were fortuitous it would not be necessary.

[Translation, Ross, 1928]

Pre-history: Aristotle's De Interpretatione 9

1. φ: there is (was) a sea-battle on 20 September, 480 B.C.
2. $\varphi \supset \Box\varphi$
3. $\neg\varphi \supset \Box\neg\varphi$
4. $\varphi \vee \neg\varphi$
5. $\Box\varphi \vee \Box\neg\varphi$
6. logical validity is universal, so $\Box\varphi \vee \Box\neg\varphi$ holds before 20 September, 480 B.C: fatalism

Pre-history: Aristotle's Square of Opposition



$$\mathbf{A} : \Box p, \mathbf{E} : \Box\neg p, \mathbf{I} : \Diamond p, \mathbf{O} : \Diamond\neg p$$

contrary: $\neg(\Box p \wedge \Box\neg p)$ subaltern: $\Box p \supset \Diamond p$, $\Box\neg p \supset \Diamond\neg p$
subcontrary: $\Diamond p \vee \Diamond\neg p$ contradictory: $\Box p \equiv \neg\Diamond p$, $\Box\neg p \equiv \neg\Diamond p$

Pre-history: Possible Worlds

- G.W. Leibniz (1646/7/1-1716/11/14):
  - a possible world is made up of individuals that are compossible – that is, individuals that can exist together.
  - possible worlds exist as possibilities in the mind of God.
  - one world among them is realized as the actual world, and this is the most perfect one

Pre-history: Possible Worlds

- modal status of a proposition:
  - truth: true in the actual world
  - falsity: false in the actual world
  - possibility: true in at least one possible world
  - impossibility: true in no possible world
  - necessity: true in all possible worlds
  - contingency: true in some possible worlds and false in others

Pre-history

Aristotle and G.W. Leibniz

Historical Overview

- Pre-history
- The syntactic era (1918-1959)
- The classical era (1959-1972)
- The modern era (1972-present)

The Syntactic Era

- paradox of material implication ($\supset$):

  1. $\neg\varphi \ \vdash \ (\varphi \supset \psi)$
  2. $\psi \ \vdash \ (\varphi \supset \psi)$
  3. $(\varphi \wedge \psi) \supset \chi \ \vdash \ (\varphi \supset \chi) \vee (\psi \supset \chi)$
  4. $(\varphi_1 \supset \varphi_2) \wedge (\psi_1 \supset \psi_2) \ \vdash \ (\varphi_1 \supset \psi_2) \vee (\psi_1 \supset \varphi_2)$
  5. $\varphi \supset \psi \ \vdash \ \varphi \wedge \chi \supset \psi$
  6. $\varphi \supset \psi, \psi \supset \chi \ \vdash \ \varphi \supset \chi$
  7. $\varphi \supset \psi \ \vdash \ \neg\psi \supset \neg\varphi$
  8. $\neg(\varphi \supset \psi) \ \vdash \ \varphi$
  9. $\vdash \ (\varphi \supset \psi) \vee (\neg\varphi \supset \psi)$
  10. $\vdash \ (\varphi \supset \psi) \vee (\psi \supset \varphi)$
  11. $\neg\varphi \supset \neg(\psi \supset \chi), \neg\psi \ \vdash \ \varphi$

The Syntactic Era

- there are counterintuitive results to formulate "if φ, then ψ" as $\varphi \supset \psi$
- Dorothy Edgington's proof of the existence of God
  - φ: God exists; ψ: I pray; χ: my prayers will be answered
  - $\neg\varphi \supset \neg(\psi \supset \chi), \neg\psi \ \vdash \ \varphi$
  - if God does not exist, then it's not the case that if I pray, my prayers will be answered; and I don't pray; so God exists!
- strict Implication (C.I. Lewis, 1912): 'it is necessarily the case that φ implies ψ

$$\varphi \rightarrow \psi \ =_{\text{def}} \ \Box(\varphi \supset \psi)$$

The Syntactic Era

- axiomatic systems: $\mathbf{S1}$ to $\mathbf{S5}$ by Lewis
- proving distinctness theorems
- lack of natural semantics
- three lines of work to next stage:
  - Carnap's state description (close to possible world semantics)
  - Prior's tense logic: with semantic ideas and insights (the model $(\omega, <)$)
  - Jónsson and Tarski: representation theorem of modal algebra (an algebraic analog of the canonical model techniques)

The Syntactic Era

C.I. Lewis, R. Carnap, A.N. Prior, and A. Tarski

Historical Overview

- Pre-history
- The syntactic era (1918-1959)
- The classical era (1959-1972)
- The modern era (1972-present)

The Classic Era

- Kripke semantics: accessibility relation (Kripke, 1959; Hintikka, 1957; Kanger, 1957)
- canonical model, completeness, filtration (Lemmon and Scott, 1977)
- relational structures: as analytic tools, not really to be described
- many applications in modeling of agents

The Classic Era

S.A. Kripke, J. Hintikka, S. Kanger, and D. Scott

Historical Overview

- Pre-history
- The syntactic era (1918-1959)
- The classical era (1959-1972)
- The modern era (1972-present)

The Modern Era

- frame incompleteness (Thomason, 1972, 1974)
- Sahlqvist correspondence theorem (1973)
- universal algebra: algebraic semantics
- classical model theory: correspondence theory, bisimulation (van Benthem)
- connections with other fields (Gabbay, Halpern, et al.):
  - computer science and AI: dynamic logic, description logic, temporal logic, epistemic logic, complexity
  - economics: game logic, (dynamic) epistemic logic
  - mathematics: co-algebra, non-well-founded set theory, geometry, topology
  - linguistics: feature logic

The Modern Era

J. van Benthem, D. Gabbay, and J. Halpern

Introduction

- Historical overview
- Conceptual overview
- Further readings

Philosophical Background

- the monotheistic approach: choosing one of all possible logical languages and saying 'This is THE Logic'
- the polytheistic approach: as a discipline that investigate different logical languages.

The Polytheistic Approach to Modal Logics

- alethic modal logic: necessity and possibility
- epistemic/doxastic logic: knowledge/belief
- deontic logic: obligation, permission, prohibition
- dynamic logic: action, program
- temporal logic: tense (future, past, since, until)
- description logic: role (universal and existent), Web 3.0, ontology language
- arrow logic, spatial logic, μ-calculus, game logic, coalition logic, dynamic epistemic logic etc.

Three Slogans

- modal languages are simple yet expressive languages for talking about relational structures
- modal languages provide an internal, local perspective on relational structures
- modal languages are not isolated formal systems
  - languages: modal vs classical (FOL,SOL), internal vs external perspective
  - relational structures vs Boolean algebra with operators (BAO): Jónsson and Tarski's representation theorem

(From P. Blackburn, M. De Rijke, and Y. Venema, Modal Logic)

The Slogans in Reality

- example: trust and reputation management in P2P systems
- internal and local perspective
  - each individual (peer) looks at itself and its neighbor
  - each neighbor is inside the community
  - distributed management by each individual
- external and global perspective
  - a central authority looks at the whole community
  - the authority is outside the community
  - centralized management by the authority

Introduction

- Historical overview
- Conceptual overview
- Further readings

Standard Textbooks and References

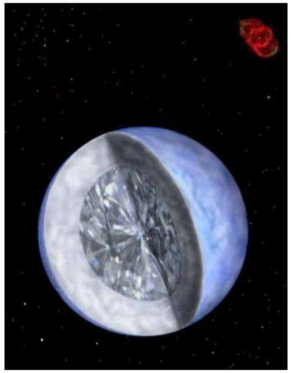
- B.F. Chellas. *Modal Logic: An Introduction*. Cambridge University Press, 1980.
- G. Hughes and M.J. Cresswell. *A Companion to Modal Logic*. Methuen, 1984.
- G. Hughes and M.J. Cresswell. *A New Introduction to Modal Logic*. Routledge, 1996.
- A. Chagrov and M. Zakharyaschev. *Modal logic*. Oxford University Press, 1997.
- P. Blackburn, M. De Rijke, and Y. Venema. *Modal Logic*. Cambridge University Press, 2001.
- P. Blackburn, J. van Benthem, and F. Wolter. *Handbook of Modal Logic*. Elsevier, 2007.

Internet Resources

- Advances in Modal Logic
- Stanford Encyclopedia of Philosophy
- Preview on the Handbook of Modal Logic
- Logic and Rational Interaction
- List of Resources in Wikipedia

Basic Modal Logic

Let me show you the diamond(s)



Basic Modal Logic

- Basic Modal Logic—Syntax
- Basic Modal Logic—Semantics
- Basic Model Theory

Basic Modal Logic—Syntax

- alphabet
  - a set of atomic propositional variables $\Phi_0 = \{p_1, p_2, \cdots\}$
  - primitive logical symbols: $\perp$ (contradiction), $\neg$ (negation), $\wedge$ (conjunction), $\Diamond$ (possibility modality)
  - defined logical symbols: $\top$ (tautology), $\vee$ (disjunction), $\supset$ (material implication), $\equiv$ (equivalence), $\Box$ (necessity modality)
  - auxiliary symbols: (,)
- well-formed formulas (wff):
  - any atomic propositional variable is a wff
  - $\perp$ is a wff
  - if φ and ψ are wffs, so are :$\neg\varphi$, $\Diamond\varphi$, and $\varphi \wedge \psi$

Basic Modal Logic—Syntax

- abbreviations:
  1. $\top$: $\neg\perp$
  2. $\varphi \vee \psi$: $\neg(\neg\varphi \wedge \neg\psi)$
  3. $\varphi \supset \psi$: $\neg\varphi \vee \psi$
  4. $\varphi \equiv \psi$: $(\varphi \supset \psi) \wedge (\psi \supset \varphi)$
  5. $\Box\varphi$: $\neg\Diamond\neg\varphi$

Several Modalities

John _______ successful.

- is necessarily
- is possibly
- is believed/known to be
- is permitted to be
- ought to be
- is now
- will be
- has a strategy to become
- ······

Conventions of Modalities

Modalities	Alethic logic	epistemic logic[1]	doxastic logic[2]	deontic logic[3]	temporal logic[4]	dynamic logic[5]	description logic
Possibility	$\Diamond$	$\neg K \neg$	$\neg B \neg$	P	F, P	$\langle\alpha\rangle$	$\exists R$
Necessity	$\Box$	K	B	O	G, H	$[\alpha]$	$\forall R$
Impossibility	$\neg\Diamond$	$K\neg$	$B\neg$	F			

1. K: know
2. B: believe
3. P: permission, O: obligation, F: prohibition (forbid)
4. $F(P)$: future (past) possibility, $G(H)$: future (past) necessity
5. $[\alpha](\langle\alpha\rangle)$: it's necessary (possible) after the execution of α

Syntax and Semantics

- Basic Modal Logic—Syntax
- Basic Modal Logic—Semantics
- Basic Model Theory

Basic Modal Logic—Semantics

- (Kripke) frame: $\mathfrak{F} = (W, R)$
  - W: a set of possible worlds (points, states, etc.)
  - $R \subseteq W \times W$: a binary relation over W
- (Kripke) model: $\mathfrak{M} = (\mathfrak{F}, \pi) = (W, R, \pi)$
  - $\mathfrak{F}$: a frame
  - $\pi : \Phi_0 \longrightarrow 2^W$: a truth assignment
- intuition
  - a frame is a (very basic) relational structure
  - $\pi(p)$: the set of all worlds in which p is true
  - $w \in \pi(p)$: the atomic proposition p is true in the world w
  - $w \notin \pi(p)$: the atomic proposition p is false in the world w

Basic Modal Logic—Semantics

- satisfaction: given a model $\mathfrak{M} = (W, R, \pi)$ and $w \in W$
  1. $\mathfrak{M}, w \not\Vdash \bot$
  2. $\mathfrak{M}, w \Vdash p \Leftrightarrow w \in \pi(p)$ for any $p \in \Phi_0$
  3. $\mathfrak{M}, w \Vdash \neg\varphi \Leftrightarrow \mathfrak{M}, w \not\Vdash \varphi$
  4. $\mathfrak{M}, w \Vdash \varphi \wedge \psi \Leftrightarrow \mathfrak{M}, w \Vdash \varphi$ and $\mathfrak{M}, w \Vdash \psi$
  5. $\mathfrak{M}, w \Vdash \Diamond\varphi \Leftrightarrow$ there exists $u \in W$ such that $(w, u) \in R$ and $\mathfrak{M}, u \Vdash \varphi$

Basic Modal Logic—Semantics

- derived rules of satisfaction
  1. $\mathfrak{M}, w \Vdash \top$
  2. $\mathfrak{M}, w \Vdash \varphi \vee \psi \Leftrightarrow \mathfrak{M}, w \Vdash \varphi$ or $\mathfrak{M}, w \Vdash \psi$
  3. $\mathfrak{M}, w \Vdash \varphi \supset \psi \Leftrightarrow$ if $\mathfrak{M}, w \Vdash \varphi$ then $\mathfrak{M}, w \Vdash \psi$
  4. $\mathfrak{M}, w \Vdash \varphi \equiv \psi \Leftrightarrow \mathfrak{M}, w \Vdash \varphi$ iff $\mathfrak{M}, w \Vdash \psi$
  5. $\mathfrak{M}, w \Vdash \Box\varphi \Leftrightarrow$ for all $u \in W$ such that $(w, u) \in R$, $\mathfrak{M}, u \Vdash \varphi$

Basic Modal Logic—Semantics

- $\mathfrak{M}, w \Vdash \varphi$: φ is satisfied or true in $\mathfrak{M}$ at state w
- $\mathfrak{M}, w \not\Vdash \varphi$: φ is refuted or false in $\mathfrak{M}$ at w
- $\mathfrak{M} \Vdash \varphi$: φ is globally or universally true in $\mathfrak{M}$: for all $w \in W$, $\mathfrak{M}, w \Vdash \varphi$
- φ is satisfiable in $\mathfrak{M}$ if there exists $w \in W$ s.t. $\mathfrak{M}, w \Vdash \varphi$
- φ is satisfiable in a class of models if it is satisfiable in some model belonging to the class
- φ is falsifiable or refutable if $\neg\varphi$ is satisfiable

Basic Modal Logic—Semantics

- let Σ denote a set of wffs
- $\mathfrak{M}, w \Vdash \Sigma$: for all $\varphi \in \Sigma$, $\mathfrak{M}, w \Vdash \varphi$
- $\mathfrak{M} \Vdash \Sigma$: Σ is globally or universally true in $\mathfrak{M}$: for all $w \in W$, $\mathfrak{M}, w \Vdash \Sigma$
- Σ is satisfiable in $\mathfrak{M}$ if there exists $w \in W$ s.t. $\mathfrak{M}, w \Vdash \Sigma$

Basic Modal Logic—Semantics

- C: a class of Kripke models, Σ: a set of wffs, φ: a wff
- $\Sigma \Vdash_{\mathtt{C}} \varphi$:
  - φ is a local semantic consequence of Σ over C
  - for all models $\mathfrak{M}$ in C and all worlds w in $\mathfrak{M}$, if $\mathfrak{M}, w \Vdash \Sigma$, then $\mathfrak{M}, w \Vdash \varphi$
- $\Sigma \Vdash^g_{\mathtt{C}} \varphi$:
  - φ is a global semantic consequence of Σ over C
  - for all models $\mathfrak{M}$ in C, if $\mathfrak{M} \Vdash \Sigma$, then $\mathfrak{M} \Vdash \varphi$
- $\Vdash_{\mathtt{C}} \varphi$: $\emptyset \Vdash_{\mathtt{C}} \varphi$: φ is valid on C
- note: $\{p\} \nVdash_{\mathtt{C}} \Box p$, but $\{p\} \Vdash^g_{\mathtt{C}} \Box p$

Properties of Binary Relations and Models

- a binary relation R is
  - serial: $\forall w \exists u, (w, u) \in R$
  - reflexive: $\forall w, (w, w) \in R$
  - symmetric: $\forall w, u, (w, u) \in R \Rightarrow (u, w) \in R$
  - transitive:

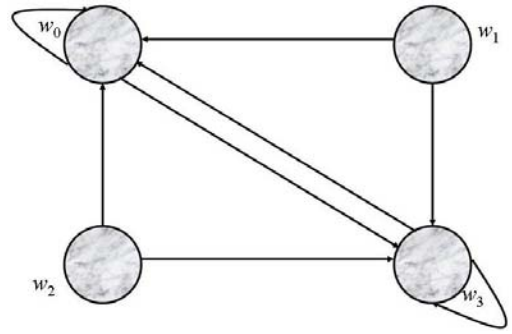
$$\forall w, u, v, (w, u) \in R \wedge (u, v) \in R \Rightarrow (w, v) \in R$$

  - Euclidean:

$$\forall w, u, v, (w, u) \in R \wedge (w, v) \in R \Rightarrow (u, v) \in R$$

- a frame $\mathfrak{F} = (W, R)$ or a models $\mathfrak{M} = (W, R, \pi)$ is serial (resp. reflexive, symmetric, transitive, Euclidean) if R is

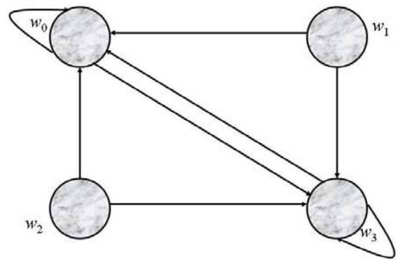
Example I: A Kripke Frame



$$\mathfrak{F} = (W, R)$$

- $W = \{w_0, w_1, w_2, w_3\}$
- $R = \{(w_0, w_0), (w_0, w_3), (w_3, w_0), (w_3, w_3), (w_1, w_0), (w_1, w_3), (w_2, w_0), (w_2, w_3)\}$

Example I: A Kripke Frame



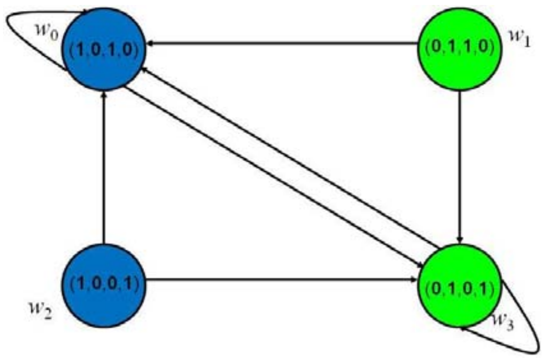
the frame may be

- a graph
- a social network
- a communication network
- a state transition system
- ......

