모달 로직의 소개

LiComR Summer Workshop 2003

신승철@동양대

월드컵 4강, 그 다음 해 여름

얘기할 순서

- 모달 로직이란?
- 간단한 모달 언어와 그 시멘틱스
- 일반 모달 언어와 그 시멘틱스
- 공리계와 그 확장
- 그리고 아무도 ...

모달 로직에 대한 말 말 말?

양상 논리(樣相 論理) - 양상, 양식, modality 를 다루는 논리 체계

Propositional logic + modal operators

C.I. Lewis

A Description Language for Relational structures

진리값이 변한다?

'....이 필연적이다', '...이 가능하다'와 같은 표현에 대한 연역 활동을 공부하는 분야

믿음(belief), 시간(tense), deontic(윤리) 등에 관한 논리로서
철학적인 논의의 형식적인 분석 뿐 아니라 컴퓨터 과학 등에 적용된다.

"다양한 모달 로직"

Alethic	$\Box$: it is necessary that ... $\Diamond$: it is possible that ...
Deontic	O : it is obligatory that ... P : it is permitted that ... F : it is forbidden that ...
Temporal	G : it will be always true in the future that ... F : it will be true at some point in the future that ... H : it was always true in the past that ... P : it was true at some point in the past that ...
Doxastic	B_x : x believes that ...
Epistemic	K_x : x knows that ...
Provability	P : it is provable that ...

Basic modal logic

Alphabet :

- A set of propositional letters p, q, ...
- Propositional connectives $\neg$ and $\wedge$ and constant true $\top$ ($\vee$, $\rightarrow$, $\leftrightarrow$, $\bot$ are definable)
- modality $\Box$ ($\Diamond$ is definable)

Well-formed formula ϕ, ψ :

$$p \mid \top \mid \neg\phi \mid \phi \wedge \psi \mid \Box\phi$$

Definable forms:

$$\begin{aligned}
\phi \vee \psi &= \neg(\neg\phi \wedge \neg\psi) \\
\phi \rightarrow \psi &= \neg(\phi \wedge \neg\psi) \\
\phi \leftrightarrow \psi &= (\phi \rightarrow \psi) \wedge (\psi \rightarrow \phi) \\
\bot &= \neg\top \\
\Diamond\phi &= \neg\Box\neg\phi
\end{aligned}$$

"Relational structures"

A *frame* for the basic modal language $\mathfrak{F} = (W, R)$
where W is a non-empty set of possible worlds
and R is a binary relation on W.

A *model* for the basic modal language $\mathfrak{M} = (\mathfrak{F}, V)$
where $\mathfrak{F}$ is a frame
and V is a valuation function $\Phi \to \mathcal{P}(W)$.

"Satisfaction"

$$
\begin{array}{rll}
\mathfrak{M}, w \models p & \text{if} & w \in V(p), \text{ where } p \in \Phi \\
\mathfrak{M}, w \models \top & \text{if} & \text{always} \\
\mathfrak{M}, w \models \neg\phi & \text{if} & \mathfrak{M}, w \not\models \phi \\
\mathfrak{M}, w \models \phi \wedge \psi & \text{if} & \mathfrak{M}, w \models \phi \text{ and } \mathfrak{M}, w \models \psi \\
\mathfrak{M}, w \models \Box\phi & \text{if} & \text{for every } v \in W \text{ such that } Rwv, \text{ we have } \mathfrak{M}, v \models \phi
\end{array}
$$

For a set Σ of formulas
$\mathfrak{M}, w \models \Sigma$ if all members of Σ are true at w

For the valuation of arbitrary formulas
$V(\phi) = \{w \mid \mathfrak{M}, w \models \phi\}$

"Global truth and satisfiability"

A formula ϕ is *globally* or *universally true* in a model $\mathfrak{M}$

$$\mathfrak{M} \models \phi \quad \text{if} \quad \mathfrak{M}, w \models \phi \quad \text{for all } w \in W$$

