
Formal Verification 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

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 $p \in \text{Var}$ are modal formulas

• If A, B are modal formulas, then

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

$\Box A$ (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

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

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

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

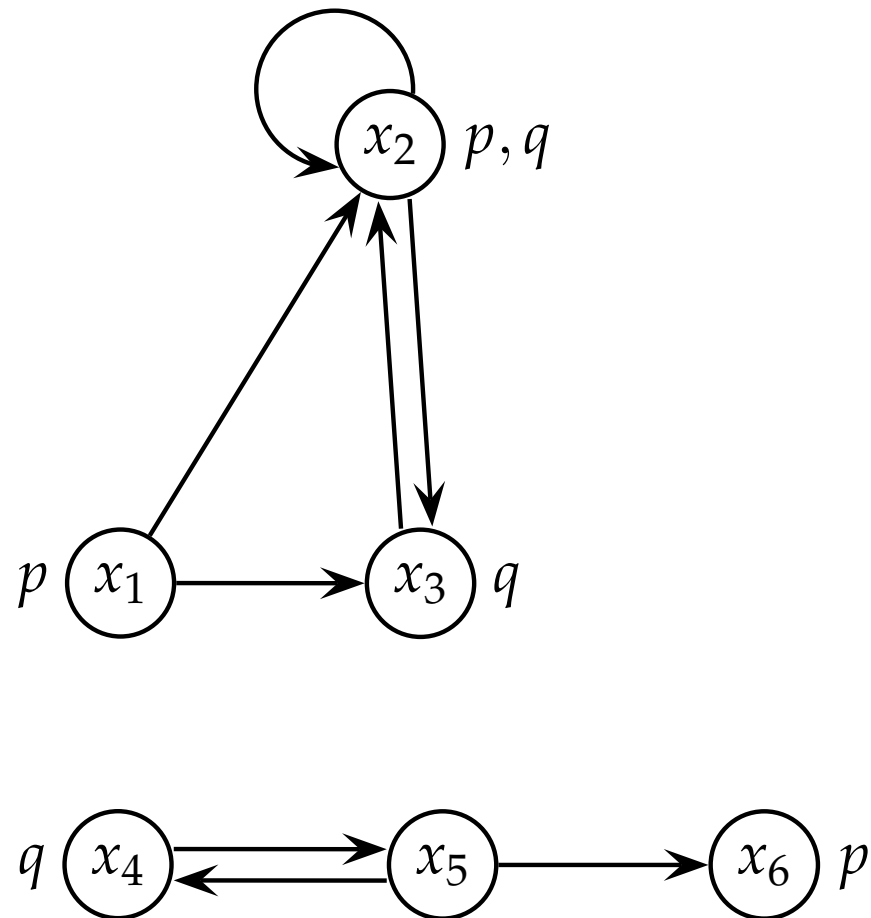
A Kripke structure

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

consists of

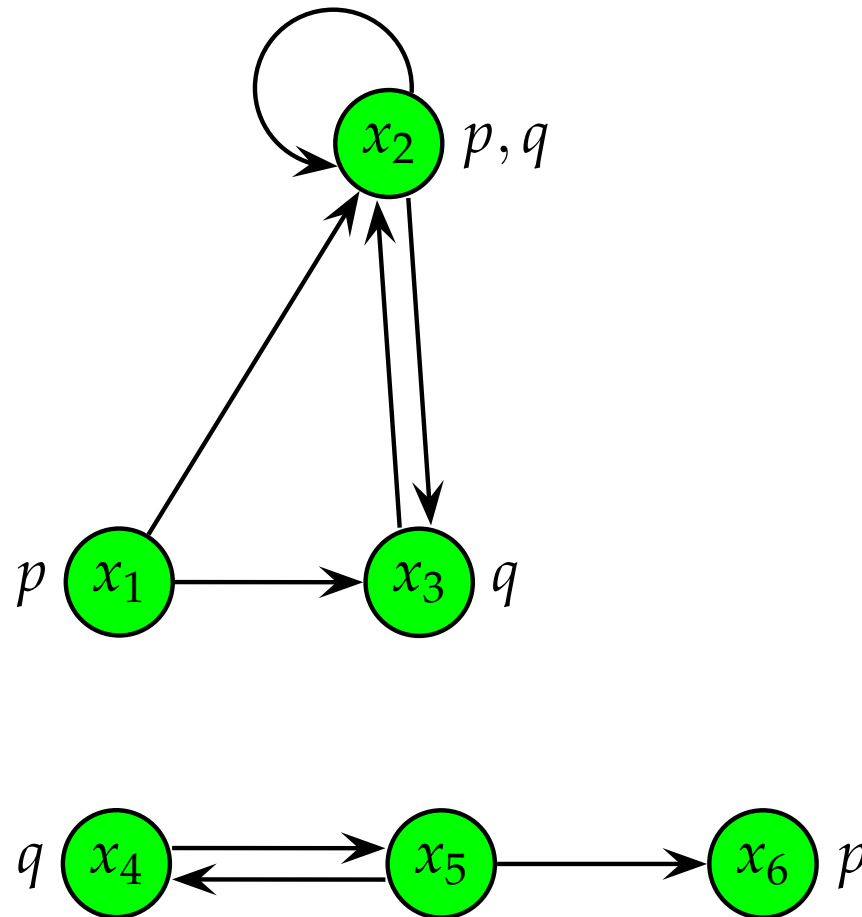
- a non-empty set S (of worlds / states)
- an *accessibility relation* $R \subseteq S \times S$
- an *interpretation* $I : \text{Var} \times S \rightarrow \{\underline{\text{true}}, \underline{\text{false}}\}$

