Formal Specification of Software

Modal Logic

Bernhard Beckert

UNIVERSITÄT KOBLENZ-LANDAU

Modal Logic

In classical logic, it is only important whether a formula is true

In modal logic, it is also important in which

- **way**
- **mode**
- **state**

a formula is true

A formula (a proposition) is

- **necessarily / possibly true**
- **true today / tomorrow**
- **believed / known**
- **true before / after an action / the execution of a program**

Propositional Modal Logic: Formulas

- **The propositional variables $p \in$ Var are modal formulas**

- **If A, B are modal formulas, then**

  $$\neg A \qquad (A \wedge B) \qquad (A \vee B) \qquad (A \rightarrow B) \qquad (A \leftrightarrow B)$$

  $\Box A$ **(read “box A”, “necessarily A”)**

  $\Diamond A$ **(read “diamond A”, “possibly A”)**

  are modal formulas

Informal Interpretations of $\Box$

$\Box F$ means

- F **is necessarily true**
- F **is always true (in future states/words)**
- **an agent** a **believes** F
- **an agent** a **knows** F
- F **is true after all possible executions of a program** p

Notation

If necessary write

$$\Box_a F \qquad \Box_p F \qquad [a]F \qquad [p]F$$

instead of $\Box F$

Informal Interpretations of $\Diamond$

$\Box F$	$\Diamond F$ (the same as $\neg\Box\neg F$)
F is necessarily true	F is possibly true
F is always true	F at least once true
agent a believes F	F is consistent with a's beliefs
agent a knows F	a does not know $\neg F$
F is true after all possible executions of program p	F is true after at least one possible execution of program p

Kripke Structures

Given: a propositional signature Var

Definition

A Kripke structure

$$\mathcal{K} = (S, R, I)$$

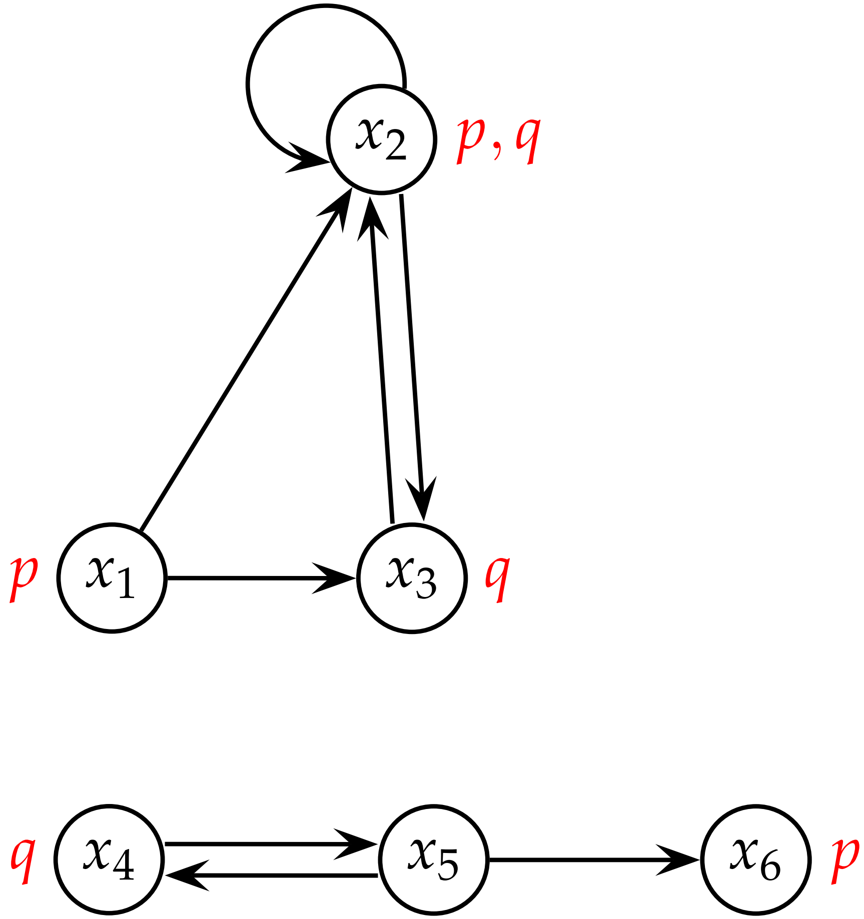
consists of

- **a non-empty set S (of worlds / states)**
- **an *accessibility relation* $R \subseteq S \times S$**
- **an *interpretation* I : Var $\times\, S \to \{$<u>true</u>, <u>false</u>$\}$**