A formula ϕ is *satisfiable* in a model $\mathfrak{M}$

$$\exists w.\ \mathfrak{M}, w \models \phi$$

A set Σ of formulas is globally true in a model $\mathfrak{M}$

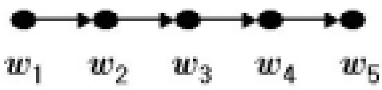
$$\mathfrak{M} \models \Sigma \quad \text{if} \quad \mathfrak{M}, w \models \Sigma \quad \text{for all } w \in W$$

A set Σ of formulas is satisfiable in a model $\mathfrak{M}$

$$\exists w.\ \mathfrak{M}, w \models \Sigma$$

"예제 1"

$\mathfrak{F} = (\{w_1, w_2, w_3, w_4, w_5\}, R)$ where Rw_iw_j iff $j = i + 1$:

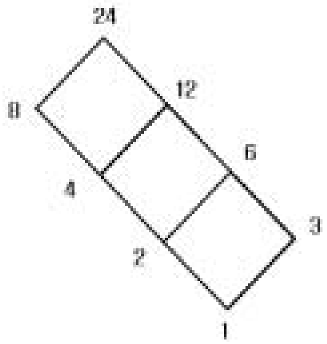


$V(p) = \{w_2, w_3\}$
$V(q) = \{w_1, w_2, w_3, w_4, w_5\}$
$V(r) = \varnothing$

$\mathfrak{M}, w_1 \models \Diamond\Box p$
$\mathfrak{M}, w_1 \not\models \Diamond\Box p \to p$
$\mathfrak{M}, w_2 \models \Diamond(p \wedge \neg r)$
$\mathfrak{M}, w_1 \models q \wedge \Diamond(q \wedge \Diamond(q \wedge \Diamond(q \wedge \Diamond q)))$

"예제 2"

$\mathfrak{F} = (\{1,2,3,4,6,8,12,24\}, R)$ where Rxy iff $x \neq y$ and x divides y:



$V(p) = \{4,8,12,24\}$, $V(q) = \{6\}$

$\mathfrak{M}, 6 \models \Box p$
$\mathfrak{M}, 2 \not\models \Box p$
$\mathfrak{M}, 2 \models \Diamond(q \wedge \Box p) \wedge \Diamond(\neg q \wedge \Box p)$

"R-accessible Possible worlds"

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

$$\mathfrak{M} = (\mathfrak{F}, V)$$

When $R = W \times W$, $(W,R,V), w \models \Box\phi$ if $\forall v \in W.(W,R,V), v \models \phi$

$\vdots$

$\vdots$

When $R = \varnothing$, $(W,R,V), w \models \Box\phi$ if always

"Modal similarity type"

$\tau = (O, \rho)$

where O is a non-empty set of *modal operators* $\triangle, \triangle_0, \triangle_1, \ldots$

and ρ is an arity function $O \to \mathbb{N}$.

For multi-modality

$\Box_a$ or $[a]$

$\Diamond_a$ or $\langle a \rangle$

where a is taken from some index set.

"Modal language"

$ML(\tau, \Phi)$

where $\tau = (O, \rho)$ is a modal similarity type

and Φ is a set of propositional letters.

The set $Form(\tau, \Phi)$ of modal formulas over τ and Φ is given by the rule

$$\phi := p \ \mid \ \bot \ \mid \ \neg\phi \ \mid \ \phi_1 \wedge \phi_2 \ \mid \ \triangle(\phi_1, \ldots, \phi_{\rho(\triangle)}),$$

where p ranges over elements of Φ.