Kripke Structures: Example



Kripke Structures: Example

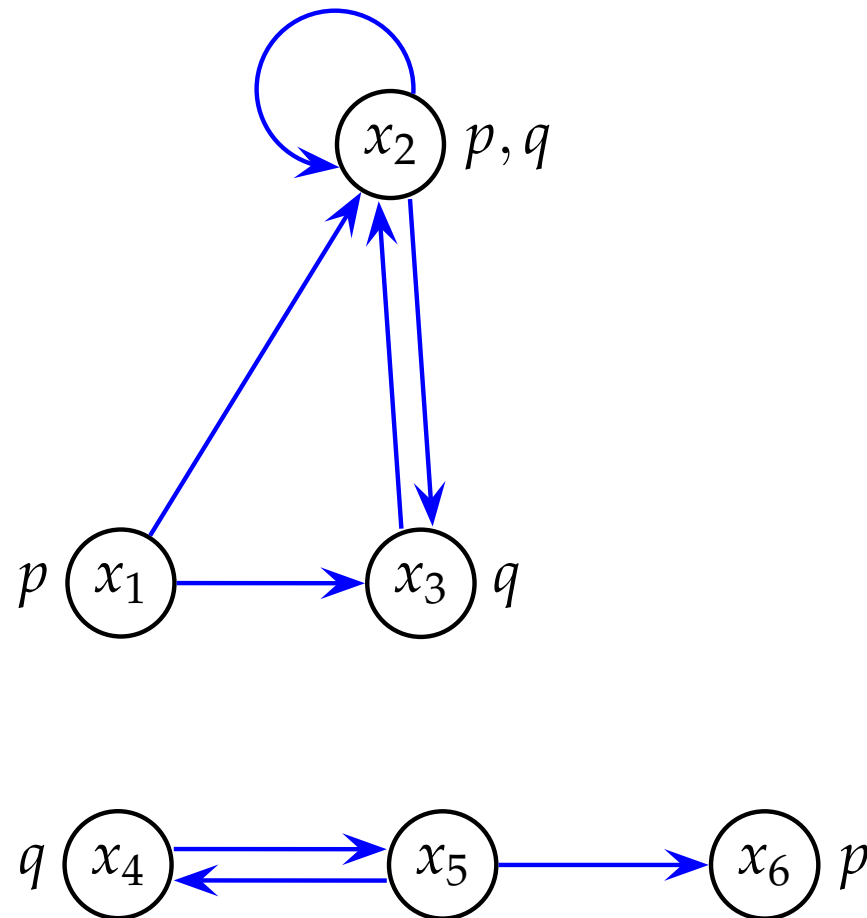
set of states



Kripke Structures: Example

accessibility
relation

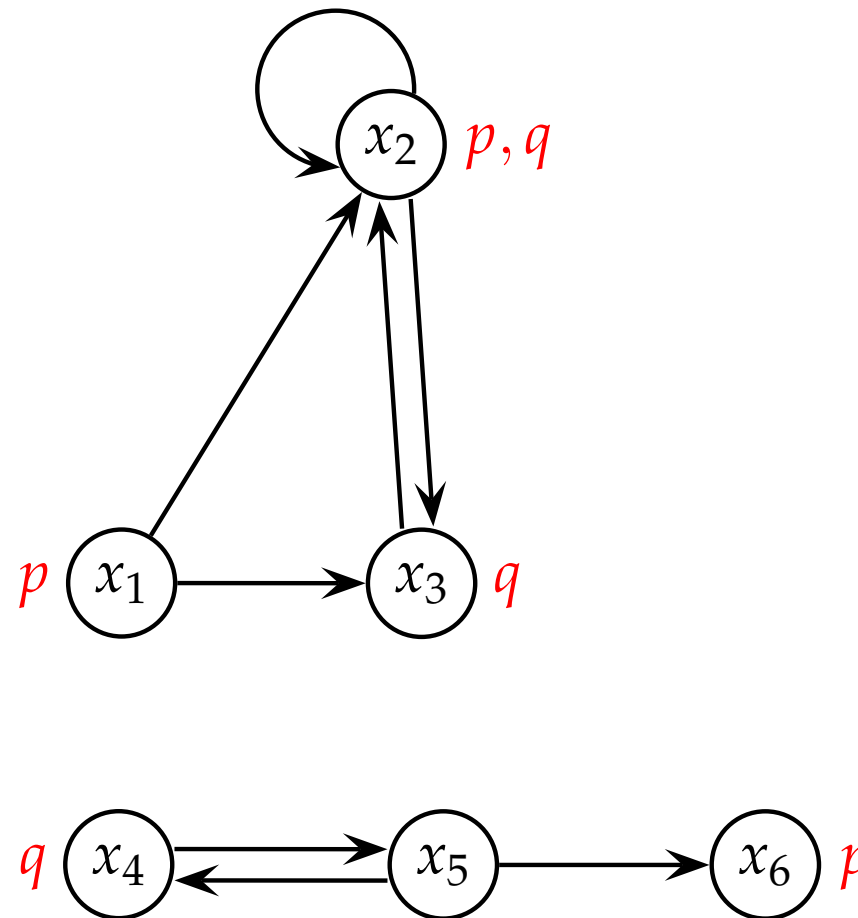
set of states



Kripke Structures: Example

accessibility
relation

set of states



Interpretation I