Kripke Structures: Example

accessibility relation

set of states



Interpretation I

Modal Logic: Semantics

Given: Kripke structure $\mathcal{K} = (S, R, I)$

Valuation

$$val_{\mathcal{K}}(p)(s) \; = \; I(p)(s) \qquad \text{for } p \in \text{Var}$$

$val_{\mathcal{K}}$ **defined for propositional operators in the same way as val**$_I$

$$val_{\mathcal{K}}(\Box A)(s) = \begin{cases} \underline{\text{true}} & \text{if } val_{\mathcal{K}}(A)(s') = \underline{\text{true}} \text{ for} \\ & \text{all } s' \in S \text{ with } sRs' \\ \underline{\text{false}} & \text{otherwise} \end{cases}$$

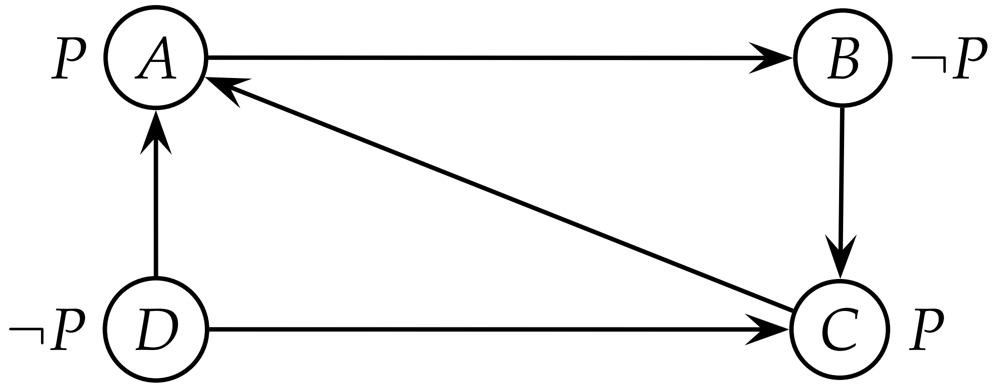
$$val_{\mathcal{K}}(\Diamond A)(s) = \begin{cases} \underline{\text{true}} & \text{if } val_{\mathcal{K}}(A)(s') = \underline{\text{true}} \text{ for} \\ & \text{at least one } s' \in S \text{ with } sRs' \\ \underline{\text{false}} & \text{otherwise} \end{cases}$$

Saul Aaron Kripke

Born 1940 in Omaha (US)

First publication:	*A Completeness Theorem in Modal Logic* The Journal of Symbolic Logic, 1959
Studied at:	Harvard, Princeton, Oxford and Rockefeller University
Positions:	Harvard, Rockefeller, Columbia, Cornell, Berkeley, UCLA, Oxford
since 1977	Professor at Princeton University
since 1998	Emeritus at Princeton University

Modal Logic: Example for Evaluation



$(\mathcal{K}, A) \models P$	$(\mathcal{K}, B) \models \neg P$	$(\mathcal{K}, C) \models P$	$(\mathcal{K}, D) \models \neg P$
$(\mathcal{K}, A) \models \Box\neg P$	$(\mathcal{K}, B) \models \Box P$	$(\mathcal{K}, C) \models \Box P$	$(\mathcal{K}, D) \models \Box P$
$(\mathcal{K}, A) \models \Box\Box P$	$(\mathcal{K}, B) \models \Box\Box P$	$(\mathcal{K}, C) \models \Box\Box\neg P$	—