For each $\triangle \in O$, the dual ∇ of $\triangle$ is defined as
$\nabla(\phi_1, \ldots, \phi_n) = \neg\triangle(\neg\phi_1, \ldots, \neg\phi_n)$

"τ-frame and τ-model"

τ-frame $\mathfrak{F} = (W, R_\triangle)_{\triangle \in \tau}$ or $\mathfrak{F} = (W, \{R_\triangle \mid \triangle \in \tau\})$

(i) a non-empty set W of possible worlds

(ii) for each $n \geq 0$, and each n-ary modal operator $\triangle$ in the similarity type τ, an $(n+1)$-ary relation $R_\triangle$

τ-model $\mathfrak{M} = (\mathfrak{F}, V)$

(i) a τ-frame $\mathfrak{F}$

(ii) a valuation function $V : \Phi \to \mathcal{P}(W)$

"Satisfaction again"

$$
\begin{array}{rll}
\mathfrak{M}, w \models p & \text{if} & w \in V(p), \text{ where } p \in \Phi \\
\mathfrak{M}, w \models \top & \text{if} & \text{always} \\
\mathfrak{M}, w \models \neg\phi & \text{if} & \mathfrak{M}, w \not\models \phi \\
\mathfrak{M}, w \models \phi \wedge \psi & \text{if} & \mathfrak{M}, w \models \phi \text{ and } \mathfrak{M}, w \models \psi \\
\mathfrak{M}, w \models \triangle(\phi_1, ..., \phi_n) & \text{if} & \text{for every } v_1, ..., v_n \in W \text{ such that } R_\triangle w v_1 ... v_n, \\
 & & \text{we have, for each } i,\ \mathfrak{M}, v_i \models \phi_i
\end{array}
$$

Note: when $\rho(\triangle) = 0$

$$\mathfrak{M}, w \models \triangle \quad \text{if} \quad w \in R_\triangle$$

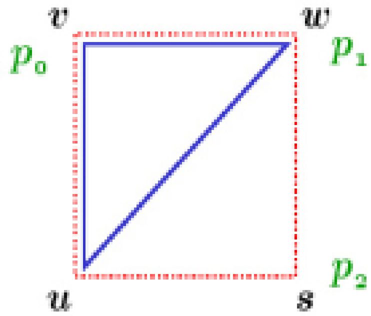
"예제 3"

similarity type $\tau = (\{\triangle, \odot\}, \{\triangle \mapsto 2, \odot \mapsto 3\})$

τ-frame $\mathfrak{F} = (\{u, v, w, s\}, R_\triangle, S_\odot)$

$R_\triangle = \{(u, v, w)\} \qquad S_\odot = \{(u, v, w, s)\}$

$V(p_0) = \{v\} \quad V(p_1) = \{w\} \quad V(p_2) = \{s\}$



$$\mathfrak{M}, u \models \triangle(p_0, p_1) \to \odot(p_0, p_1, p_2)$$

$$\mathfrak{M} \models \triangle(p_0, p_1) \to \odot(p_0, p_1, p_2)$$

"Validity"

$\mathfrak{F}, w \models \phi$ iff for every $\mathfrak{M}$ such that $\mathfrak{M} = (\mathfrak{F}, V)$ $\mathfrak{M}, w \models \phi$

$\mathfrak{F} \models \phi$ iff for every $w \in W$ $\mathfrak{F}, w \models \phi$

$\mathsf{F} \models \phi$ iff for every $\mathfrak{F}$ in a class of frames F $\mathfrak{F} \models \phi$

$\models \phi$ iff for every $\mathfrak{F}$ $\mathfrak{F} \models \phi$

Note: validity vs. truth

$\phi \vee \psi$ is true at w = either ϕ or ψ is true at w

$\phi \vee \psi$ is valid on $\mathfrak{F} \neq$ either ϕ or ψ is valid on $\mathfrak{F}$

"예제 4: $\Diamond(p \vee q) \rightarrow (\Diamond p \vee \Diamond q)$ is valid on all frames?"