Modal Logic: Semantics

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

Valuation

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

$val_{\mathcal{K}}$ **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

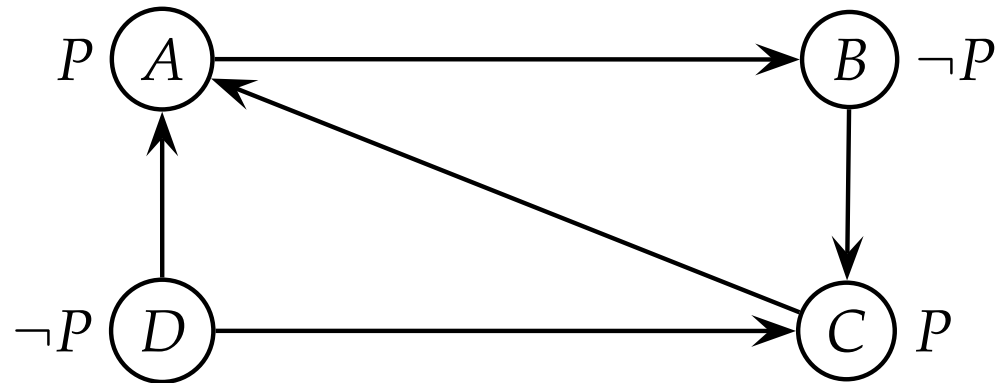
Studied at: **Harvard, Princeton, Oxford
and Rockefeller University**