Example I: A Scenario Based on the Frame

- the frame is a state transition system
- the scenario
  - there are two political parties —BLUE and GREEN— in a country
  - the country may be in two situations — BAD and GOOD
- atomic propositions
  - $blue$: the ruling party of the country is BLUE
  - $green$: the ruling party of the country is GREEN
  - bad: the country is in a BAD situation
  - $good$: the country is in a GOOD situation

Example I: A Kripke Model



- $(blue, green, bad, good)$
- $\mathfrak{M} = (W, R, \pi)$
- $\pi(blue) = \{w_0, w_2\}$
- $\pi(green) = \{w_1, w_3\}$
- $\pi(bad) = \{w_0, w_1\}$
- $\pi(good) = \{w_2, w_3\}$

Example I: A Kripke Model

$$R = \{(w, w_0), (w, w_3) \mid w \in W\}$$

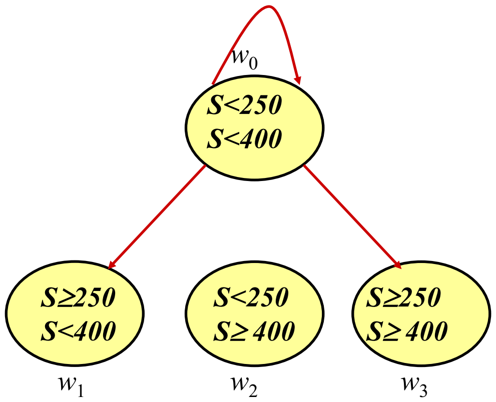
- $\mathfrak{M}, w_0 \Vdash bad$
- $\mathfrak{M}, w_0 \Vdash \neg green$
- $\mathfrak{M}, w_3 \Vdash good$
- $\mathfrak{M}, w_3 \Vdash \neg blue$
- $\mathfrak{M}, w_0 \Vdash blue \supset bad$
- $\mathfrak{M}, w_3 \Vdash blue \supset bad$
- $\mathfrak{M}, w_0 \Vdash green \supset good$
- $\mathfrak{M}, w_3 \Vdash green \supset good$
- $\mathfrak{M}, w \Vdash \Box(blue \supset bad)$
- $\mathfrak{M}, w \Vdash \Box(green \supset good)$
- $\mathfrak{M} \Vdash \Box(blue \supset bad)$
- $\mathfrak{M} \Vdash \Box(green \supset good)$

$$\forall \pi, \varphi, (\mathfrak{F}, \pi) \Vdash \Box\varphi \supset \Box\Box\varphi$$

Example II: Logical and Physical Possibility

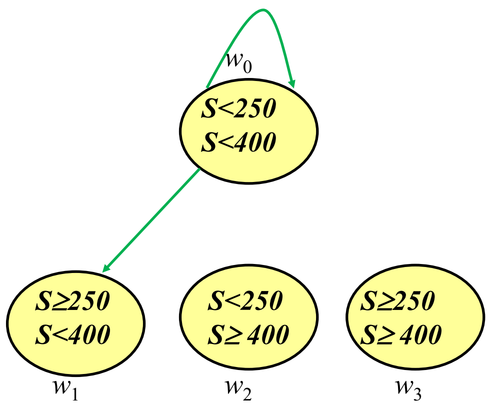
- physical constraint: the speed limit of T700 train of Taiwan High Speed Rail is 315km/h
- the actual scenario: in some day, I take the train which runs in a speed, say only 200km/h
- logical possibility: although the speed is now lower than 250km/h, it is logically possible that it is higher than 400km/h
- logical impossibility: it is logically impossible that the speed is lower than 250km/h and higher than 400km/h simultaneously
- physical possibility: although the speed is now lower than 250km/h, it is logically possible that it is higher than 250km/h
- physical impossibility: it is physically impossible that the speed is higher than 400km/h

Example II: Logical Possibility and Impossibility



Actually: $S<250 \wedge S<400$
Logical possibility: $S\geq 250 \wedge S\geq 400$
Logical impossibility: $S<250 \wedge S\geq 400$

Example II: Physical Possibility and Impossibility



Actually: $S<250 \wedge S<400$
Physical possibility: $S\geq 250 \wedge S<400$
Physical impossibility: $S\geq 250 \wedge S\geq 400$

Possibility: Logical and Physical

- actuality vs possibility:
  - actuality: something actually happens, e.g., p: the speed of the train is under 250km/h, q: the speed of the train is under 400km/h
  - possibility: although something has happened, it might have not happened if there are other alternatives, e.g., the speed of the train might have been higher than 250km/h if the driver have chosen to do so, $p \wedge \Diamond\neg p$
- physical possibility: under the physical constraint, the driver does not have the alternative to make the speed of the train higher than 315km/h
- logical possibility: however, logically, we can imagine such a situation

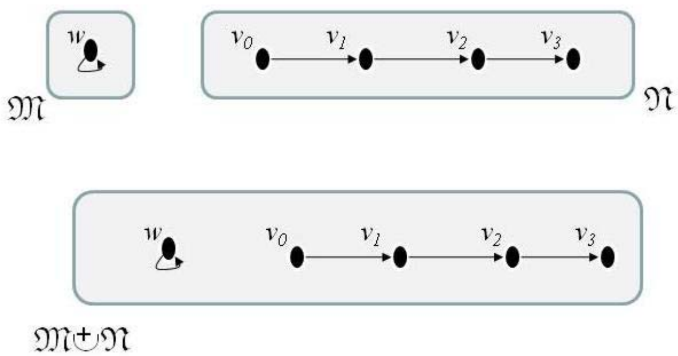
Syntax and Semantics

- Basic Modal Logic—Syntax
- Basic Modal Logic—Semantics
- Basic Model Theory

Disjoint Union: Definitions and Invariance

- two models $\mathfrak{M}_1 = (W_1, R_1, \pi_1)$ and $\mathfrak{M}_2 = (W_2, R_2, \pi_2)$ are disjoint if $W_1 \cap W_2 = \emptyset$
- for disjoint models $\mathfrak{M}_i = (W_i, R_i, \pi_i)(i \in I)$, their disjoint union is $\biguplus_i \mathfrak{M}_i = (W, R, \pi)$
  - $W = \bigcup_i W_i$
  - $R = \bigcup_i R_i$
  - $\pi(p) = \bigcup_i \pi_i(p)$ for each proposition letter
- for each wff φ, for each $i \in I$ and $w \in W_i$, $\mathfrak{M}_i, w \Vdash \varphi$ iff $\biguplus_i \mathfrak{M}_i, w \Vdash \varphi$

Disjoint Union: Example



Disjoint Union: Application

- universal modality A: $\mathfrak{M}, w \Vdash A\varphi \Leftrightarrow$ for all $u \in W$, $\mathfrak{M}, u \Vdash \varphi$ (i.e. $\mathfrak{M} \Vdash \varphi$)
- universal modality is not definable in basic modal logic
- suppose we could, that is, there exists wff $\alpha(p)$ such that $\mathfrak{M}, w \Vdash \alpha(p)$ iff $\mathfrak{M} \Vdash p$ for any model $\mathfrak{M}$
- let $\mathfrak{M}_1$ and $\mathfrak{M}_2$ be models such that $\mathfrak{M}_1 \Vdash p$ and $\mathfrak{M}_2 \Vdash \neg p$.
- for any w of $\mathfrak{M}_1$, $\mathfrak{M}_1, w \Vdash \alpha(p)$, so $\mathfrak{M}_1 \uplus \mathfrak{M}_2, w \Vdash \alpha(p)$.
- this implies $\mathfrak{M}_1 \uplus \mathfrak{M}_2, u \Vdash p$ for every world u of $\mathfrak{M}_2$, thus $\mathfrak{M}_2 \Vdash p$, a contradiction.

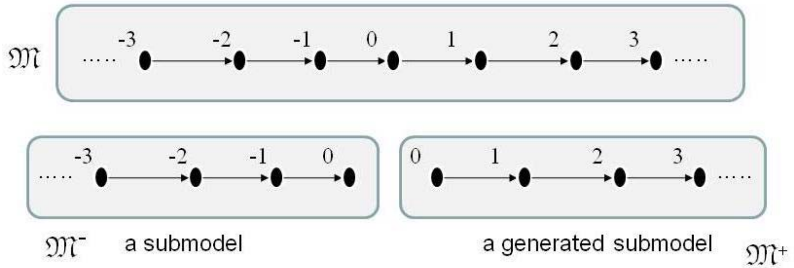
Generated Submodels: Definitions

- a model $\mathfrak{M}' = (W', R', \pi')$ is a submodel of $\mathfrak{M} = (W, R, \pi)$ if $W' \subseteq W$, $R' = R \cap (W' \times W')$ and $\pi'(p) = \pi(p) \cap W'$ for every p
- $\mathfrak{M}' \rightarrowtail \mathfrak{M}$: $\mathfrak{M}' = (W', R', \pi')$ is a generated submodel of $\mathfrak{M} = (W, R, \pi)$ if $\mathfrak{M}' = (W', R', \pi')$ is a submodel of $\mathfrak{M} = (W, R, \pi)$ and for all worlds w, if $w \in W'$ and $(w, u) \in R$, then $u \in W'$

Generated Submodels: Definitions and Invariance

- for $X \subseteq W$, the submodel generated by X is the smallest generated submodel whose domain contains X
- $X = \{w\}$ is a singleton: rooted or point generated model, w is the root
- if $\mathfrak{M}' \rightarrowtail \mathfrak{M}$, then for each wff φ and $w \in W'$, $\mathfrak{M}, w \Vdash \varphi$ iff $\mathfrak{M}', w \Vdash \varphi$
- $\mathfrak{M} = \biguplus_i \mathfrak{M}_i$ implies $\mathfrak{M}_i \rightarrowtail \mathfrak{M}$ for every $i \in I$

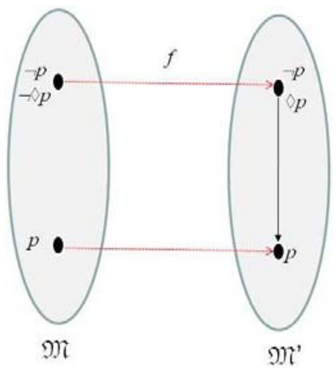
Generated Submodels: Example



Morphisms: Homomorphisms

- $f : \mathfrak{M} \to \mathfrak{M}'$: a homomorphisms from a model $\mathfrak{M} = (W, R, \pi)$ to a model $\mathfrak{M}' = (W', R', \pi')$ is a function $f : W \to W'$ such that for $w, u \in W$ and atomic proposition p
  - $w \in \pi(p)$ implies $f(w) \in \pi'(p)$ and
  - $(w, u) \in R$ implies $(f(w), f(u)) \in R'$
- $\mathfrak{M}$: the source and $\mathfrak{M}'$: the target

Homomorphisms: Example



modal formulas are not invariant under homomorphisms: $\mathfrak{M}, w \Vdash \neg\Diamond p$ but $\mathfrak{M}', f(w) \Vdash \Diamond p$

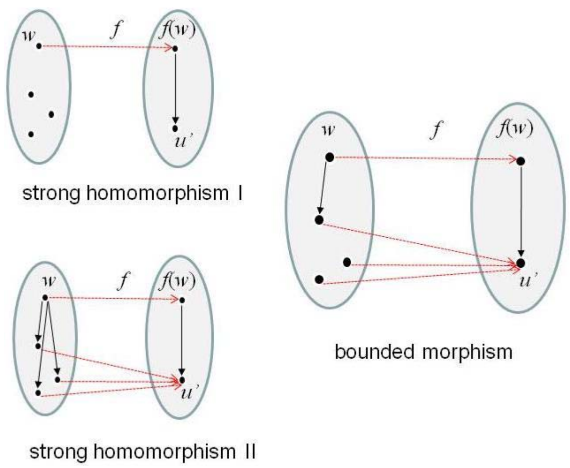
Morphisms: Strong Homomorphisms

- a homomorphism $f : \mathfrak{M} \to \mathfrak{M}'$: is a strong homomorphisms if it satisfies
  - $w \in \pi(p)$ iff $f(w) \in \pi'(p)$ and
  - $(w, u) \in R$ iff $(f(w), f(u)) \in R'$
- embedding: an injective (1-1) strong homomorphism
- isomorphism: a bijective (1-1 and onto) strong homomorphism
- if $f : \mathfrak{M} \to \mathfrak{M}'$ is a surjective (onto) strong homomorphism, then for each wff φ and $w \in W$, $\mathfrak{M}, w \Vdash \varphi$ iff $\mathfrak{M}', f(w) \Vdash \varphi$

Morphisms: Bounded Morphisms

- a bounded morphisms from a model $\mathfrak{M} = (W, R, \pi)$ to a model $\mathfrak{M}' = (W', R', \pi')$ is a function $f : W \to W'$ such that for $w, u \in W$, $v' \in W'$, and proposition letter p
  - $w \in \pi(p)$ iff $f(w) \in \pi'(p)$;
  - $(w, u) \in R$ implies $(f(w), f(u)) \in R'$; and
  - if $(f(w), u') \in R'$ then there exists $u \in W$ such that $(w, u) \in R$ and $f(u) = u'$ (back condition)
- $f : \mathfrak{M} \twoheadrightarrow \mathfrak{M}'$ if f is a surjective (onto) bounded morphism
- if $f : \mathfrak{M} \to \mathfrak{M}'$ is a bounded morphism, then for each wff φ and $w \in W$, $\mathfrak{M}, w \Vdash \varphi$ iff $\mathfrak{M}', f(w) \Vdash \varphi$

Strong Homomorphism and Bounded Morphisms: Difference



Bisimulations: Definitions and Invariance

- $Z : \mathfrak{M} \underline{\leftrightarrow} \mathfrak{M}'$: a bisimulation between $\mathfrak{M} = (W, R, \pi)$ and $\mathfrak{M}' = (W', R', \pi')$ is a relation $Z \subseteq W \times W'$ such that
  - if wZw' then $w \in \pi(p)$ iff $w' \in \pi'(p)$ for any p;
  - if wZw' and $(w, u) \in R$ then there exists $u' \in W'$ such that uZu' and $(w', u') \in R'$(forth condition); and
  - if wZw' and $(w', u') \in R'$ then there exists $u \in W$ such that uZu' and $(w, u) \in R$ (back condition)
- if $Z : \mathfrak{M} \underline{\leftrightarrow} \mathfrak{M}'$ and wZw' then w and w' are bisimular, denoted by $Z : \mathfrak{M}, w \underline{\leftrightarrow} \mathfrak{M}', w'$

Bisimulations: Definitions and Invariance

- if for some $Z : \mathfrak{M}, w \underline{\leftrightarrow} \mathfrak{M}', w'$, we write $\mathfrak{M}, w \underline{\leftrightarrow} \mathfrak{M}', w'$ or $w \underline{\leftrightarrow} w'$
- if for some $Z : \mathfrak{M} \underline{\leftrightarrow} \mathfrak{M}'$, we write $\mathfrak{M} \underline{\leftrightarrow} \mathfrak{M}'$
- if $\mathfrak{M}, w \underline{\leftrightarrow} \mathfrak{M}', w'$ then $\mathfrak{M}, w \Vdash \varphi$ iff $\mathfrak{M}', w' \Vdash \varphi$ for each wff φ
- the invariance can be proved by induction on the structure of φ