임의의 $\mathfrak{F}, w, V$ 를 취하고 $(\mathfrak{F}, V), w \models \Diamond(p \vee q)$ 임을 가정하자. 그러면 정의에 의해서 Rwv 이고 $(\mathfrak{F}, V), v \models p \vee q$ 인 v 가 존재한다. 그런데 $(\mathfrak{F}, V), v \models p \vee q$ 이면 $(\mathfrak{F}, V), v \models p$ 이거나 $(\mathfrak{F}, V), v \models q$ 이다. 따라서 $(\mathfrak{F}, V), w \models \Diamond p$ 이거나 $(\mathfrak{F}, V), w \models \Diamond q$ 이고 어느 쪽이든 $(\mathfrak{F}, V), w \models \Diamond p \vee \Diamond q$ 이다.

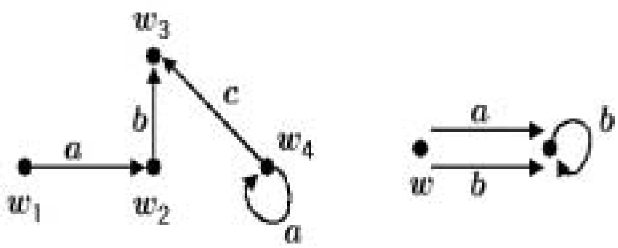
"예제 5: $\Box p \rightarrow \Box\Box p$ is not valid on all frames?"

$\mathfrak{F} = (\{0, 1, 2\}, \{(0, 1), (1, 2)\})$ 와 $V(p) = 1$ 을 취하면 counter-example을 만들수 있다. 즉, $(\mathfrak{F}, V), 0 \models \Box p$ 이지만 $(\mathfrak{F}, V), 0 \models \Box\Box p$ 는 아니다.

"예제 6: $\Box p \rightarrow \Box\Box p$ is valid on transitive frames?"

임의의 transitive $\mathfrak{F}, w, V$ 를 취하고 $(\mathfrak{F}, V), w \models \Box p$ 임을 가정하자. 그러면 정의에 의해서 Rwu 인 모든 u 에 대하여 $(\mathfrak{F}, V), u \models p$ 이다. 그런데 R 이 transitive 이므로 Rwu 이고 Ruv 인 모든 v 에 대하여 Rwv 이고 $(\mathfrak{F}, V), v \models p$ 이다. 따라서 $(\mathfrak{F}, V), w \models \Box\Box p$ 임을 알수 있다.

"예제 7: $\langle a \rangle p \rightarrow \langle b \rangle p$?"



$\langle a \rangle p \rightarrow \langle b \rangle p$ defines $R_a \subseteq R_b$

"General frames"

Frames	vs.	Models
Validity	vs.	Satisfaction

A *general frame* $(\mathfrak{F}, A)$ is a frame $\mathfrak{F}$ together with a restricted, but suitably well-behaved collection A of *admissible valuations*.

"Operations corresponding to modalities"

Given a frame $=(W, R)$ and $X \subseteq W$,

$$m_R(X) = \{w \in W \mid Rwx \text{ for all } x \in X\}$$

note: $V(\Box\phi) = m_R(V(\phi))$

Given an $(n+1)$-ary relation R on a set W,

$$m_R(X_1, ..., X_n) = \{w \in W \mid Rww_1...w_n \text{ for all } w_1 \in X_1, ..., w_n \in X_n\}$$

"General frames" (formally)

general τ-frame $(\mathfrak{F}, A)$ where $\mathfrak{F} = (W, R_\triangle)_{\triangle\in\tau}$
and A is a non-empty collection of *admissible* subsets of W closed under the following operations:

(i) intersection: if $X, Y \in A$, then $X \cap Y \in A$

(ii) relative complement: if $X \in A$, then $W \setminus X \in A$

(iii) modal operations: if $X_1, ..., X_n \in A$, then $m_{R_\triangle}(X_1, ..., X_n) \in A$ for all $\triangle \in \tau$

A *model based on a general frame* is a triple $(\mathfrak{F}, A, V)$ where $(\mathfrak{F}, A)$ is a general frame and V is a valuation satisfying the constraint that for each proposition letter p, $V(p)$ is an element of A. Valuations satisfying this constraint are called *admissible* for $(\mathfrak{F}, A)$.