Positions: **Harvard, Rockefeller, Columbia,
Cornell, Berkeley, UCLA, Oxford**

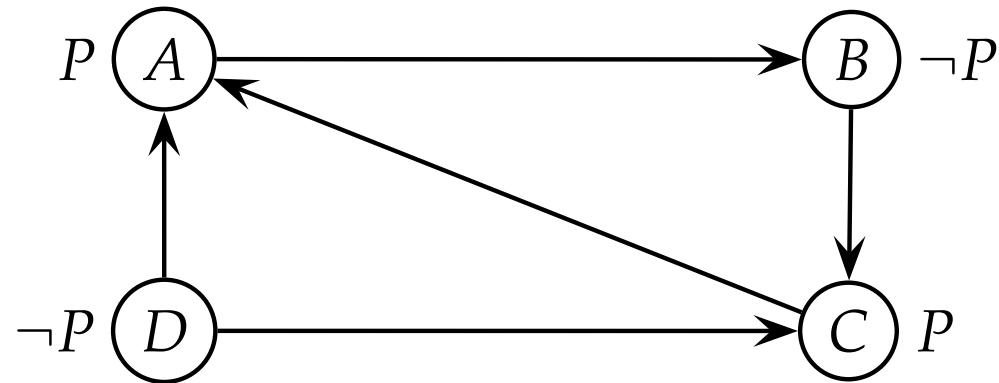
since 1977 **Professor at Princeton University**

since 1998 **Emeritus at Princeton University**

Modal Logic: Example for Evaluation



Modal Logic: Example for Evaluation



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

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

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

Modal Logic: Valid Formulas

Valid

● $\Box(P \rightarrow Q) \rightarrow (\Box P \rightarrow \Box Q)$

● $(\Box P \wedge \Box(P \rightarrow Q)) \rightarrow \Box Q$

● $(\Box P \vee \Box Q) \rightarrow \Box(P \vee Q)$

● $(\Box P \wedge \Box Q) \leftrightarrow \Box(P \wedge Q)$

● $\Box P \leftrightarrow \neg \Diamond \neg P$

● $\Diamond(P \vee Q) \leftrightarrow (\Diamond P \vee \Diamond Q)$

● $\Diamond(P \wedge Q) \rightarrow (\Diamond P \wedge \Diamond Q)$

Modal Logic: Valid Formulas

Valid

● $\Box(P \rightarrow Q) \rightarrow (\Box P \rightarrow \Box Q)$

● $(\Box P \wedge \Box(P \rightarrow Q)) \rightarrow \Box Q$

● $(\Box P \vee \Box Q) \rightarrow \Box(P \vee Q)$

● $(\Box P \wedge \Box Q) \leftrightarrow \Box(P \wedge Q)$

● $\Box P \leftrightarrow \neg \Diamond \neg P$

● $\Diamond(P \vee Q) \leftrightarrow (\Diamond P \vee \Diamond Q)$

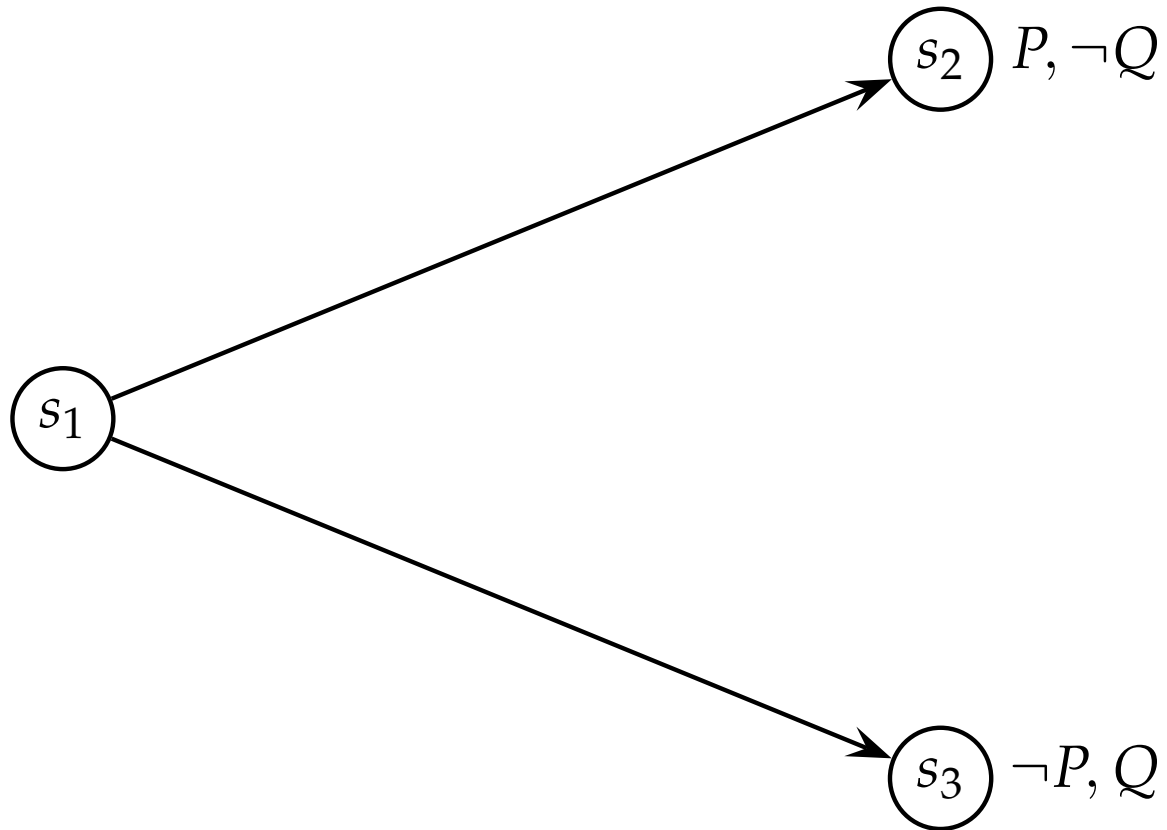
● $\Diamond(P \wedge Q) \rightarrow (\Diamond P \wedge \Diamond Q)$