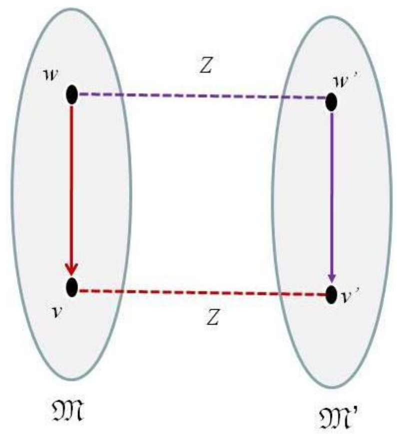
Bisimulations and Related Notions

- if $\mathfrak{M}$ and $\mathfrak{M}'$ are isomorphic, then $\mathfrak{M} \underline{\leftrightarrow} \mathfrak{M}'$
- disjoint union: for every $i \in I$ and $w \in \mathfrak{M}_i$, $\mathfrak{M}_i, w \underline{\leftrightarrow} \biguplus_i \mathfrak{M}_i, w$
- generated submodel: if $\mathfrak{M}' \rightarrowtail \mathfrak{M}$, then $\mathfrak{M}', w \underline{\leftrightarrow} \mathfrak{M}, w$ for all w in $\mathfrak{M}'$
- bounded morphism: if $f : \mathfrak{M} \twoheadrightarrow \mathfrak{M}'$, then $\mathfrak{M}, w \underline{\leftrightarrow} \mathfrak{M}', f(w)$ for all w in $\mathfrak{M}$

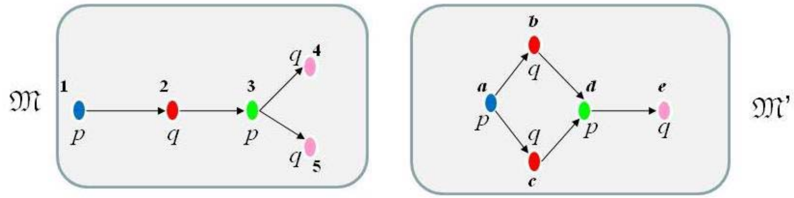
Bisimulations and Computation

- computational interpretation of a model: a process (a finite state automaton if the model is finite)
- a possible world is a state
- the accessibility relation is simply the state transition relation
- the set of wff true in a state is the language accepted by the automaton with the state as the initial state
- bisimulation: two model are bisimilar if they are observationally equivalent black boxes

Bisimulations: Back and Forth Conditions

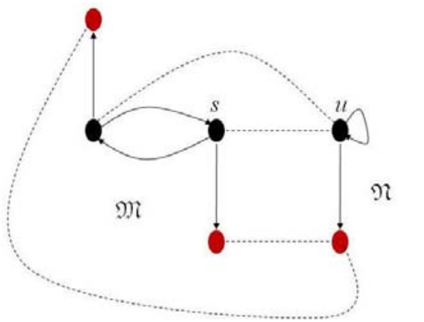


Bisimulations: Example I



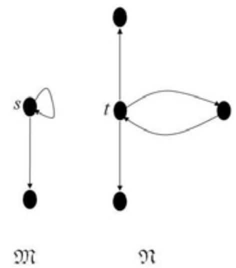
$$Z = \{(1, a), (2, b), (2, c), (3, d), (4, e), (5, e)\}$$

Bisimulations: Example II



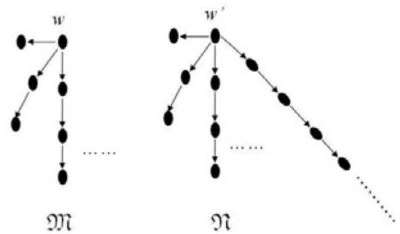
- bisimulation: $\mathfrak{M}, s \underline{\leftrightarrow} \mathfrak{N}, u$
- modal equivalence: let $\Phi_0 = \emptyset$, then for each wff φ, $\mathfrak{M}, s \Vdash \varphi$ iff $\mathfrak{N}, u \Vdash \varphi$
- bisimulation implies modal equivalence

Bisimulations: Example III



- $\mathfrak{M}, s$ and $\mathfrak{N}, t$ are not bisimilar
- $\mathfrak{M}, s \Vdash \Box(\Box\bot \vee \Diamond\Box\bot)$ and $\mathfrak{N}, t \nVdash \Box(\Box\bot \vee \Diamond\Box\bot)$
- $\mathfrak{M}, w \Vdash \Box\bot$ means that w is an end point
- not bisimular and not modally equivalent

Bisimulations: Example IV



- each of $\mathfrak{M}$ and $\mathfrak{N}$ has a finite branch of length n for each $n > 0$
- $\mathfrak{N}$ has an additional infinite branch
- let $\Phi_0 = \emptyset$, then for each wff φ, $\mathfrak{M}, w \Vdash \varphi$ iff $\mathfrak{N}, w' \Vdash \varphi$
- however, w and w' are not bisimular
- not bisimular but modally equivalent

Bisimulations: Hennessy-Milner Theorem

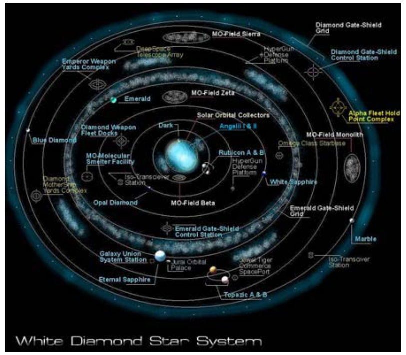
- a model $\mathfrak{M} = (W, R, \pi)$ is image-finite if for all $w \in W$ $R(w) = \{u \mid (w,u) \in R\}$ is finite
- $w \leftrightsquigarrow w'$: let $\mathfrak{M} = (W, R, \pi)$ and $\mathfrak{M}' = (W', R', \pi')$ be two models, then $w \in W$ and $w' \in W'$ are modally equivalent if for each wff φ, $\mathfrak{M}, w \Vdash \varphi$ iff $\mathfrak{M}', w' \Vdash \varphi$
- Hennessy-Milner theorem: let $\mathfrak{M} = (W, R, \pi)$ and $\mathfrak{M}' = (W', R', \pi')$ be two image-finite models, then for every $w \in W$ and $w' \in W'$, $w \underline{\leftrightarrow} w'$ iff $w \leftrightsquigarrow w'$

Proof of Hennessy-Milner Theorem

- $w \underline{\leftrightarrow} w'$ implies $w \leftrightsquigarrow w'$: the invariance theorem
- $w \leftrightsquigarrow w'$ implies $w \underline{\leftrightarrow} w'$: $\leftrightsquigarrow$ is itself a bisimulation
  1. the first condition is immediate, so proof of forth condition
  2. assume that $w \leftrightsquigarrow w'$ and $(w, u) \in R$
  3. if there is no $u' \in W'$ such that $(w', u') \in R$ and $u \leftrightsquigarrow u'$
  4. let $S' = R'(w')$, then S' is finite and nonempty
  5. $S' = \{w'_1, \cdots, w'_n\}$
  6. for every $w'_i \in S'$, there exists ψ_i such that $\mathfrak{M}, u \Vdash \psi_i$ but $\mathfrak{M}', w'_i \nVdash \psi_i$
  7. $\mathfrak{M}, w \Vdash \Diamond(\wedge_i \psi_i)$ but $\mathfrak{M}, w' \nVdash \Diamond(\wedge_i \psi_i)$
  8. contradiction with $w \leftrightsquigarrow w'$

Normal Systems of Modal Logic

Let us make systems out of the diamonds



Normal Systems of Modal Logic

- Hilbert-Style Axiomatization of Normal Systems
- Basic Notions of Proof Theory
- Properties of Proof-Theoretic Notions

Normal Systems of Modal Logic—Motivation

Q: given a class of models C, are there syntactic mechanisms capable of generating the formulas valid on C?

A: the normal systems

Hilbert-Style Axiomatization—Axiom Schemata

- PL: all instances of propositional tautologies
- Dual: $\Diamond\varphi \equiv \neg\Box\neg\varphi$
- **K**: $\Box(\varphi \supset \psi) \supset (\Box\varphi \supset \Box\psi)$
- **D**: $\Box\varphi \supset \Diamond\varphi$
- **T**: $\Box\varphi \supset \varphi$
- **B**: $\varphi \supset \Box\Diamond\varphi$
- **4**: $\Box\varphi \supset \Box\Box\varphi$
- **5**: $\Diamond\varphi \supset \Box\Diamond\varphi$

Hilbert-Style Axiomatization—Rules of Inference

- R1 (Modus ponens, MP):

$$\frac{\varphi \quad \varphi \supset \psi}{\psi}$$

- R2 (Generalization, Gen):

$$\frac{\varphi}{\Box\varphi}$$

Remarks on Axiomatic Schemata

- PL: the starting point for modal reasoning
- **K**:
  - distribution axiom: the distribution of $\Box$ operator over $\supset$ operator
  - transform $\Box(\varphi \supset \psi)$ into $(\Box\varphi \supset \Box\psi)$
  - valid in all Kripke models (prove it!)
  - alethic reading: if φ necessarily implies ψ and φ is necessary, then ψ is necessary
  - epistemic reading: if an (ideal) agent knows that φ implies ψ and knows φ, then he also knows ψ

Remarks on Axiom Schemata

- Dual: why do we need it?
  - expansion of shorthand: $\Diamond\varphi \equiv \neg\neg\Diamond\neg\neg\varphi$
  - by PL: $\Diamond\varphi \equiv \Diamond\neg\neg\varphi$
  - we need it because $\mathbf{K}$+PL only give us $\Box\varphi \equiv \Box\neg\neg\varphi$, which in turn give us $\Diamond\neg\varphi \equiv \Diamond\neg\neg\neg\varphi$ (with expansion of $\Box$ and PL)

Remarks on Axiom Schemata

- $\mathbf{D}$:
  - alethic reading: if something is necessary, then it is possible
  - deontic reading: if something is obligatory, then it is permitted
- $\mathbf{T}$:
  - alethic reading: if something is necessary, then it is actually true
  - epistemic reading: what is known is true (verity of knowledge)
  - knowledge axiom or truth axiom
  - distinguished feature of knowledge from belief

Remarks on Axiom Schemata

- $\mathbf{B}$: what is actually true is necessarily possible
- $\mathbf{4}$:
  - positive introspection axiom
  - epistemic reading: if you know something, then you know that you know it
- $\mathbf{5}$:
  - it is equivalent to $\neg\Box\varphi \supset \Box\neg\Box\varphi$
  - negative introspection axiom
  - epistemic reading: if you don't know something, then you know that you don't know it

Normal Systems of Modal Logic

- the minimal normal system $\mathbf{K}$: PL+Dual+$\mathbf{K}$+MP+Gen
- Lemmon code for normal systems: $\mathbf{KX_0} \ldots \mathbf{X_{m-1}}$ denote the system $\mathbf{K}$ plus axiomatic schemata $\mathbf{X_0}, \ldots,$ and $\mathbf{X_{m-1}}$
- some well-known systems
  1. $\mathbf{KT}$=$\mathbf{T}$= the Gödel/Feys/Von Wright system
  2. $\mathbf{KT4}$=$\mathbf{S4}$
  3. $\mathbf{KT4B}$=$\mathbf{KT45}$=$\mathbf{S5}$=epistemic system
  4. $\mathbf{KD}$= deontic $\mathbf{T}$
  5. $\mathbf{KD4}$=deontic $\mathbf{S4}$
  6. $\mathbf{KD45}$=deontic $\mathbf{S5}$=doxastic system
  7. $\mathbf{KTB}$=the Brouwer (Brouwersche) system

Normal Systems of Modal Logic

- Hilbert-Style Axiomatization of Normal Systems
- Basic Notions of Proof Theory
- Properties of Proof-Theoretic Notions

Proof Theory: Basic Notions

- $\mathbf{S}$: a normal system, Σ: a set of wffs, φ: a wff
- $\mathbf{S}$-proof: a finite sequence of wffs, each of which is an instance of an axiom schema in $\mathbf{S}$, or follows from one or more earlier items in the sequence by applying a rule of inference
- $\vdash_{\mathbf{S}} \varphi$:
  - φ is a theorem of $\mathbf{S}$
  - there is an $\mathbf{S}$-proof $\varphi_0, \cdots, \varphi_k$ such that $\varphi = \varphi_k$

Proof Theory: Basic Notions

- $\Sigma \vdash_{\mathbf{S}} \varphi$:
  - φ is a local syntactic consequence of φ in $\mathbf{S}$
  - there some finite subset $\{\sigma_1, \cdots, \sigma_n\} \subseteq \Sigma$ such that $\vdash_{\mathbf{S}} \sigma_1 \wedge \cdots \wedge \sigma_n \supset \varphi$
- $\Sigma \vdash^g_{\mathbf{S}} \varphi$:
  - φ is a global syntactic consequence of φ in $\mathbf{S}$
  - there is a finite sequence of wffs $\varphi_0, \cdots, \varphi_k$ such that $\varphi = \varphi_k$ and each φ_i is
    - ∗ an instance of an axiom schema in $\mathbf{S}$
    - ∗ an element of Σ, or
    - ∗ follows from one or more earlier items in the sequence by applying a rule of inference

Proof Theory: Basic Notions

- Σ is $\mathbf{S}$-inconsistent: $\Sigma \vdash_{\mathbf{S}} \perp$; otherwise, Σ is $\mathbf{S}$-consistent
- Σ is $\mathbf{S}$-maximal: Σ is $\mathbf{S}$-consistent and for any $\varphi \notin \Sigma$, $\Sigma \cup \{\varphi\}$ is $\mathbf{S}$-inconsistent
- Σ is $\mathbf{S}$-closed: if $\Sigma \vdash_{\mathbf{S}} \varphi$, then $\varphi \in \Sigma$
- Σ is an $\mathbf{S}$-system: if Σ is $\mathbf{S}$-closed

Proof Theory: Example

- $\mathbf{K}$-proof of $(\Box p \wedge \Box q) \supset \Box(p \wedge q)$

1.	$p \supset (q \supset (p \wedge q))$	PL
2.	$\Box(p \supset (q \supset (p \wedge q)))$	Gen : 1
3.	$\Box(p \supset (q \supset (p \wedge q))) \supset (\Box p \supset \Box(q \supset (p \wedge q)))$	Inst. of $\mathbf{K}$
4.	$\Box p \supset \Box(q \supset (p \wedge q))$	MP : $2, 3$
5.	$\Box(q \supset (p \wedge q)) \supset (\Box q \supset \Box(p \wedge q))$	Inst. of $\mathbf{K}$
6.	$\Box p \supset (\Box q \supset \Box(p \wedge q))$	PL : $4, 5$
7.	$(\Box p \wedge \Box q) \supset \Box(p \wedge q)$	PL : 6

Normal Systems of Modal Logic

- Hilbert-Style Axiomatization of Normal Systems
- Basic Notions of Proof Theory
- Properties of Proof-Theoretic Notions

Local Syntactic Consequence: Properties

1. $\vdash_{\mathbf{S}} \varphi$ iff $\emptyset \vdash_{\mathbf{S}} \varphi$ iff for every Σ, $\Sigma \vdash_{\mathbf{S}} \varphi$
2. If $\Sigma \vdash_{\mathsf{PL}} \varphi$ then $\Sigma \vdash_{\mathbf{S}} \varphi$
3. If $\varphi \in \Sigma$, then $\Sigma \vdash_{\mathbf{S}} \varphi$
4. Cut: if $\Sigma \vdash_{\mathbf{S}} \psi$ and $\{\psi\} \vdash_{\mathbf{S}} \varphi$, then $\Sigma \vdash_{\mathbf{S}} \varphi$
5. If $\Sigma \vdash_{\mathbf{S}} \varphi$ and $\Sigma \subseteq \Gamma$ then $\Gamma \vdash_{\mathbf{S}} \varphi$
6. Compactness theorem: $\Sigma \vdash_{\mathbf{S}} \varphi$ iff there is a finite subset Γ of Σ such that $\Gamma \vdash_{\mathbf{S}} \varphi$
7. Deduction theorem: $\Sigma \vdash_{\mathbf{S}} \varphi \supset \psi$ iff $\Sigma \cup \{\varphi\} \vdash_{\mathbf{S}} \psi$