"Local semantic consequense"

ϕ is a *local semantic consequence* of Σ over S : $\Sigma \models_{\mathsf{S}} \phi$

for all models $\mathfrak{M}$ from S, and all points w in $\mathfrak{M}$,
if $\mathfrak{M}, w \models \Sigma$ then $\mathfrak{M}, w \models \phi$

"Global semantic consequense"

ϕ is a *global semantic consequence* of Σ over S : $\Sigma \models^g_{\mathsf{S}} \phi$

for all structures $\mathfrak{S}$ in S,
if $\mathfrak{S} \models \Sigma$ then $\mathfrak{S} \models \phi$

"System **K**"

The axioms of **K**:

- propositional tautologies
- (K) $\Box(p \to q) \to (\Box p \to \Box q)$

The rules of proof of **K**:

- Modus ponens: given ϕ and $\phi \to \psi$, prove ψ
  - preserves validity, global truth and satisfaction
- Uniform substitution: given ϕ, prove θ, where θ is obtained from ϕ by uniformly replacing proposition letters in ϕ by arbitrary formulas.
  - preserves only validity
- Necessitation: given ϕ, prove $\Box\phi$
  - preserves validity and global truth

"**K** the minimal axiom system"

A **K**-*proof* is a finite sequence of formula, each of which is an axiom, or follows from one or more earlier items in the sequence by applying a rule of proof.(Hilbert style)

A formula ϕ is **K**-*provable* ($\vdash_{\mathbf{K}} \phi$)
if it occurs as the last item of some **K**-proof.

K is *sound* with respect to the class of all frames
: All **K**-provable formulas are valid
- its axioms are all valid and all 3 rules of proof preserve validity.

K is *complete* with respect to the class of all frames
: All valid formulas are **K**-provable.

"예제 8: $(\Box p \wedge \Box q) \rightarrow \Box(p \wedge q)$ is valid ?"

1.	$\vdash p \rightarrow (q \rightarrow (p \wedge q))$	Tautology
2.	$\vdash \Box(p \rightarrow (q \rightarrow (p \wedge q)))$	Necessitation: 1
3.	$\vdash \Box(p \rightarrow q) \rightarrow (\Box p \rightarrow \Box q)$	K axiom
4.	$\vdash \Box(p \rightarrow (q \rightarrow (p \wedge q))) \rightarrow (\Box p \rightarrow \Box(q \rightarrow (p \wedge q)))$	Uniform substitution: 3
5.	$\vdash \Box p \rightarrow \Box(q \rightarrow (p \wedge q))$	Modus Ponens: 2,4
6.	$\vdash \Box(q \rightarrow (p \wedge q)) \rightarrow (\Box q \rightarrow \Box(p \wedge q))$	Uniform substitution: 3
7.	$\vdash \Box p \rightarrow (\Box q \rightarrow \Box(p \wedge q))$	Propositional logic: 5,6
8.	$\vdash (\Box p \wedge \Box q) \rightarrow \Box(p \wedge q)$	propositional logic: 7

"System **K4**"

The axioms of **K4**:

- propositional tautologies
- (K) $\Box(p \rightarrow q) \rightarrow (\Box p \rightarrow \Box q)$
- (4) $\Box p \rightarrow \Box\Box p$

The rules of proof of **K4**:

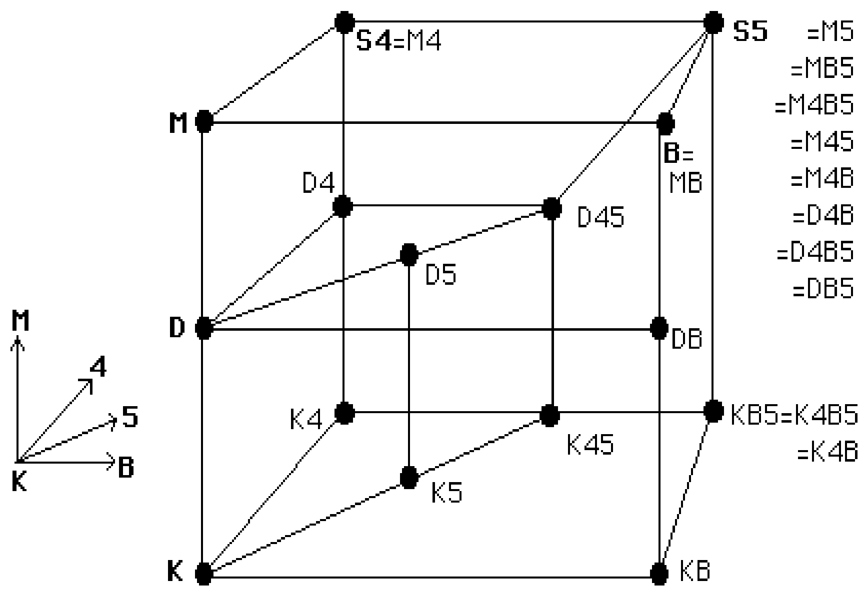
- Modus ponens
- Uniform substitution
- Necessitation

$$\Sigma \vdash_{\mathsf{K4}} \phi \quad \text{iff} \quad \Sigma \models_{\mathsf{Tran}} \phi$$

"Axioms and frame conditions"

Name	Axiom	Condition on Frames	R is ...
(D)	$\Box p \rightarrow \Diamond p$	$\exists u.wRu$	Serial
(M)	$\Box p \rightarrow p$	wRw	Reflexive
(4)	$\Box p \rightarrow \Box\Box p$	if $(wRv$ and $vRu)$ then wRu	Transitive
(B)	$p \rightarrow \Box\Diamond p$	if wRv then vRw	Symmetric
(5)	$\Diamond p \rightarrow \Box\Diamond p$	if $(wRv$ and $wRu)$ then vRu	Euclidean
(CD)	$\Diamond p \rightarrow \Box p$	if $(wRv$ and $wRu)$ then $v = u$	Deterministic
$(\Box M)$	$\Box(\Box p \rightarrow p)$	if wRv then vRv	Shift Reflexive
$(C4)$	$\Box\Box p \rightarrow \Box p$	if wRv then $\exists u.(wRu$ and $uRv)$	Dense
(C)	$\Diamond\Box p \rightarrow \Box\Diamond p$	if $(wRv$ and $wRx)$ then $\exists u.(vRu$ and $xRu)$	Convergent

"Relationships among modal logics"



"Result by Scott and Lemmon"

(G) $\Diamond^h\Box^i p \rightarrow \Box^j\Diamond^k p$

(4) $\Box p \rightarrow \Box\Box p = \Diamond^0\Box^1 p \rightarrow \Box^2\Diamond^0 p$

(hijk-Convergence) if $R^h wv$ and $R^j wu$ then $\exists x.(R^i vx$ and $R^k ux)$

(0120-Convergence) if $R^0 wv$ and $R^2 wu$ then $\exists x.(R^1 vx$ and $R^0 ux)$

(transitivity) if Rvx and Rxu then Rvu

Note: Sahlqvist(1975) has discovered important generalizations of the Scott-Lemmon result covering a much wider range of axiom types.

"모달 로직에 관심을 갖게 하는 것들"

- Temporal logics
- Dynamic logics
- Fixpoint logics
- Modal type system
- Model checking
- Semantics
- Bisimulation
- Analysis and Verification of modal properties
- ...

"모달 타입"

New typing ideas from (intuitionistic variants of) standard modal logics

Potential applications include type systems for...

- run-time code generation
- meta-programming and higher-order syntax with free-variables
- memoization and incremental computation
- information flow and security
- distributed computation
- resource-bounded computation
- ...

taken from B. Pierce's slides

"더 이상 슬라이드가 없습니다."