Not valid:

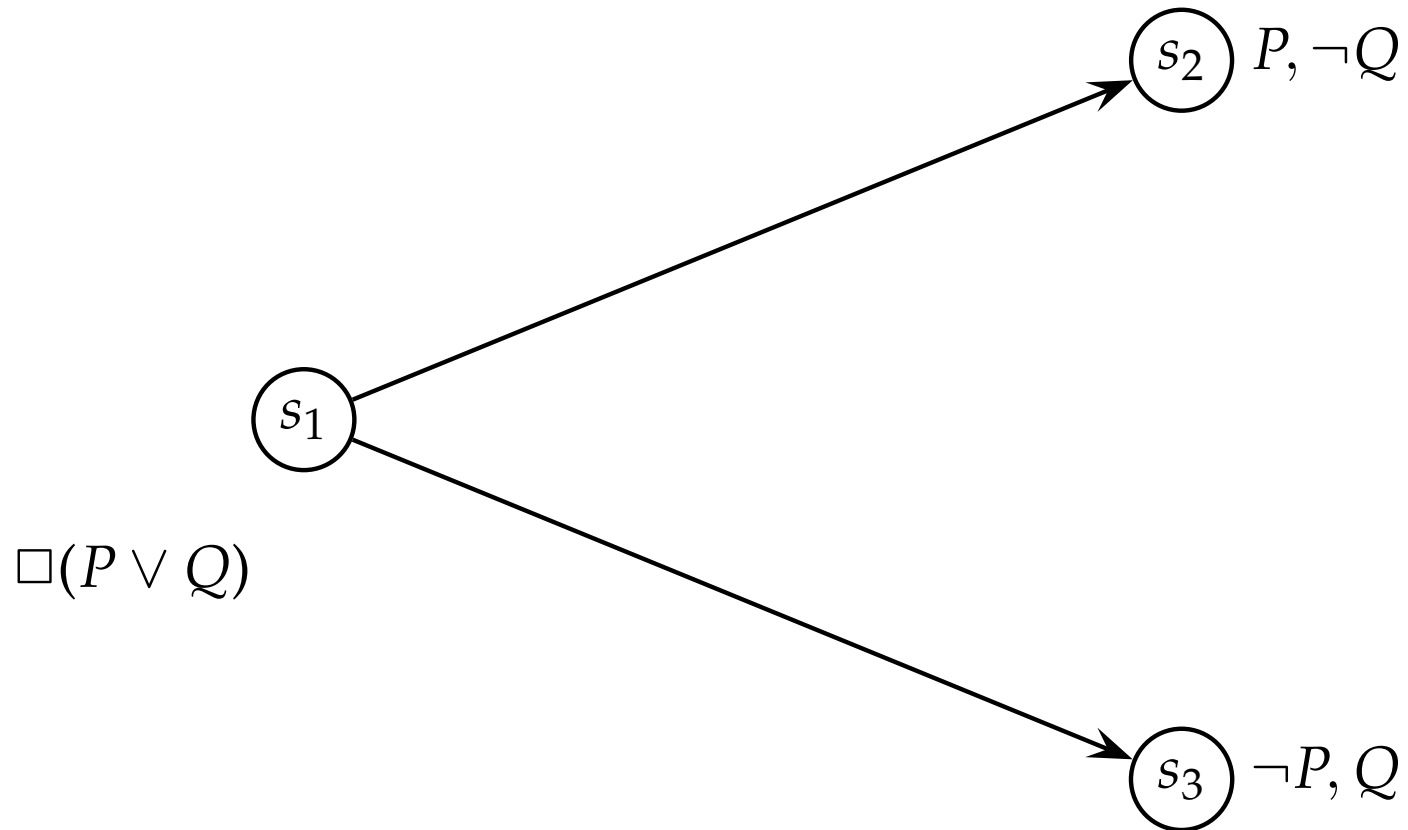
● $\Box(P \vee Q) \rightarrow (\Box P \vee \Box Q)$