Consistency: Properties

1. Σ is $\mathbf{S}$-consistent iff there is a φ such that $\Sigma \nvdash_{\mathbf{S}} \varphi$
2. Σ is $\mathbf{S}$-consistent iff there is no φ such that both $\Sigma \vdash_{\mathbf{S}} \varphi$ and $\Sigma \vdash_{\mathbf{S}} \neg\varphi$
3. If Σ is $\mathbf{S}$-consistent and $\Gamma \subseteq \Sigma$, then Γ is $\mathbf{S}$-consistent
4. Compactness theorem: Σ is $\mathbf{S}$-consistent iff every finite subset of Σ is
5. $\Sigma \vdash_{\mathbf{S}} \varphi$ iff $\Sigma \cup \{\neg\varphi\}$ is $\mathbf{S}$-inconsistent
6. $\Sigma \nvdash_{\mathbf{S}} \neg\varphi$ iff $\Sigma \cup \{\varphi\}$ is $\mathbf{S}$-consistent

Maximality: Properties I

Let Σ be an $\mathbf{S}$-maximal set of wffs. Then:

1. $\varphi \in \Sigma$ iff $\Sigma \vdash_{\mathbf{S}} \varphi$
2. Σ is $\mathbf{S}$-closed and an $\mathbf{S}$-system
3. $\bot \notin \Sigma$
4. $\top \in \Sigma$
5. $\neg\varphi \in \Sigma$ iff $\varphi \notin \Sigma$
6. $\varphi \wedge \psi \in \Sigma$ iff both $\varphi \in \Sigma$ and $\psi \in \Sigma$
7. $\varphi \vee \psi \in \Sigma$ iff either $\varphi \in \Sigma$ or $\psi \in \Sigma$
8. $\varphi \supset \psi \in \Sigma$ iff if $\varphi \in \Sigma$ then $\psi \in \Sigma$
9. $\varphi \equiv \psi \in \Sigma$ iff $\varphi \in \Sigma$ if and only if $\psi \in \Sigma$

Lindenbaum Lemma

- if Σ is $\mathbf{S}$-consistent, then there exists an $\mathbf{S}$-maximal set of wffs Γ such that $\Sigma \subseteq \Gamma$
- Γ is called an $\mathbf{S}$-maximal extension of Σ

Lindenbaum Construction

1. Assume a fixed enumeration of all wffs: $\varphi_1, \varphi_2, \cdots$
2. Define $\Gamma_0 = \Sigma$
3. For $n > 0$,

$$\Gamma_n = \begin{cases} \Gamma_{n-1} \cup \{\varphi_n\}, & \text{if it is } \mathbf{S}\text{-consistent} \\ \Gamma_{n-1}, & \text{otherwise} \end{cases}$$

4. $\Gamma = \bigcup_{n \geq 0} \Gamma_n$

Proof of Lindenbaum Lemma

1. for $n \geq 0$, Γ_n is $\mathbf{S}$-consistent
2. for $n \geq 0$, $\Gamma_n \subseteq \Gamma$, so $\Sigma = \Gamma_0 \subseteq \Gamma$
3. for $n \geq k \geq 0$, $\Gamma_k \subseteq \Gamma_n$
4. for $n > 0$, if $\varphi_n \in \Gamma$, then $\varphi_n \in \Gamma_n$
5. for any finite subset Γ' of Γ, $\Gamma' \subseteq \Gamma_n$ for some $n \geq 0$
6. Γ is $\mathbf{S}$-consistent (by 1 and 5)
7. for every φ, if $\Gamma \cup \{\varphi\}$ is $\mathbf{S}$-consistent, then $\varphi \in \Gamma$
8. Γ is $\mathbf{S}$-maximal

Corollaries of Lindenbaum Lemma

1. $\Sigma \vdash_{\mathbf{S}} \varphi$ iff φ is in every $\mathbf{S}$-maximal extension of Σ
2. $\vdash_{\mathbf{S}} \varphi$ iff φ is in every $\mathbf{S}$-maximal set
3. $|\varphi|_{\mathbf{S}}$:
   - the proof set of φ in $\mathbf{S}$
   - the set of all $\mathbf{S}$-maximal sets containing φ

Proof Set: Properties

- Let Σ be $\mathbf{S}$-maximal, then $\Sigma \in |\varphi|_{\mathbf{S}}$ iff $\varphi \in \Sigma$ iff $\Sigma \vdash_{\mathbf{S}} \varphi$
- $|\varphi|_{\mathbf{S}} \subseteq |\psi|_{\mathbf{S}}$ iff $\vdash_{\mathbf{S}} \varphi \supset \psi$
- $|\varphi|_{\mathbf{S}} = |\psi|_{\mathbf{S}}$ iff $\vdash_{\mathbf{S}} \varphi \equiv \psi$
- $|\bot|_{\mathbf{S}} = \emptyset$
- $|\top|_{\mathbf{S}} =$ the set of all $\mathbf{S}$-maximal sets
- $|\neg\varphi|_{\mathbf{S}} = |\top|_{\mathbf{S}} - |\varphi|_{\mathbf{S}}$
- $|\varphi \wedge \psi|_{\mathbf{S}} = |\varphi|_{\mathbf{S}} \cap |\psi|_{\mathbf{S}}$
- $|\varphi \vee \psi|_{\mathbf{S}} = |\varphi|_{\mathbf{S}} \cup |\psi|_{\mathbf{S}}$

Maximality: Properties II

Let Σ and Γ be $\mathbf{S}$-maximal sets of wffs. Then:

1. $\{\varphi \mid \Box\varphi \in \Sigma\} \subseteq \Gamma$ iff $\{\Diamond\varphi \mid \varphi \in \Gamma\} \subseteq \Sigma$
2. $\Box\psi \in \Sigma$ iff for every $\mathbf{S}$-maximal set of wffs Γ such that $\{\varphi \mid \Box\varphi \in \Sigma\} \subseteq \Gamma$, $\psi \in \Gamma$
3. $\Diamond\psi \in \Sigma$ iff for some $\mathbf{S}$-maximal set of wffs Γ such that $\{\Diamond\varphi \mid \varphi \in \Gamma\} \subseteq \Sigma$, $\psi \in \Gamma$

Maximality: Proof of Property II.1

- left to right

$$
\begin{array}{ll}
 & \{\varphi \mid \Box\varphi \in \Sigma\} \subseteq \Gamma \text{ and } \varphi \in \Gamma \\
\Rightarrow & \neg\varphi \notin \Gamma \\
\Rightarrow & \Box\neg\varphi \notin \Sigma \\
\Rightarrow & \neg\Box\neg\varphi \in \Sigma \\
\Rightarrow & \Diamond\varphi \in \Sigma
\end{array}
$$

- right to left

$$
\begin{array}{ll}
 & \{\Diamond\varphi \mid \varphi \in \Gamma\} \subseteq \Sigma \text{ and } \Box\varphi \in \Sigma \\
\Rightarrow & \neg\Diamond\neg\varphi \in \Sigma \\
\Rightarrow & \Diamond\neg\varphi \notin \Sigma \\
\Rightarrow & \neg\varphi \notin \Gamma \\
\Rightarrow & \varphi \in \Gamma
\end{array}
$$

Maximality: Proof of Property II.2

- left to right: trivial
- right to left
  1. Suppose that ψ is in every $\mathbf{S}$-maximal extension of $\{\varphi \mid \Box\varphi \in \Sigma\}$
  2. $\{\varphi \mid \Box\varphi \in \Sigma\} \vdash_{\mathbf{S}} \psi$ (by corollary of Lindenbaum lemma)
  3. there are wffs $\varphi_1 \cdots \varphi_n \in \{\varphi \mid \Box\varphi \in \Sigma\}$ such that $\vdash_{\mathbf{S}} (\varphi_1 \wedge \cdots \wedge \varphi_n) \supset \psi$ (by def)
  4. $\vdash_{\mathbf{S}} (\Box\varphi_1 \wedge \cdots \wedge \Box\varphi_n) \supset \Box\psi$ (by modal reasoning)
  5. $\Sigma \vdash_{\mathbf{S}} \Box\varphi_i$ for $1 \leq i \leq n$ (by 3 and maximality of Σ)
  6. $\Sigma \vdash_{\mathbf{S}} \Box\psi$ (by 4,5, and modal reasoning)
  7. $\Box\psi \in \Sigma$ (by 6 and maximality of Σ)

Maximality: Proof of Property II.3

$\Diamond\psi \in \Sigma$

iff $\neg\Box\neg\psi \in \Sigma$ (by Dual and maximality of Σ)

iff $\Box\neg\psi \notin \Sigma$ (by maximality of Σ)

iff for some $\mathbf{S}$-maximal set of wffs Γ such that $\{\varphi \mid \Box\varphi \in \Sigma\} \subseteq \Gamma$, $\neg\psi \notin \Gamma$ (by Property II.2)

iff for some $\mathbf{S}$-maximal set of wffs Γ such that $\{\Diamond\varphi \mid \varphi \in \Gamma\} \subseteq \Sigma$, $\neg\psi \notin \Gamma$ (by Property II.1)

iff for some $\mathbf{S}$-maximal set of wffs Γ such that $\{\Diamond\varphi \mid \varphi \in \Gamma\} \subseteq \Sigma$, $\psi \in \Gamma$ (by maximality of Γ)

Meta-Theorems of Normal Systems

Let us take a closer look at the systems

Meta-Theorems of Normal Systems

- Soundness
- Completeness
- Finite Model Property and Decidability

Classes of Models

- D: the class of all serial models
- T: the class of all reflexive models
- B: the class of all symmetric models
- 4: the class of all transitive models
- 5: the class of all Euclidean models

Correspondence between Axioms and Classes of Models

every instance of the axiom schema $\mathbf{X}$ is valid in the corresponding class of models X as shown in the following table:

Schema	$\mathbf{D}$	$\mathbf{T}$	$\mathbf{B}$	$\mathbf{4}$	$\mathbf{5}$
Model Classes	D	T	B	4	5

let us prove the correspondence between $\mathbf{B}$ and symmetric models as an example $\downarrow$

Correspondence between Axioms and Classes of Models

1. let $\mathfrak{M} = (W, R, \pi)$ be any symmetric model, φ be any wff, and $w \in W$ such that $\mathfrak{M}, w \Vdash \varphi$
2. for any u such that $(w, u) \in R$, we have $(u, w) \in R$, so $\mathfrak{M}, u \Vdash \Diamond\varphi$
3. therefore, $\mathfrak{M}, w \Vdash \Box\Diamond\varphi$
4. $\mathfrak{M} \Vdash \varphi \supset \Box\Diamond\varphi$

Fifteen Distinct Normal Systems

	$\mathbf{K}$	$\mathbf{KD}$	$\mathbf{KT}$	$\mathbf{KB}$	$\mathbf{K4}$	$\mathbf{K5}$	$\mathbf{KDB}$	$\mathbf{KD4}$	$\mathbf{KD5}$	$\mathbf{K45}$
serial		•					•	•	•	
reflexive			•							
symmetry				•			•			
transitive					•			•		•
Euclidean						•			•	•

Fifteen Distinct Normal Systems

	KD45	KB4		KTB	KT4	KT5			
serial	•							•	•
reflexive				•	•	•	•		
symmetry		•	•	•			•	•	•
transitive	•	•			•		•	•	
Euclidean	•		•			•			•

Soundness

Let $\mathbf{S}$ be the normal system $\mathbf{KX_1 \ldots X_n}$ $(n \geq 0)$ and $\mathtt{C}$ denote $\mathtt{C_1} \cap \ldots \cap \mathtt{C_n}$ where each $\mathtt{C_i}$ is the corresponding class of models for axiom schema $\mathbf{X_i}$. Then for any subset of wffs Σ and wff φ,

1. if $\vdash_{\mathbf{S}} \varphi$ then $\Vdash_{\mathtt{C}} \varphi$
2. if $\Sigma \vdash_{\mathbf{S}} \varphi$ then $\Sigma \Vdash_{\mathtt{C}} \varphi$

Proof of Soundness

- 2 follows from 1 by definition
- proof of 1: by induction on the length of an $\mathbf{S}$-proof
  - every instance of axiom schemata is valid in the corresponding class of models
  - every application of inference rules preserves the validity

Meta-Theorems of Normal Systems

- Soundness
- Completeness
- Finite Model Property and Decidability

Completeness

Let $\mathbf{S}$ be the normal system $\mathbf{KX_1 \ldots X_n}$ ($n \geq 0$) and $\mathtt{C}$ denote $\mathtt{C}_1 \cap \ldots \cap \mathtt{C}_n$ where each $\mathtt{C}_i$ is the corresponding class of models for axiom schema $\mathbf{X_i}$. Then for any subset of wffs Σ and wff φ,

1. if $\Sigma \Vdash_{\mathtt{C}} \varphi$ then $\Sigma \vdash_{\mathbf{S}} \varphi$
2. if $\Vdash_{\mathtt{C}} \varphi$ then $\vdash_{\mathbf{S}} \varphi$

Proof of Completeness

- suppose that $\Sigma \nvdash_{\mathbf{S}} \varphi$
- $\Sigma \cup \{\neg\varphi\}$ is $\mathbf{S}$-consistent (by property 6 of consistency)
- existence of $\mathbf{S}$-maximal extension of $\Sigma \cup \{\neg\varphi\}$ (by Lindenbaum lemma)
- canonical model construction
- verify that the canonical model is in $\mathtt{C}$
- $\Sigma \cup \{\neg\varphi\}$ is $\mathbf{S}$-satisfiable in the canonical model (truth lemma)
- $\Sigma \nVdash_{\mathtt{C}} \varphi$ (by the definition of validity)

Canonical Model Construction

$$\mathfrak{M} = (W, R, \pi)$$

- W: the set of all $\mathbf{S}$-maximal sets of wffs
  - each world is a $\mathbf{S}$-maximal set
  - each world w is identified with an $\mathbf{S}$-maximal set Σ_w
  - there is a world containing $\Sigma \cup \{\neg\varphi\}$
- $(w, u) \in R$ iff $\{\varphi \mid \Box\varphi \in \Sigma_w\} \subseteq \Sigma_u$
- $\pi(p) = |p|_{\mathbf{S}}$ (the proof set of p) for every atomic proposition p

Properties of the Canonical Model

- if $\mathbf{S}$ contains $\mathbf{D}$, then $\mathfrak{M}$ is serial
- if $\mathbf{S}$ contains $\mathbf{T}$, then $\mathfrak{M}$ is reflexive
- if $\mathbf{S}$ contains $\mathbf{B}$, then $\mathfrak{M}$ is symmetric
- if $\mathbf{S}$ contains $\mathbf{4}$, then $\mathfrak{M}$ is transitive
- if $\mathbf{S}$ contains $\mathbf{5}$, then $\mathfrak{M}$ is Euclidean

let us prove item 4 as an example $\downarrow$

Properties of the Canonical Model

1. suppose $\mathbf{S}$ contains $\mathbf{4}$, (w, u) and $(u, v) \in R$
2. $\Box\varphi \supset \Box\Box\varphi \in \Sigma_w$ (1 and property I.1 of maximality)
3. $\{\varphi \mid \Box\varphi \in \Sigma_w\} \subseteq \Sigma_u$ (1 and def. of canonical model)
4. $\{\varphi \mid \Box\varphi \in \Sigma_u\} \subseteq \Sigma_v$ (1 and def. of canonical model)
5. let us consider any $\Box\varphi \in \Sigma_w$, then $\Box\Box\varphi \in \Sigma_w$ (2 and property I.8 of maximality)
6. $\Box\varphi \in \Sigma_u$ (3 and 5)
7. $\varphi \in \Sigma_v$ (4 and 6)
8. $(w, v) \in R$ (5, 7, and def. of canonical model)

Truth Lemma

$$\mathfrak{M}, w \Vdash \varphi \text{ iff } \varphi \in \Sigma_w$$

- by induction on the structure of φ
- induction base: by definition of π and properties of a proof set
- induction step for $\neg\psi$, $\varphi_1 \wedge \varphi_2$: exercise
- induction step for $\Diamond\psi$:

  $\mathfrak{M}, w \Vdash \Diamond\psi$

  iff there exists u such that $(w, u) \in R$ and $\mathfrak{M}, u \Vdash \psi$ (by def. of satisfaction)

  iff there exists u such that $\{\varphi \mid \Box\varphi \in \Sigma_w\} \subseteq \Sigma_u$ and $\psi \in \Sigma_u$ (by def. of R and induction hyp.)

  iff for some Σ_u such that $\{\Diamond\varphi \mid \varphi \in \Sigma_u\} \subseteq \Sigma_w$, $\psi \in \Sigma_u$ (by property II.1 of maximality)

  iff $\Diamond\psi \in \Sigma_w$ (by property II.3 of maximality)