Modal Logic: Valid Formulas

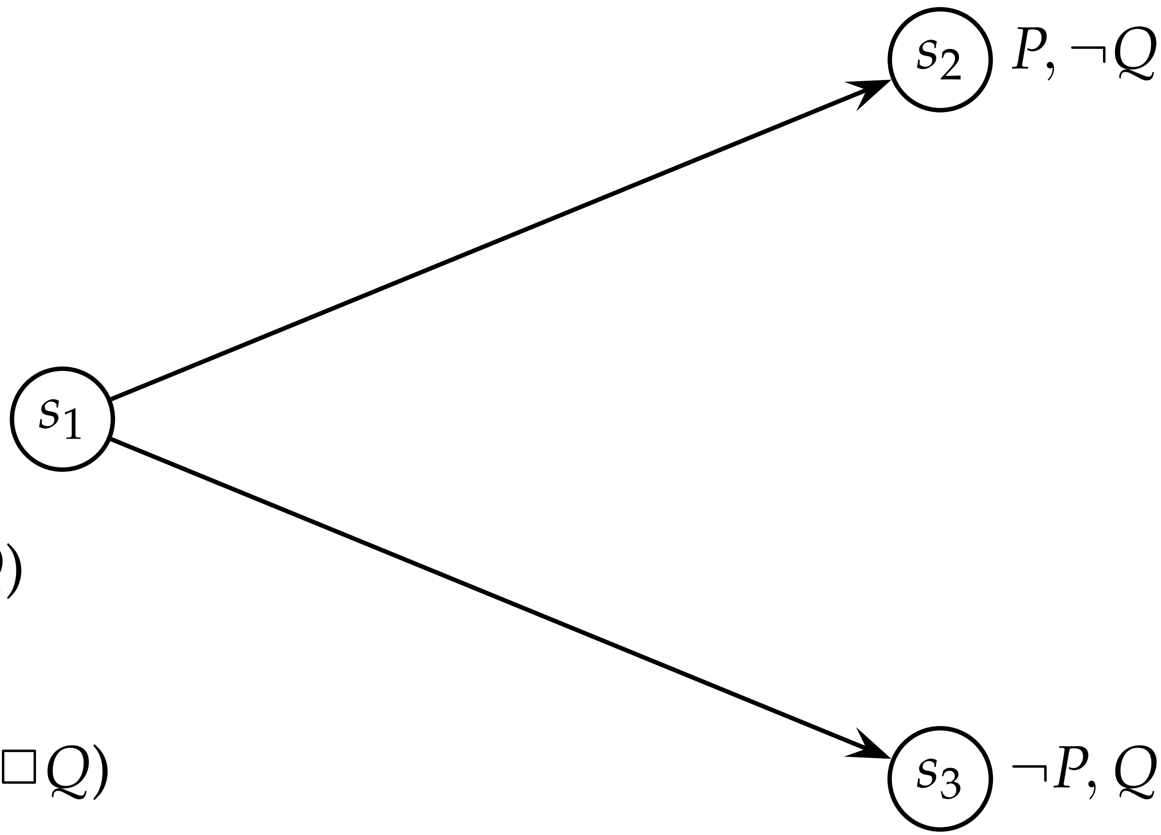
Valid

- $\Box(P \to Q) \to (\Box P \to \Box Q)$
- $(\Box P \land \Box(P \to Q)) \to \Box Q$
- $(\Box P \lor \Box Q) \to \Box(P \lor Q)$
- $(\Box P \land \Box Q) \leftrightarrow \Box(P \land Q)$
- $\Box P \leftrightarrow \neg\Diamond\neg P$
- $\Diamond(P \lor Q) \leftrightarrow (\Diamond P \lor \Diamond Q)$
- $\Diamond(P \land Q) \to (\Diamond P \land \Diamond Q)$

Not valid:

- $\Box(P \lor Q) \to (\Box P \lor \Box Q)$
- $(\Diamond P \land \Diamond Q) \to \Diamond(P \land Q)$

Not Valid: $\Box(P \vee Q) \rightarrow (\Box P \vee \Box Q)$



$\Box(P \vee Q)$
$\neg\Box P$
$\neg\Box Q$
$\neg(\Box P \vee \Box Q)$

$\Box(P \vee Q) \rightarrow (\Box P \vee \Box Q)$ **not true in state** s_1

Formulas Characterising Properties of R

Formula	Property of R
$\Box p \rightarrow p$	**reflexive**
$p \rightarrow \Diamond p$	**reflexive**
$\Box\Box p \rightarrow \Box p$	**reflexive**
$\Box\Diamond p \rightarrow \Diamond p$	**reflexive**
$\Box p \rightarrow \Diamond\Box p$	**reflexive**
$\Diamond\Diamond p \rightarrow \Diamond p$	**reflexive**

Formula	Property of R
$\Box p \rightarrow \Box\Box p$	**transitive**
$p \rightarrow \Box\Diamond p$	**symmetrical**
$\Box\Box p \leftrightarrow \Box p$	**reflexive, transitive**
$\Diamond\Diamond p \leftrightarrow \Diamond p$	**reflexive, transitive**
$\Diamond\Box p \leftrightarrow \Box p$	**equivalence relation**
$\Box\Diamond p \leftrightarrow \Diamond p$	**equivalence relation**

Modal Logic: Valid Formulas

$\Box F$	$\Box F \to F$	$\Box F \to \Box\Box F$	$\Box F \to \Diamond F$	$(\Box(F \to G) \land \Box F) \to \Box G$	$\Diamond true$
F **is necessarily true**	yes	yes	yes	yes	yes
agent a **knows** F	yes	yes	yes	yes	yes
agent a **believes** F	no	yes	yes	yes	yes
F **holds after executing program** p	no	no	no	yes	no