● $(\Diamond P \wedge \Diamond Q) \rightarrow \Diamond(P \wedge Q)$

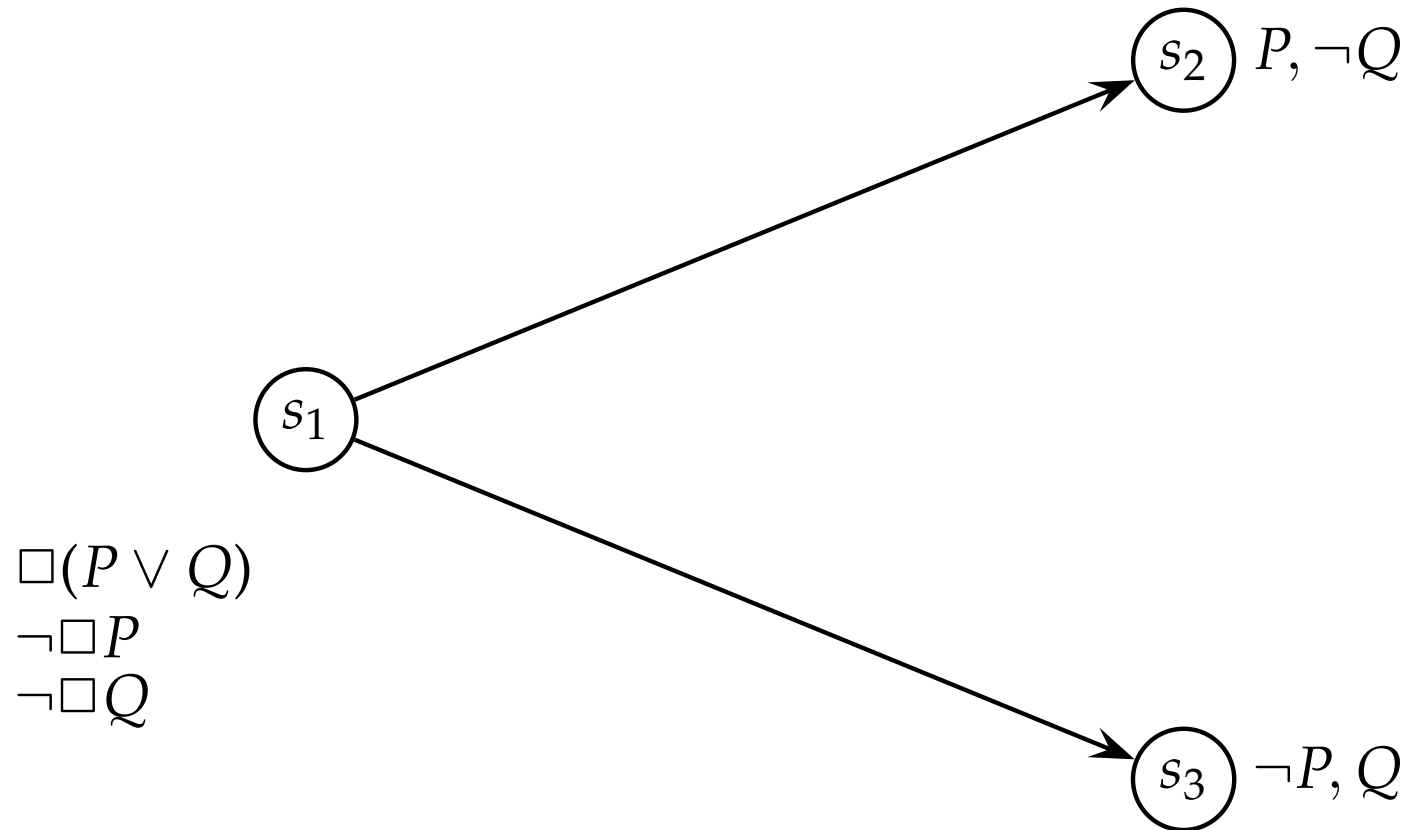
Not Valid: $\Box(P \vee Q) \rightarrow (\Box P \vee \Box Q)$