Proof of Completeness

- there is a $w \in W$ such that $\Sigma \cup \{\neg\varphi\} \subseteq \Sigma_w$
- $\mathfrak{M}, w \Vdash \psi$ for every wff ψ in $\Sigma \cup \{\neg\varphi\}$
- $\Sigma \cup \{\neg\varphi\}$ is $\mathbf{S}$-satisfiable in the canonical model
- $\Sigma \nVdash_{\mathbf{C}} \varphi$ (by the definition of validity)

Meta-Theorems of Normal Systems

- Soundness
- Completeness
- Finite Model Property and Decidability

Finite Model Property via Filtrations

- for a wff φ, find the set of all its subformulas $Sub(\varphi)$ (it's a finite set)
- filtrations of a model: for a (possibly infinite) model $\mathfrak{M} = (W, R, \pi)$, find a model that identifies as many worlds as possible according to $Sub(\varphi)$ (such a filtration of $\mathfrak{M}$ is finite)
- if φ is satisfiable in $\mathfrak{M}$, then it is also satisfiable in a filtration of $\mathfrak{M}$
- φ is satisfiable in a model iff it is satisfiable in a finite model
- the size of such a finite model is bounded by a function of the size of φ
- the satisfiability checking of φ is decidable by enumeration of all models within this bounded size

Subformula Closed Sets

- a set of wffs Σ is closed under subformulas (subformula closed) if for all wffs φ and ψ
  - if $\neg\varphi \in \Sigma$ then so is φ;
  - if $\Diamond\varphi \in \Sigma$ then so is φ; and
  - if $\varphi \wedge \psi \in \Sigma$ then so are φ and ψ
- Note: for a wff φ, $Sub(\varphi)$ is closed under subformulas
- for a model $\mathfrak{M} = (W, R, \pi)$ and a subformula closed set Σ, define an equivalence relation $\asymp_\Sigma \subseteq W \times W$ by

  $w \asymp_\Sigma u$ iff for all $\varphi \in \Sigma$: $(\mathfrak{M}, w \Vdash \varphi$ iff $\mathfrak{M}, u \Vdash \varphi)$
- $[w]_\Sigma$ (or simply $[w]$): the equivalence class of a world with respect to $\asymp_\Sigma$

Filtrations: Definition

Let $\mathfrak{M} = (W, R, \pi)$ be a model and Σ be a subformula closed set. Suppose $\mathfrak{M}^f_\Sigma$ is any model (W^f, R^f, π^f) such that

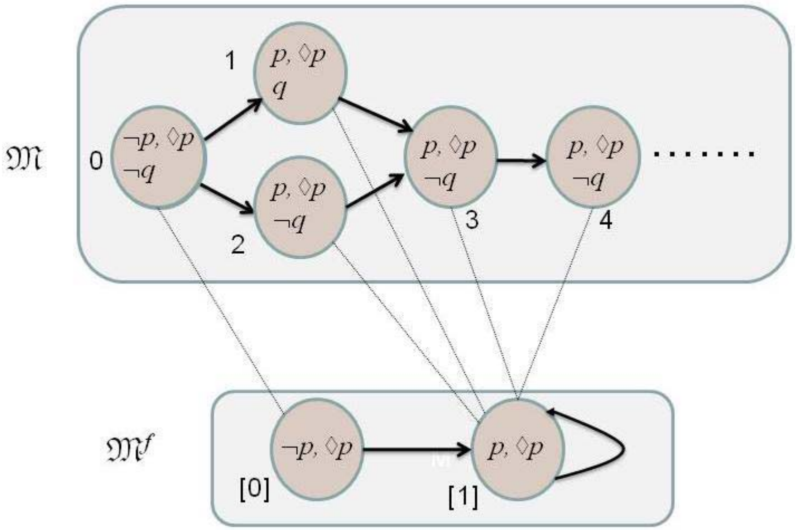
1. $W^f = W_\Sigma = \{[w]_\Sigma \mid w \in W\}$
2. if $(w, u) \in R$, then $([w], [u]) \in R^f$
3. if $([w], [u]) \in R^f$, then for all $\Diamond\varphi \in \Sigma$, if $\mathfrak{M}, u \Vdash \varphi$ then $\mathfrak{M}, w \Vdash \Diamond\varphi$
4. $\pi^f(p) = \{[w] \mid w \in \pi(p)\}$ for all atomic propositions p in Σ

Then $\mathfrak{M}^f_\Sigma$ is a filtration of $\mathfrak{M}$ through Σ.

Filtrations: Example

- $\mathfrak{M} = (\mathbb{N}, R, \pi)$
  - $R = \{(0,1), (0,2), (1,3)\} \cup \{(n, n+1) \mid n \geq 2\}$
  - $\pi(p) = \mathbb{N} - \{0\}$; $\pi(q) = \{1\}$
- $\Sigma = \{\Diamond p, p\}$
- $\asymp_\Sigma = \{(0,0)\} \cup \{(i,j) \mid i, j > 0\}$
- $\mathfrak{M}^f = (\{[0], [1]\}, R^f, \pi^f)$
  - $R^f = \{([0],[1]), ([1],[1])\}$
  - $\pi^f(p) = \{[1]\}$

Filtrations: Example



Filtration Theorem

Let $\mathfrak{M}^f_\Sigma = (W_\Sigma, R^f, \pi^f)$ be a filtration of $\mathfrak{M} = (W, R, \pi)$ through a subformula closed set Σ. Then for all wff $\varphi \in \Sigma$ and $w \in W$,

$$\mathfrak{M}, w \Vdash \varphi \Leftrightarrow \mathfrak{M}^f_\Sigma, [w] \Vdash \varphi$$

1. by induction on the structure of φ since Σ is subformula closed
2. induction base: by definition of π^f
3. Boolean cases: straightforward
4. $\mathfrak{M}, w \Vdash \Diamond\varphi \Rightarrow \mathfrak{M}^f_\Sigma, [w] \Vdash \Diamond\varphi$: clause 2 of the definition of filtration
5. $\mathfrak{M}^f_\Sigma, [w] \Vdash \Diamond\varphi \Rightarrow \mathfrak{M}, w \Vdash \Diamond\varphi$: clause 3 of the definition of filtration

Existence of Filtrations

let $\mathfrak{M} = (W, R, \pi)$ be a model and Σ be a subformula closed set.

1. define $R^s \subseteq W_\Sigma \times W_\Sigma$:
   - $([w], [u]) \in R^s$ iff there exist $w' \in [w]$ and $u' \in [u]$ such that $(w, u) \in R$
2. define $R^l \subseteq W_\Sigma \times W_\Sigma$:
   - $([w], [u]) \in R^l$ iff for all $\Diamond\varphi \in \Sigma$: $\mathfrak{M}, u \Vdash \varphi$ implies $\mathfrak{M}, w \Vdash \Diamond\varphi$
3. both (W_Σ, R^s, π^f) and (W_Σ, R^l, π^f) are filtrations of $\mathfrak{M}$ through Σ
4. if (W_Σ, R^f, π^f) is any filtration of $\mathfrak{M}$ through Σ then $R^s \subseteq R^f \subseteq R^l$

Filtrations: Remarks

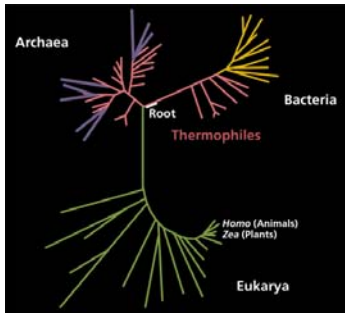
- all filtrations of $\mathfrak{M}$ preserve the reflexivity and seriality
- not all filtrations of $\mathfrak{M}$ preserve the transitivity, symmetry, and Euclideaness $\Rightarrow$ we need some techniques to select among the filtrations (Cf. Chellas, 1980)
- in some cases, we have to consider not only subformulas of a wff but also its modal closure

Finite Model Property and Decidability

- a filtration of $\mathfrak{M}$ through Σ has at most 2^n possible worlds if the cardinality of Σ is n
- if φ is satisfiable then it is satisfiable on a finite model containing at most $2^{|Sub(\varphi)|}$ possible worlds
- consistency checking (theoremhood, validity checking, and satisfiability test) in the fifteen normal systems mentioned above is decidable

Variants of Modal Logics

Let us meet the challenge of diversity



Variants of Modal Logic

- Generalization of Basic Modal Logic
- First-order Correspondence of Modal Logic
- Multi-agent Epistemic Logic
- Dynamic Logic

Modal Logic in a More General Setting

- we need more than one relations in the relational structure
- the arity of each relation may be greater than 2
- each k-ary relation corresponds to a $(k-1)$-ary modal operator
- example: in basic modal logic, the binary relation R corresponds to the unary modal operator $\Diamond$

General Modal Logic—Syntax

- modal similarity type: $\tau = (\Delta, \rho)$
  - Δ: a set of modal operators $\{\triangle_1, \triangle_2, \cdots\}$
  - $\rho : \Delta \to \mathbb{N}$ the arity function
- well-formed formulas: $ML(\tau, \Phi_0)$
  - any atomic propositional variable is a wff
  - $\perp$ is a wff
  - if φ and ψ are wffs, so are $\neg\varphi$ and $\varphi \wedge \psi$
  - if $\triangle \in \Delta$, $\rho(\triangle) = k$, and $\varphi_1, \cdots, \varphi_k$ are wffs, so is $\triangle(\varphi_1, \cdots, \varphi_k)$

General Modal Logic—Syntax

- $\nabla(\varphi_1, \cdots, \varphi_k)$: shorthand of $\neg \triangle (\neg\varphi_1, \cdots, \neg\varphi_k)$
- nullary modal operators: modal constants (also propositional constants)
- unary modal operators: $\triangle_i$ is usually written as $\Diamond_i$, and ∇_i as $\Box_i$
- binary modal operators: $\triangle(\varphi, \psi)$ is usually written as $\varphi \triangle \psi$

General Modal Logic—Semantics

- τ frame: $\mathfrak{F} = (W, (R_\triangle)_{\triangle \in \tau})$
  - W: a set of possible worlds (points, states, etc.)
  - $R_\triangle \subseteq W^{k+1}$ if $\rho(\triangle) = k$
- τ model: $\mathfrak{M} = (\mathfrak{F}, \pi)$
  - $\mathfrak{F}$: a τ frame
  - $\pi : \Phi_0 \to 2^W$: a truth assignment
- when $\rho(\triangle) > 0$, $\mathfrak{M}, w \Vdash \triangle(\varphi_1, \cdots, \varphi_k) \Leftrightarrow$ there exist $u_1, \cdots, u_k \in W$ such that $(w, u_1, \cdots, u_k) \in R_\triangle$ and $\mathfrak{M}, u_i \Vdash \varphi_i$ for $1 \le i \le k$
- when $\rho(\triangle) = 0$, $\mathfrak{M}, w \Vdash \triangle \Leftrightarrow w \in R_\triangle$

General Modal Logic—Semantics

- the difference between modal operators and Boolean connectives
  - Boolean connectives are truth-functional: the truth value of a wff in a world depends on the truth values of its components in the same world
  - modal operators are non-truth-functional: the truth value of a wff in a world depends on the truth values of its components in the accessible worlds
- example:
  - $\mathfrak{M}, w \Vdash \varphi \wedge \psi \Leftrightarrow \mathfrak{M}, w \Vdash \varphi$ and $\mathfrak{M}, w \Vdash \psi$
  - $\mathfrak{M}, w \Vdash \varphi \triangle \psi \Leftrightarrow$ there exist $u, v \in W$ such that $(w, u, v) \in R_\triangle$ and $\mathfrak{M}, u \Vdash \varphi$ and $\mathfrak{M}, v \Vdash \psi$

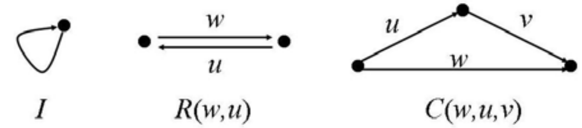
Example of General Modal Logic—Basic Temporal Logic

- modal similarity type: $\tau = (\Delta, \rho)$
  - $\Delta = \{F, P, X\}$
  - $\rho(F) = \rho(P) = \rho(X) = 1$
- temporal model: $\mathfrak{M} = (W, R_F, R_P, R_X, \pi)$
  - $W = \mathbb{Z}$: the set of integers (time points)
  - $(i, j) \in R_F$ if $i < j$
  - $(i, j) \in R_P$ if $i > j$
  - $(i, j) \in R_X$ if $j = i + 1$
- $\mathfrak{M}, i \Vdash F\varphi \Leftrightarrow$ there exist $j > i$ such that $\mathfrak{M}, j \Vdash \varphi$
- $\mathfrak{M}, i \Vdash P\varphi \Leftrightarrow$ there exist $j < i$ such that $\mathfrak{M}, j \Vdash \varphi$
- $\mathfrak{M}, i \Vdash X\varphi \Leftrightarrow \mathfrak{M}, i + 1 \Vdash \varphi$

Example of General Modal Logic—Arrow Logic

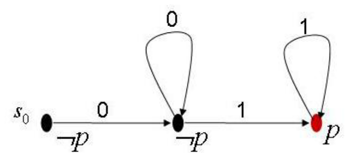
- modal similarity type: $\tau = (\Delta, \rho)$
  - $\Delta = \{\iota, \otimes, \circ\}$
  - $\rho(\iota) = 0, \rho(\otimes) = 1, \rho(\circ) = 2$
- arrow model: $\mathfrak{M} = (W, I, R, C, \pi)$
  - $W =$: a set of arrows (directed arcs)
  - $I \subseteq W$
  - $R \subseteq W \times W$
  - $C \subseteq W \times W \times W$

Example of General Modal Logic—Arrow Logic



- $\mathfrak{M}, w \Vdash \iota \Leftrightarrow \iota \in I$
- $\mathfrak{M}, w \Vdash \otimes\varphi \Leftrightarrow$ there exist $u \in W$ such that $(w, u) \in R$ and $\mathfrak{M}, u \Vdash \varphi$
- $\mathfrak{M}, w \Vdash \varphi\circ\psi \Leftrightarrow$ there exist $u, v \in W$ such that $(w, u, v) \in C$, $\mathfrak{M}, u \Vdash \varphi$, and $\mathfrak{M}, v \Vdash \psi$

Example of General Modal Logic—Finite State Automata Logic



finite state automation for $0^n1^m (n, m > 0)$

- modal similarity type: $\tau = (\{0, 1\}, \rho)$, $\rho(0) = \rho(1) = 1$
- $\Diamond_i$ is written as $\langle i \rangle$
- $\mathfrak{M}, s_0 \Vdash \langle 0 \rangle^n \langle 1 \rangle^m p$ for all $n, m > 0$

Example of General Modal Logic—Finite State Automata Logic

- a finite state automation: $A = (Q, I, \delta, s_0, F)$
  - Q: a finite set of states
  - I: a finite set of input symbols
  - $\delta \subseteq Q \times I \times Q$: (labeled) state transition relation
  - $s_0 \in Q$: initial state
  - $F \subseteq Q$: the set of final states
- $L(A) \subseteq I^*$: the language (set of strings) accepted by A

Example of General Modal Logic—Finite State Automata Logic

- modal similarity type: $\tau = (I, \rho)$ and $\rho(i) = 1$ for $i \in I$
- $\Phi_0 = \{p\}$
- $\mathfrak{M}_A = (Q, (R_i)_{i \in I}, \pi)$
  - $(s, t) \in R_i$ iff $(s, i, t) \in \delta$
  - $\pi(p) = F$
- if $\alpha = i_1 i_2 \cdots i_k \in I^*$ then $\langle \alpha \rangle = \langle i_1 \rangle \langle i_2 \rangle \cdots \langle i_k \rangle$
- $\mathfrak{M}, s_0 \Vdash \langle \alpha \rangle p$ iff $\alpha \in L(A)$

Variants of Modal Logic

- Generalization of Basic Modal Logic
- First-order Correspondence of Modal Logic
- Multi-agent Epistemic Logic
- Dynamic Logic

First Order Correspondence Language

- $ML(\tau, \Phi_0)$: modal language defined by the modal similarity type $\tau = (\Delta, \rho)$ and the set of atomic propositions Φ_0
- $\mathcal{L}^1_\tau(\Phi_0)$: first order language with equality which has:
  - unary predicates P_i for each $p_i \in \Phi_0$
  - $(n+1)$-ary predicate symbol $R_\triangle$ for $\triangle \in \Delta$ if $\rho(\triangle) = n$
- $\alpha(x)$ denote a FOL formula with one free variable x

Standard Translation from ML to FOL

- let x be a first order variable, $ST_x : ML(\tau, \Phi_0) \to \mathcal{L}^1_\tau(\Phi_0)$:
  1. $ST_x(p) = P(x)$ if $p \in \Phi_0$
  2. $ST_x(\bot) = x \neq x$
  3. $ST_x(\neg\varphi) = \neg ST_x(\varphi)$
  4. $ST_x(\varphi \wedge \psi) = ST_x(\varphi) \wedge ST_x(\psi)$
  5. $ST_x(\triangle(\varphi_1, \cdots, \varphi_n)) = \exists y_1 \ldots \exists y_n(R_\triangle(x, y_1, \cdots, y_n) \wedge ST_{y_1}(\varphi_1) \wedge \cdots \wedge ST_{y_1}(\varphi_n))$

Standard Translation from ML to FOL

- Kripke model $\mathfrak{M} = (W, (R_\triangle)_{\triangle\in\tau}, \pi)$ as an FOL interpretation
  - W: the domain of interpretation
  - $R_\triangle$: the interpretation of the predicate symbol $R_\triangle$)
  - $\pi(p)$: the interpretation of the predicate symbol P
- for all $\mathfrak{M} = (W, (R_\triangle)_{\triangle\in\tau}, \pi)$ and $w \in W$
  - $\mathfrak{M}, w \Vdash \varphi$ iff $\mathfrak{M} \Vdash ST_x(\varphi)[x \leftarrow w]$, where $x \leftarrow w$ means that we use a variable assignment such that w is assigned to x
  - $\mathfrak{M} \Vdash \varphi$ iff $\mathfrak{M} \Vdash \forall x ST_x(\varphi)$

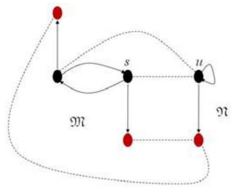
Standard Translation from ML to FOL: Example

$$\begin{aligned} ST_x(\Diamond(\Box p \supset q)) &= \exists y(Rxy \wedge ST_y(\Box p \supset q)) \\ &= \exists y(Rxy \wedge (ST_y(\Box p) \supset ST_y(q))) \\ &= \exists y(Rxy \wedge (\forall z(Ryz \supset ST_z(p)) \supset Qy)) \\ &= \exists y(Rxy \wedge (\forall z(Ryz \supset Pz) \supset Qy)) \end{aligned}$$

Importing Properties of FOL to ML

- compactness property: if Θ is a set of FOL formulas, and every finite subset of Θ is satisfiable, then so is Θ itself.
- Löwenheim-Skolem property: if a set of FOL formulas has an infinite model, then it has a countably infinite model
- modal logic has both these properties

Bisimulations: Example II Revisited



- bisimulation: $\mathfrak{M}, s \underline{\leftrightarrow} \mathfrak{N}, u$
- modal equivalence: let $\Phi_0 = \emptyset$, then for each modal wff φ, $\mathfrak{M}, s \Vdash \varphi$ iff $\mathfrak{N}, u \Vdash \varphi$
- not FOL equivalent: $R(x, x)$ is satisfiable in $\mathfrak{N}$ (with x assigned u) but not in $\mathfrak{M}$
- $R(x, x) \neq ST_x(\varphi)$ for any modal wff φ

van Benthem Characterization Theorem

- FOL formula $\alpha(x)$ is invariant for bisimulation if for all $\mathfrak{M}, w \underline{\leftrightarrow} \mathfrak{M}', w'$, $\mathfrak{M} \Vdash \alpha[x \leftarrow w]$ iff $\mathfrak{M}' \Vdash \alpha[x \leftarrow w']$
- characterization theorem: $\alpha(x)$ is invariant for bisimulation iff it is equivalent to the standard translation of a modal wff
- proof of "if" part: follows from invariance of modal wff under bisimulation
- proof of "only if" part: beyond the scope of the course

Variants of Modal Logic

- Generalization of Basic Modal Logic
- First-order Correspondence of Modal Logic
- Multi-agent Epistemic Logic
- Dynamic Logic

Epistemic Logic—Historical Notes

- knowledge in philosophy: epistemology (starting with the Greeks)
- formal logical analysis: [von Wright, 1951]
- Hintikka[1962]: knowledge and belief
- Fagin, Halpern, Vardi, Moses[1995]: Reasoning about knowledge

Epistemic Logic—Some Applications

- computer science: AI, distributed systems, multi-agent systems, security protocols, etc.
- linguistics: discourse reasoning
- economics: game theory

Common Knowledge

- the facts that everyone knows, everyone knows that everyone knows, everyone knows that everyone knows that everyone knows, and so on.
- examples:
  - three wise men
  - coordinated attack
  - email game [Rubinstein,1989]
  - mediated email game [Dimitri, 2003]

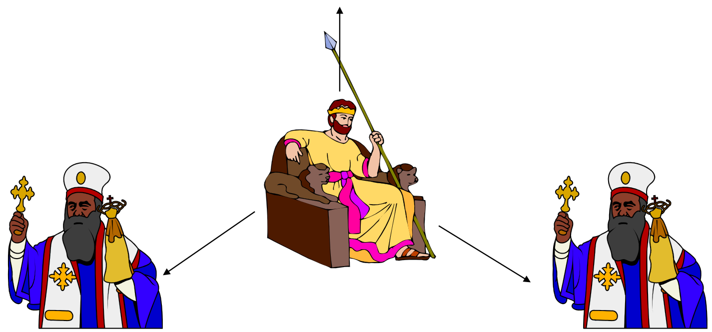
Three Wise Men

Once upon a time, a king
wished to test his three wise men.
He arranged them in a circle so
that they can see and hear each other.

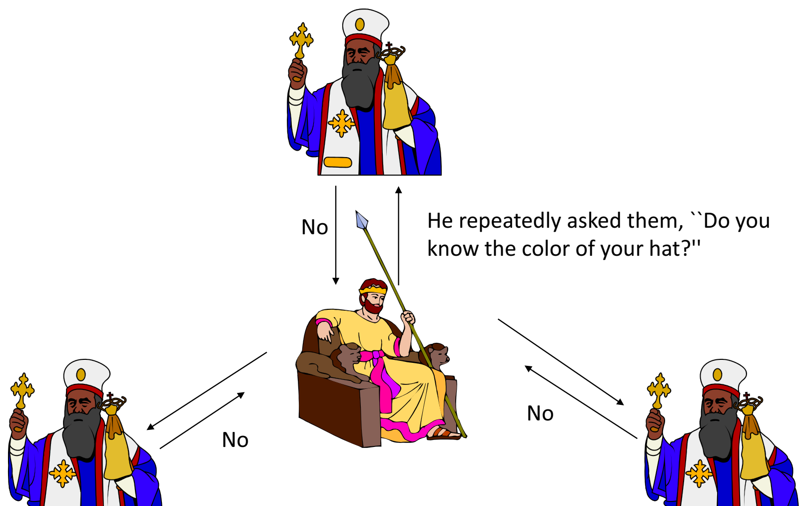
Three Wise Men

The king announced that he will put a
white or black hat on each of their
heads but that at least one hat will be
white.

In fact all three hats are white.

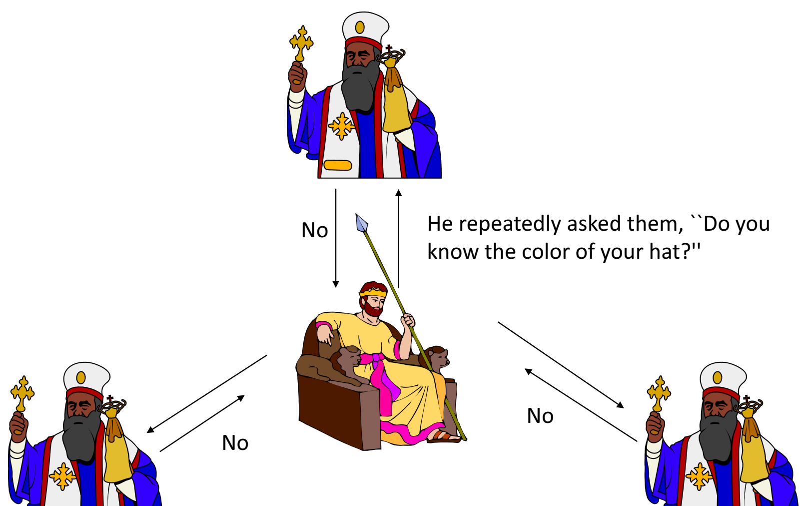


Three Wise Men



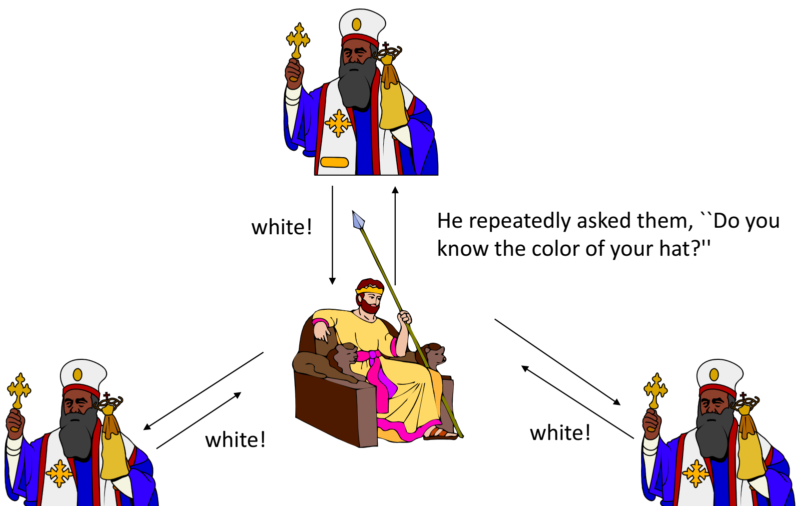
The first time, the response is ``no”

Three Wise Men



The second time, the response is still ``no”

Three Wise Men

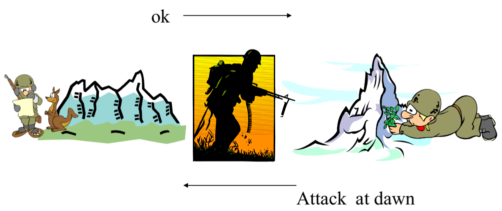


The third time, the response is finally ``white!”

Three Wise Men

- how can it happen that the king helps the wise men along by telling them something they already know?
- how can the wise men learn definite positive facts from hearing statements of ignorance?
- common knowledge

Coordinated Attack



each time the messenger makes it, the level of knowledge rises. first $K_B m$, then $K_A K_B m$, $K_B K_A K_B m, \ldots$

Coordinated Attack

- m will never become common knowledge using a k-round handshake protocol.
- m will never become common knowledge in any run of any protocol. In fact, common knowledge is not attainable in any system where communication is not guaranteed.

Distributed Knowledge

- distributed knowledge is that can be deduced by pooling together the knowledge of everyone
- application: belief fusion of multiple agents, collective intelligence

Logical Omniscience Problem

- modeling of ideal agents with unbounded reasoning capability
- if $K_i\varphi$ then $K_i\psi$ for any logical consequence ψ of φ
- example: if an agent knows the basic axioms of probability theory, then he knows all of its theorems
- in practice, agents do not have such a magic power

Epistemic Logic—Syntax

- alphabet
  - a set of atomic propositional variables $\Phi_0 = \{p_1, p_2, \cdots\}$
  - a set of agents $\mathbb{N}_n = \{1, 2, \cdots, n\}$
  - primitive logical symbols: $\bot$, $\neg$, $\wedge$, K_i $(i \in \mathbb{N}_n)$, C_G, D_G, E_G $(G \subseteq \mathbb{N}_n)$
  - defined logical symbols: $\top$, $\vee$, $\supset$, $\equiv$
  - auxiliary symbols: (,)
- formation rules of wffs

$$\varphi ::= p \mid \neg\varphi \mid \varphi \wedge \psi \mid K_i\varphi \mid E_G\varphi \mid C_G\varphi \mid D_G\varphi$$

where $i \in \mathbb{N}_n$ and $G \subseteq \mathbb{N}_n$

Epistemic Logic—Intuition

- $K_i\varphi$: agent i knows (or believes) φ
- $E_G\varphi$: every agent in G knows φ
- $D_G\varphi$: φ is distributed knowledge for the agent group G
- $C_G\varphi$: φ is common knowledge for the agent group G

Epistemic Logic—Semantics

$$\mathfrak{M} = (W, (R_i)_{1 \le i \le n}, \pi)$$

- W: a set of possible worlds (points)
- R_i: a binary relation over W for each i (the epistemic alternative relation)
- $\pi : \Phi_0 \to 2^W$
- $\mathcal{D}_G = \cap_{i \in G} R_i$
- $\mathcal{E}_G = \cup_{i \in G} R_i$
- $\mathcal{C}_G = \cup_{k \ge 0} \mathcal{E}_G^k = (\cup_{i \in G} R_i)^*$

Epistemic Logic—Semantics

- $\mathfrak{M}, w \models p$ iff $w \in \pi(p)$
- $\mathfrak{M}, w \models \neg\varphi$ iff $\mathfrak{M}, w \not\models \varphi$
- $\mathfrak{M}, w \models \varphi \wedge \psi$ iff $\mathfrak{M}, w \models \varphi$ and $(\mathfrak{M}, w \models \psi$
- $\mathfrak{M}, w \models K_i\varphi$ iff $\mathfrak{M}, u \models \varphi$ for all $(w, u) \in R_i$
- $\mathfrak{M}, w \models E_G\varphi$ iff $\mathfrak{M}, u \models \varphi$ for all $(w, u) \in \mathcal{E}_G$
- $\mathfrak{M}, w \models C_G\varphi$ iff $\mathfrak{M}, u \models \varphi$ for all $(w, u) \in \mathcal{C}_G$
- $\mathfrak{M}, w \models D_G\varphi$ iff $\mathfrak{M}, u \models \varphi$ for all $(w, u) \in \mathcal{D}_G$

Epistemic Logic—Semantics

- agent i in the world w may know something about the world, but does not know what the world is exactly
- $(w, u) \in R_i$ means that the agent considers that the actual world may be u while he is actually in the world w
- $R_i(w) = \{u \mid (w, u) \in R_i\}$ is the set of all worlds that agent i consider possible while he is actually in w
- i's knowledge about w constrains the worlds he considers possible
- if he is totally ignorant of the world w, $R_i(w) = W$
- if he knows φ is true, those worlds satisfying $\neg\varphi$ will be excluded from $R_i(w)$

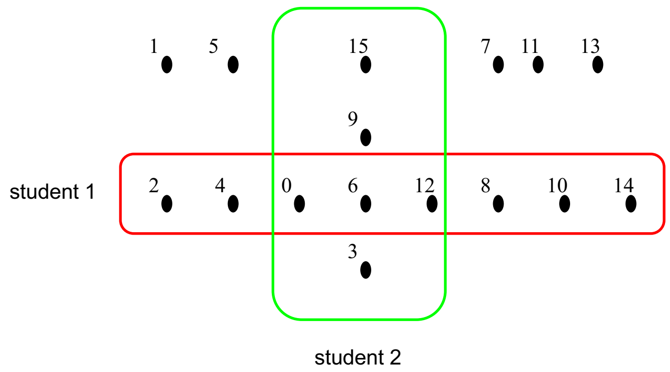
Epistemic Logic—Semantics

- distributed knowledge: when a group of agents can pool their knowledge together, their constraints on $R_i(w)$ are also pooled together
- a world is considered possible by the group, only when all agents in the group consider it possible, so $\mathcal{D}_G = \cap_{i\in G} R_i$

Epistemic Logic—Semantics

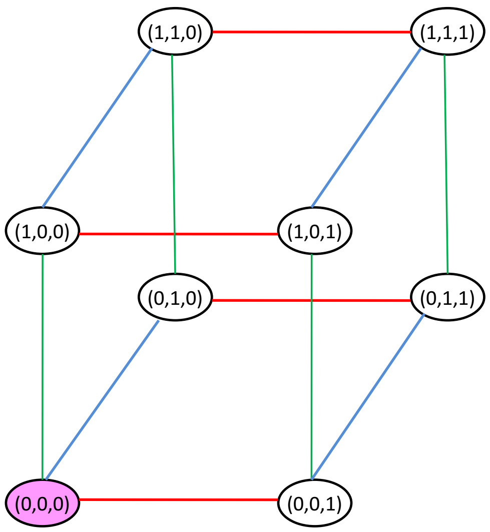
- everybody knows: the knowledge that everybody knows will constrain $R_i(w)$ of each i
- if everybody knows φ, only worlds satisfying φ will remain in $R_i(w)$ for each agent i
- if everybody knows φ, only worlds satisfying φ will remain in $\cup_{i\in G} R_i(w)$, so $\mathcal{E}_G = \cup_{i\in G} R_i$
- common knowledge: "everybody knows" depends on $\mathcal{E}_G$, "everybody knows everybody knows" depends on $\mathcal{E}_G^2$, and so no, so $\mathcal{C}_G = \cup_{k\geq 0} \mathcal{E}_G^k$

Distributed Knowledge: Example



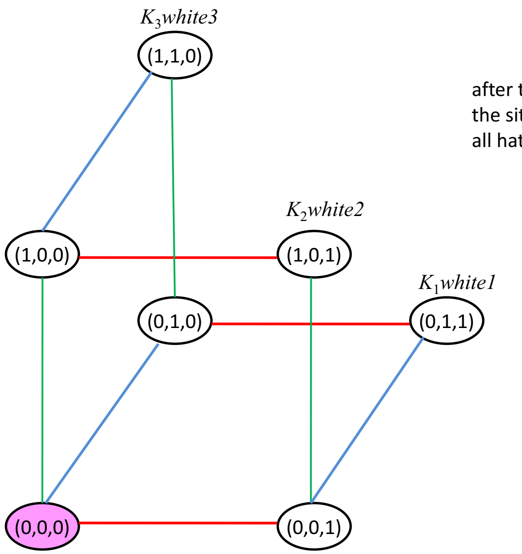
The teacher announce to two students that he writes down a natural number $0 \leq n \leq 15$ in a paper.
He told student 1 that the number is even privately.
He told student 2 that the number is divisible by 3 privately.
The distributed knowledge of both students: the number is 0 or 6 or 12

The Kripke Model of Three Wise Men



- Initial condition
  - actual situation: (0,0,0)
  - all possible situations
- Agent 1:
- Agent 2:
- Agent 3:
- 0: white, 1: black

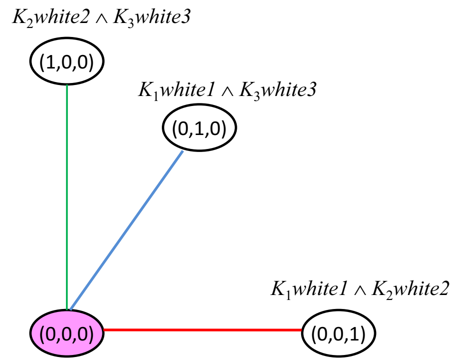
The Kripke Model of Three Wise Men



after the king's announcement ,
the situation that
all hats are black is deleted

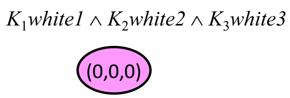
The Kripke Model of Three Wise Men

since no response to the first call:
delete all possible worlds where
some agent knows the color of his hat



The Kripke Model of Three Wise Men

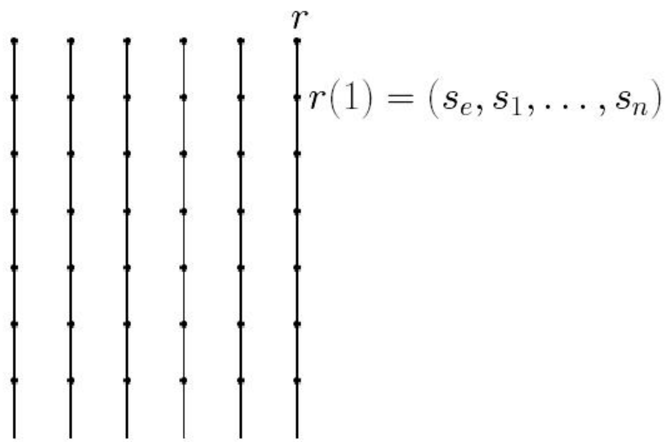
since no response to the second call:
delete all possible worlds where
some agent knows the color of his hat,
in the only remaining world, every agent knows
that the color of his hat is white



Knowledge in Multi-agent System

- global state: $(s_e, s_1, \cdots, s_n)$
- local state: s_i is the local state of agent i and s_e is the state of the environment
- run (execution): a function from time (natural numbers) to global states
- a system $\mathcal{R}$: a set of runs
- point: a pair (r, m) consisting of a run r and a time m ($r(m)$ is a global state)
- if $r(m) = (s_e, s_1, \cdots, s_n)$, then take $r_i(m)$ to be s_i

A System



A Instance of Kripke Model—Interpreted System Semantics

- interpreted system: $\mathcal{I} = (\mathcal{R}, \pi)$
  - $\mathcal{R}$: a system (a set of runs)
  - π: $\pi(p)$ is a set of global states
- for each $1 \leq i \leq n$, $\mathcal{K}_i$ is an equivalence relation on points:

$$(r, m)\mathcal{K}_i(r', m') \text{ iff } r_i(m) = r'_i(m')$$

- $\mathcal{D}_G = \cap_{i \in G} \mathcal{K}_i$
- $\mathcal{E}_G = \cup_{i \in G} \mathcal{K}_i$
- $\mathcal{C}_G = (\cup_{i \in G} \mathcal{K}_i)^*$

An Instance of Kripke Models—Interpreted System Semantics

- $(\mathcal{I}, r, m) \models p$ iff $r(m) \in \pi(p)$
- $(\mathcal{I}, r, m) \models \neg\varphi$ iff $(\mathcal{I}, r, m) \not\models \varphi$
- $(\mathcal{I}, r, m) \models \varphi \wedge \psi$ iff $(\mathcal{I}, r, m) \models \varphi$ and $(\mathcal{I}, r, m) \models \psi$
- $(\mathcal{I}, r, m) \models K_i\varphi$ iff $(\mathcal{I}, r', m') \models \varphi$ for all $(r', m') \in \mathcal{K}_i(r, m)$
- $(\mathcal{I}, r, m) \models E_G\varphi$ iff $(\mathcal{I}, r', m') \models \varphi$ for all $(r', m') \in \mathcal{E}_G(r, m)$
- $(\mathcal{I}, r, m) \models C_G\varphi$ iff $(\mathcal{I}, r', m') \models \varphi$ for all $(r', m') \in \mathcal{C}_G(r, m)$
- $(\mathcal{I}, r, m) \models D_G\varphi$ iff $(\mathcal{I}, r', m') \models \varphi$ for all $(r', m') \in \mathcal{D}_G(r, m)$

An Instance of Kripke Models—Interpreted System Semantics

- a point (r, m) corresponds to a possible world in a Kripke model
- $\mathcal{K}_i$ corresponds to R_i
- each $\mathcal{K}_i$ is determined by the local state of agent i
- agent i can know only his local state, so he considers (r, m) possible while he is in (r', m') (i.e. $(r, m) \in \mathcal{K}_i(r', m')$), if his local state is the same in both (r, m) and (r', m')
- each $\mathcal{K}_i$ is an equivalence relation

Model Classes in Epistemic Logic

- $\mathtt{C}_n$: all models
- $\mathtt{C}_n^r$ all reflexive models
- $\mathtt{C}_n^{rt}$ all reflexive and transitive models
- $\mathtt{C}_n^{rst}$ all equivalence models
- $\mathtt{C}_n^{rlt}$ all Euclidean, serial, and transitive models

Axiom Schemata

- PL: all tautologies of the propositional calculus
- **K**: $(K_i\varphi \wedge K_i(\varphi \supset \psi)) \supset K_i\psi$
- **T**: $K_i\varphi \supset \varphi$
- **4**: $K_i\varphi \supset K_iK_i\varphi$
- **5**: $\neg K_i\varphi \supset K_i\neg K_i\varphi$
- **D**: $\neg K_i\bot$
- **C1**: $E_G\varphi \equiv \bigwedge_{i\in G} K_i\varphi$
- **C2**: $C_G\varphi \supset E_G(\varphi \wedge C_G\varphi)$
- **D1**: $D_{\{i\}}\varphi \equiv K_i\varphi$
- **D2**: $D_G\varphi \supset D_{G'}\varphi$ if $G \subseteq G'$

Rules of Inference

- R1 (Modus ponens, MP):

$$\frac{\varphi \quad \varphi \supset \psi}{\psi}$$

- R2 (Knowledge Generalization, Gen):

$$\frac{\varphi}{K_i\varphi}$$

- RC1 (Induction):

$$\frac{\varphi \supset E_G(\psi \wedge \varphi)}{\varphi \supset C_G\psi}$$

Hilbert Style Axiomatic Systems

- $\mathbf{K}_n$: PL, $\mathbf{K}$, MP, Gen
- $\mathbf{T}_n$: $\mathbf{K}_n$+$\mathbf{T}$
- $\mathbf{S4}_n$: $\mathbf{K}_n$+$\mathbf{T}$+$\mathbf{4}$
- $\mathbf{S5}_n$: K_n+$\mathbf{T}$+$\mathbf{4}$+$\mathbf{5}$
- $\mathbf{KD45}_n$: K_n+$\mathbf{4}$+$\mathbf{5}$+$\mathbf{D}$
- $\mathbf{S}^C$: $\mathbf{S}$+$\mathbf{C1}$+$\mathbf{C2}$+RC1
- $\mathbf{S}^D$: $\mathbf{S}$+$\mathbf{D1}$+$\mathbf{D2}$
- $\mathbf{S}^{CD}$: $\mathbf{S}^C$+$\mathbf{S}^D$

Completeness

- the correspondence:

axiom	constraint
PL, $\mathbf{K}$	none
$\mathbf{T}$	reflexive
$\mathbf{4}$	transitive
$\mathbf{5}$	Euclidean
$\mathbf{D}$	serial

- example: $\vdash_{\mathbf{S5}_n^{CD}} \varphi$ iff φ is valid in C_n^{rst}.

Complexity

- knowledge and common knowledge:

Logic	Completeness
$\mathbf{S5}_1$, $\mathbf{KD45}_1$	NP
$\mathbf{K}_n$, $\mathbf{T}_n$, $\mathbf{S4}_n$, $n \geq 1$; $\mathbf{S5}_n$, $\mathbf{KD45}_n$, $n \geq 2$	$PSPACE$
$\mathbf{K}_n^C$, $\mathbf{T}_n^C$, $n \geq 1$; $\mathbf{S4}_n^C$, $\mathbf{S5}_n^C$, $\mathbf{KD45}_n^C$, $n \geq 2$	$EXPTIME$

- adding distributed knowledge to the language does not affect complexity

Variants of Modal Logic

- Generalization of Basic Modal Logic
- First-order Correspondence of Modal Logic
- Multi-agent Epistemic Logic
- Dynamic Logic

Dynamic Logic: Reasoning about Programs

- program: a recipe written in a formal language for computing desired output data from given input data
- programs typically use variables to hold input and output values and intermediate results
- state: a function that assigns a value to each program variable
- a program can be viewed as a transformation on states
- proposition: a description of a state

Dynamic Logic: Programming Constructs

- programs are built inductively from atomic programs and tests using various program operators
- regular program operators:
  - sequential composition: $\alpha;\beta$
  - non-deterministic choice: $\alpha \cup \beta$
  - iteration: α^*

Dynamic Logic: Program Verification

- I/O specification: φ, ψ
- partial correctness: whenever a program started in a state satisfying the input condition φ, then if it halts, it does so in a state satisfying the output condition ψ
- total correctness: partially correct and halts whenever it started in a state satisfying φ
- dynamic logic vs temporal logic:
  - dynamic logic is exogenous: programs are explicit in the logical language
  - temporal logic is endogenous: program is fixed and is considered part of the structure over which the logic is interpreted

Precursor of Dynamic Logic: Hoare Logic

- $\{\varphi\}\alpha\{\psi\}$: α is partially correct with respect to the I/O specification φ, ψ (FOL formulas)
- rules
  - assignment rule: if e is free for x in φ

$$\{\varphi[x/e]\}x := e\{\varphi\}$$

  - composition rule::

$$\frac{\{\varphi\}\alpha\{\psi\}, \quad \{\psi\}\beta\{\chi\}}{\{\varphi\}\alpha;\beta\{\chi\}}$$

Precursor of Dynamic Logic: Hoare Logic

- rules
  - conditional rule:

$$\frac{\{\varphi \wedge \psi\}\alpha\{\chi\}, \quad \{\varphi \wedge \neg\psi\}\beta\{\chi\}}{\{\varphi\}\textbf{if } \psi \textbf{ then } \alpha \textbf{ else } \beta\{\chi\}}$$

  - while rule:

$$\frac{\{\varphi \wedge \psi\}\alpha\{\psi\}}{\{\psi\}\textbf{while } \varphi \textbf{ do } \alpha\{\neg\varphi \wedge \psi\}}$$

  - weakening rule:

$$\frac{\varphi' \supset \varphi \quad \{\varphi\}\alpha\{\psi\} \quad \psi \supset \psi'}{\{\varphi'\}\alpha\{\psi'\}}$$

Propositional Dynamic Logic: Syntax

- alphabet
  - a set of atomic propositional variables $\Phi_0 = \{p_1, p_2, \cdots\}$
  - a set of atomic programs $\Pi_0 = \{a_1, a_2, \cdots\}$
  - propositional operators: $\perp$, $\neg$, $\wedge$
  - program operators: ; (sequential composition), $\cup$ (non-deterministic choice), $*$ (iteration)
  - mixed operators: $[\,]$ (necessity modality formation operator), ?(test)
  - defined symbols: $\top$, $\vee$, $\supset$, $\equiv$, $\langle\rangle$ (possibility modality formation operator)
  - auxiliary symbols: (,)

Propositional Dynamic Logic: Syntax

- wffs Φ and programs Π: the smallest sets such that
  - $\Phi_0 \subseteq \Phi$ and $\Pi_0 \subseteq \Pi$
  - if $\varphi, \psi \in \Phi$, then $\perp, \neg\varphi, \varphi \wedge \psi \in \Phi$
  - if $\alpha, \beta \in \Pi$, then $\alpha; \beta, \alpha \cup \beta, \alpha^* \in \Pi$
  - if $\alpha \in \Pi$ and $\varphi \in \Phi$, then $[\alpha]\varphi \in \Phi$
  - if $\varphi \in \Phi$, then $\varphi? \in \Pi$
- abbreviation: $\langle\alpha\rangle\varphi = \neg[\alpha]\neg\varphi$
- precedence of operators: unary operators bind tighter than binary ones, and ; binds tighter that $\cup$

Propositional Dynamic Logic: Syntax

- $[\alpha]\varphi$: it is necessary that after executing α, φ is true
- $\alpha; \beta$: execute α, then execute β
- $\alpha \cup \beta$: choose either α or β non-deterministically and execute it
- α^*: execute α non-deterministically chosen finite number of times (zero or more)
- $\varphi?$: proceed if φ is true, fail if false

Propositional Dynamic Logic: Shorthand

- **skip**: $\top?$
- **fail**: $\bot?$
- **if** $\varphi_1 \to \alpha_1 \mid \cdots \mid \varphi_n \to \alpha_n$ **fi**: $\varphi_1?;\alpha_1 \cup \cdots \cup \varphi_n?;\alpha_n$
- **do** $\varphi_1 \to \alpha_1 \mid \cdots \mid \varphi_n \to \alpha_n$ **od**: $(\varphi_1?;\alpha_1 \cup \cdots \cup \varphi_n?;\alpha_n)^*;(\neg\varphi_1 \wedge \cdots \wedge \neg\varphi_n)?$
- **if** φ **then** α **else** β: **if** $\varphi \to \alpha \mid \neg\varphi \to \beta$ **fi**
- **while** φ **do** α: **do** $\varphi \to \alpha$ **od**
- **repeat** α **until** φ: α; **while** $\neg\varphi$ **do** α
- $\{\varphi\}\alpha\{\psi\}$: $\varphi \supset [\alpha]\psi$

Propositional Dynamic Logic—Semantics

- (Kripke) model: $\mathfrak{M} = (W, (R_a)_{a\in\Pi_0}, \pi)$
  - W: a set of possible worlds (points, states, etc.)
  - $R_a \subseteq W \times W$: a binary relation over W
  - $\pi : \Phi_0 \to 2^W$: a truth assignment
- intuition
  - a model is a state transition system
  - R_a: the set of I/O pairs of states of the atomic program a

Propositional Dynamic Logic—Semantics

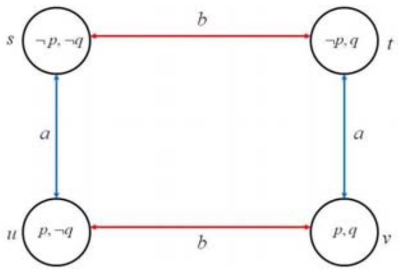
given a model $\mathfrak{M} = (W, (R_a)_{a\in\Pi_0}, \pi)$ and $w \in W$

- state transition of compound programs:
  - $R_{\alpha;\beta} = R_\alpha \circ R_\beta = \{(w,u) \mid \exists v \in W, (w,v) \in R_\alpha, (v,u) \in R_\beta\}$
  - $R_{\alpha\cup\beta} = R_\alpha \cup R_\beta$
  - $R_{\alpha^*} = \bigcup_{n\geq 0} R_\alpha^n$
  - $R_{\varphi?} = \{(w,w) \mid \mathfrak{M}, w \Vdash \varphi\}$
- satisfaction:
  - $\mathfrak{M}, w \Vdash [\alpha]\varphi \Leftrightarrow$ for every $u \in W$, if $(w,u) \in R_\alpha$, then $\mathfrak{M}, u \Vdash \varphi$

Propositional Dynamic Logic—Semantics

- satisfiability and validity are defined as in basic modal logic
- the set of all finite computation sequences of α: $CS(\alpha)$
  - $CS(a) = \{a\}$ if $a \in \Pi_0$
  - $CS(\varphi?) = \{\varphi?\}$
  - $CS(\alpha;\beta) = \{\gamma\delta \mid \gamma \in CS(\alpha), \delta \in CS(\beta)\}$
  - $CS(\alpha \cup \beta) = CS(\alpha) \cup CS(\beta)$
  - $CS(\alpha^*) = \bigcup_{n\geq 0} CS(\alpha^n)$, where $\alpha^0 =$ **skip** and $\alpha^{k+1} = \alpha;\alpha^k$
- property: $R_\alpha = \bigcup_{\sigma\in CS(\alpha)} R_\sigma$

PDL Semantics: Example



- $\mathfrak{M} \Vdash p \equiv [(ab^*a)^*]p$ (we write $\alpha; \beta$ as $\alpha\beta$)
- $\mathfrak{M} \Vdash q \equiv [(ba^*b)^*]q$
- $\alpha = (aa \cup bb \cup (ab \cup ba)(aa \cup bb)^*(ab \cup ba))^*$
- $\mathfrak{M} \Vdash \varphi \equiv [\alpha]\varphi$ for any φ

PDL—Axiom Schemata

1. PL: all tautologies of the propositional calculus
2. $[\alpha](\varphi \supset \psi) \supset ([\alpha]\varphi \supset [\alpha]\psi)$
3. $[\alpha \cup \beta]\varphi \equiv ([\alpha]\varphi \wedge [\beta]\varphi)$
4. $[\alpha; \beta]\varphi \equiv [\alpha][\beta]\varphi$
5. $[\varphi?]\psi \equiv (\varphi \supset \psi)$
6. $(\varphi \wedge [\alpha][\alpha^*]\varphi) \equiv [\alpha^*]\varphi$
7. induction axiom: $\varphi \wedge [\alpha^*](\varphi \supset [\alpha]\varphi) \supset [\alpha^*]\varphi$

PDL—Rules of Inference

- R1 (Modus ponens, MP):

$$\frac{\varphi \quad \varphi \supset \psi}{\psi}$$

- R2 (Generalization, Gen):

$$\frac{\varphi}{[\alpha]\varphi}$$

PDL—Alternative Formulations of the Induction Axiom

- RTC (reflexive transitive closure rule):

$$\frac{\varphi \supset (\psi \wedge [\alpha]\varphi)}{\varphi \supset [\alpha^*]\psi}$$

- LI (loop invariance rule):

$$\frac{\varphi \supset [\alpha]\varphi}{\varphi \supset [\alpha^*]\varphi}$$

- IND$\Box$ (the induction axiom): $\varphi \wedge [\alpha^*](\varphi \supset [\alpha]\varphi) \supset [\alpha^*]\varphi$
- IND$\Diamond$ (in dual form): $\langle\alpha^*\rangle\varphi \supset (\varphi \vee \langle\alpha^*\rangle(\neg\varphi \wedge \langle\alpha\rangle\varphi))$

PDL—Meta-Theorems

- soundness and completeness: let φ be a PDL wff, then we have $\Vdash \varphi$ iff $\vdash \varphi$
- the satisfiability problem for PDL is EXPTIME-complete
- RTC, LI, IND$\Box$, and IND$\Diamond$ are inter-derivable in PDL without the induction axiom
- the rules of Hoare logic are derivable in PDL
- compactness fails for PDL

Inter-derivation of Induction Axioms

- (IND$\Box$) $\Rightarrow$(LI):
  1. premise of LI: $\varphi \supset [\alpha]\varphi$
  2. $[\alpha^*](\varphi \supset [\alpha]\varphi)$ (Gen,1)
  3. $\varphi \supset (\varphi \wedge [\alpha^*](\varphi \supset [\alpha]\varphi))$ (2. PL)
  4. $\varphi \supset [\alpha^*]\varphi$ (IND$\Box$, PL, 3)
- (LI)$\Rightarrow$(RTC):
  1. premise of RTC: $\varphi \supset (\psi \wedge [\alpha]\varphi)$
  2. $\varphi \supset \psi$ (PL, 1)
  3. $\varphi \supset [\alpha]\varphi$ (PL, 1)
  4. $\varphi \supset [\alpha^*]\varphi$ (LI, 3)
  5. $[\alpha^*](\varphi \supset \psi)$ (Gen, 2)
  6. $\varphi \supset [\alpha^*]\psi$ (Ax2, PL, 4, 5)

Inter-derivation of Induction Axioms

- (RTC)$\Rightarrow$(IND$\Box$):
  1. $\varphi \wedge [\alpha^*](\varphi \supset [\alpha]\varphi)$
     $\supset \varphi \wedge (\varphi \supset [\alpha]\varphi) \wedge [\alpha][\alpha^*](\varphi \supset [\alpha]\varphi)$ (Ax6)
  2. $\varphi \wedge [\alpha^*](\varphi \supset [\alpha]\varphi)$
     $\supset \varphi \wedge [\alpha]\varphi \wedge [\alpha][\alpha^*](\varphi \supset [\alpha]\varphi)$ (1, PL)
  3. $\underline{\varphi \wedge [\alpha^*](\varphi \supset [\alpha]\varphi)}$
     $\supset \varphi \wedge [\alpha]\underline{(\varphi \wedge [\alpha^*](\varphi \supset [\alpha]\varphi))}$ (2, modal reasoning)
  4. $\varphi \wedge [\alpha^*](\varphi \supset [\alpha]\varphi) \supset [\alpha^*]\varphi$ (3, RTC)
- (IND$\Diamond$) $\Leftrightarrow$(IND$\Box$): PL and the duality of $[\alpha]$ and $\langle\alpha\rangle$

PDL Encoding of Hoare Logic

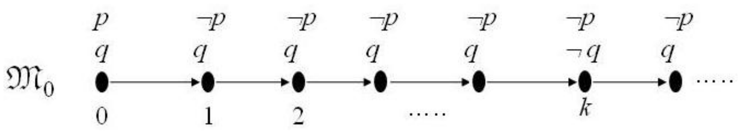
- we derive the while rule:

$$\frac{\{\varphi \wedge \psi\}\alpha\{\psi\}}{\{\psi\}\mathbf{while}\ \varphi\ \mathbf{do}\ \alpha\{\neg\varphi \wedge \psi\}}$$

  1. premise: $(\varphi \wedge \psi) \supset [\alpha]\psi$
  2. $\psi \supset (\varphi \supset [\alpha]\psi)$ (PL,1)
  3. $\psi \supset [\varphi?;\alpha]\psi$ (Ax4, Ax5, 2)
  4. $\psi \supset [(\varphi?;\alpha)^*]\psi$ (LI rule, 3)
  5. $\psi \supset [(\varphi?;\alpha)^*](\neg\varphi \supset (\neg\varphi \wedge \psi))$ (PL, Ax2, MP, 4)
  6. $\psi \supset [(\varphi?;\alpha)^*;\neg\varphi?](\neg\varphi \wedge \psi))$ (Ax4, Ax5, 5)

Failure of Compactness

- let $\Sigma = \{p \supset q, p \supset [a]q, p \supset [a^2]q, \cdots\}$
- $\varphi = p \supset [a^*]q$
- $\Sigma \Vdash \varphi$ in PDL: for every model $\mathfrak{M}$ and w, $\mathfrak{M}, w \Vdash \Sigma$ implies $\mathfrak{M}, w \Vdash \varphi$
- if $\Sigma' \subset \Sigma$ and $p \supset [a^k]q \notin \Sigma'$ for some k, then $\mathfrak{M}_0, 0 \Vdash \Sigma'$ but $\mathfrak{M}_0, 0 \nVdash \varphi$



PDL—Remarks

- our finite state automata logic is a special case of PDL without program operators (only atomic programs are allowed)
- note the analogy between C_G in multi-agent epistemic logic and $[\alpha^*]$ in PDL
- translation from multi-agent epistemic logic $\mathbf{K}_n^C$ to PDL: $me2d$

1. $me2d(p) = p$
2. $me2d(\bot) = \bot$
3. $me2d(\neg\varphi) = \neg me2d(\varphi)$
4. $me2d(\varphi \wedge \psi) = me2d(\varphi) \wedge me2d(\psi)$
5. $me2d(K_i\varphi) = [i]me2d(\varphi)$
6. $me2d(C_G\varphi) = [\bigcup G][(\bigcup G)^*]me2d(\varphi)$

Conclusion

You can now explore the modal space by yourself

Conclusion

- The entry point to the modal space
- Summary of the course
- A rough guide to the future study

The Entry Point

- you have arrived at the entry point of the modal space
- you are ready to answer the following questions posed by the "immigration officer"
  1. what is the purpose of your visit?—why would you like to study modal logic?
  2. where will you stay?—which part of modal logic you are interested in?
  3. how long will you stay?—will your interests in modal logic persist?
- after all, you should be able to form a coherent map of the territory
- but, before that, I will provide a rough guide to you

Conclusion

- The entry point to the modal space
- Summary of the course
- A rough guide to the future study

Summary

we have touched on the following topics

- the evolution of modal logic
- basic modal logic:
  - syntax of the diamond language
  - Kripke frames and models
  - basic notions of model theory: validity, satisfiability, semantic consequence, disjoint union, generated submodel, bounded morphism, and bisimulation
- normal systems of basic modal logic:
  - Hilbert-style axiomatization
  - proof-theoretic notions: theoremhood, consistency, syntactic consequence, Lindenbaum Lemma

Summary

we have touched on the following topics

- meta-theorems of normal systems:
  - soundness
  - strong completeness (by canonical model construction)
  - decidability by the filtration method
- variants of modal logic:
  - general modal logic: more modalities and higher arity
  - standard translation to FOL
  - reasoning about knowledge: multi-agent epistemic logic
  - reasoning about regular programs: propositional dynamic logic

Conclusion

- The entry point to the modal space
- Summary of the course
- A rough guide to the future study

Where to Stay—Interested Areas

- computer science
  - software engineering
  - artificial intelligence
  - world wide web
- philosophy
  - formal epistemology
  - philosophy of information
- mathematics
- economics and social science
- linguistics
- system science

What to See—Interesting Topics: Temporal Logics

- software engineering: software/hardware specification and verification
- basic temporal logic extended with operators S (since) and U (until)
- model checking
- linear time vs. branching time
- point-based vs interval-based
- combination with other modal logic: temporal-epistemic and spatio-temporal logics

What to See—Interesting Topics: Spatial Logics

- mathematics: geometry and topology
- point-based logics: logic of elsewhere and everywhere, collinearity and qualitative distance
- line-based logics: logics of parallelism, orthogonality, intersections of lines
- incidence logic: incidence relation between a point and a line, projective geometry, affine geometry
- topological logic: $\Box$ as interior and $\Diamond$ as closure

What to See—Interesting Topics: Deontic Logics

- AI: normative agent systems
- computer security: specification of security policies
- standard deontic logic (SDL): accessibility relation points to "ideal" or "perfect deontic alternatives" of the world under consideration
- $w \Vdash O\varphi$: φ is true in all such ideal worlds
- SDL suffers from a number of paradoxes
- Ross'sparadox: $O\varphi \supset O(\varphi \vee \psi)$: if one ought to mail the letter then one ought to mail it or burn it
- dynamic deontic logic: $O\alpha = [\overline{\alpha}]V$: an action is obligatory if failing to do it leads to a state of violation
- defeasible deontic logic: deontic rules with exceptions

What to See—Interesting Topics: Intelligent Agents

- AI: modeling of mental attitudes of intelligent agents
- types of mental attitudes
  - informational: knowledge, belief, and awareness
  - motivational: commitment, choice, intentions, plans (internal commitment), goals (a degree of internal commitment), desire, want, wish, preference
  - social: obligation and permission
  - emotional: joy, hope, sorrow, happiness, fear, distress, pride, relief, love, hate, anger, shame, gratitude etc.
- BDI logic: belief, desire, intention

What to See—Interesting Topics: Description Logics

- AI: knowledge representation
- WWW: web 3.0 (semantic web), ontology representation and resource description language
- the alphabet: concept names (atomic concepts A, B) and role names (atomic roles R)
- concept terms:

$$C ::= A \mid \bot \mid \neg C \mid C \sqcap D \mid \forall R : C \mid \exists R : C$$

- $\exists R : C$ and $\forall R : C$ correspond to $\langle R \rangle C$ and $[R]C$ in multi-modal logic respectively
- more expressive extensions

What to See—Interesting Topics: Boolean Modal Logics

- instances: temporal logic, dynamic logic, and multi-agent epistemic logic
- modal similarity type (Δ, ρ), where Δ is not only a set but also an algebraic structure
- in temporal logic: past and future operators are mutually converse
- in dynamic logic: program operators form a regular algebra
- in epistemic logic C_G corresponds to a transitive closure of E_G
- AI: analysis of information systems, rough set theory in data mining

What to See—Interesting Topics: Dynamic Epistemic Logic

- applications to philosophy of information
- AI and formal epistemology: belief revision
- epistemic action: to change mental states of cognitive agents
- public announce logic: $[\varphi]\psi$: after the announcement of φ, ψ holds
- dynamic doxastic logic: modal logic of belief revision by Segerberg

What to See—Interesting Topics: Many-Dimensional Modal Logics

- each possible world has some inner structure instead of an abstract entity: a tuple or a sequence over some base set
- the accessibility relations are (partly) determined by this inner structure of the states
- system science: complex combined systems out of relatively simple ones
- instances: interval temporal logic (an interval as a pair of time points), arrow logic in square frame (an arrow as a pair of points), combination of epistemic and temporal logics
- combinations of modal logics:
  - fusion (independent join or dovetailing): combined components do not interact at all
  - product: interaction is strong

What to See—Interesting Topics: Much More

- mathematics: logic of provability, logic of justification (Artemov)
- economics and social science: game logic, coalition logic, interactive epistemology (Aumann)
- system science: regular equivalence in social network analysis, modeling of complex networks, different graded modalities for uncertainty reasoning
- linguistics: feature logic, Montague semantics, hybrid logic
- philosophical logic: first-order and higher-order modal logic

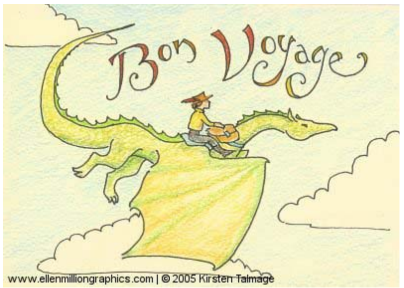
Getting Around—Approaches

- syntactic approach: natural deduction, Gentzen systems, tableau methods (in particular for description logics), resolution, translation to FOL
- semantic approach: frame correspondence theory, fragments of FOL or HOL, model theory
- computational approach: computability and complexity, modal logic programming
- algebraic approach: algebraic semantics for modal logic, algebra and coalgebra
- topological approach: topological interpretation of modal logic

Side Trips—Related Logics

- conditional logic:
  - original motivation of modal logic by Lewis
  - possible world semantics
  - $\varphi \to \psi$: if minimal change to φ-world, then ψ
  - related to belief revision and dynamic doxastic logic
- nonmonotonic logic: $\Sigma \vdash \varphi$ does not imply $\Sigma \cup \{\psi\} \vdash \varphi$
- relevant logic and substructural logic
- intuitionistic logic: Kripke semantics for intuitionistic logic
- quantum logic: Kripke semantics with Hilbert space models

Ok! My guide will stop here!



Epilogue

- The set of slides was originally designed for a mini-course (9 hours) of the FLOLAC'2009 held in National Taiwan University
- I have revised it slightly based on the response (or silence) of the students. As in the example of three wise men, a teacher must learn from hearing statements of ignorance, as well as from silence.

Acknowledgements

- Most materials are from standard textbooks:
  - Introduction, basic modal logic: (Blackburn et al., 2001)
  - Normal systems and meta-theorems: (Chellas, 1980)
  - Generalization of modal logic: (Blackburn et al., 2001)
  - multi-agent epistemic logic: (Fagin et.al., 1995)
  - dynamic logic: (Harel et. al., 2000)
- A few slides are from Areces and Blackburn's ESSLLI'08 course "Logic for Computation"
- A few slides are from Pacuit's Stanford university course "An Invitation to Modal Logic"
- Most pictures are downloaded from the WWW.