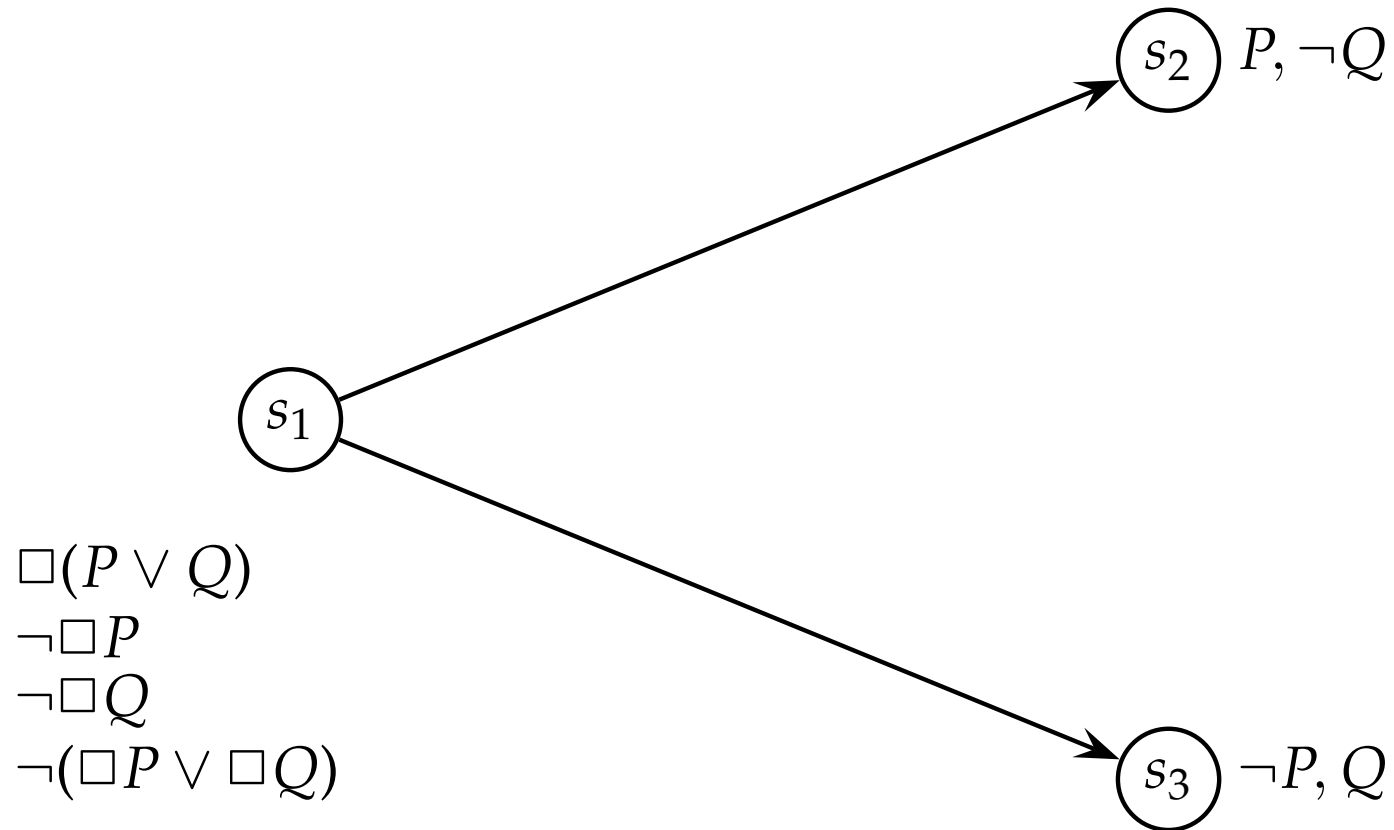
Not Valid: $\Box(P \vee Q) \rightarrow (\Box P \vee \Box Q)$



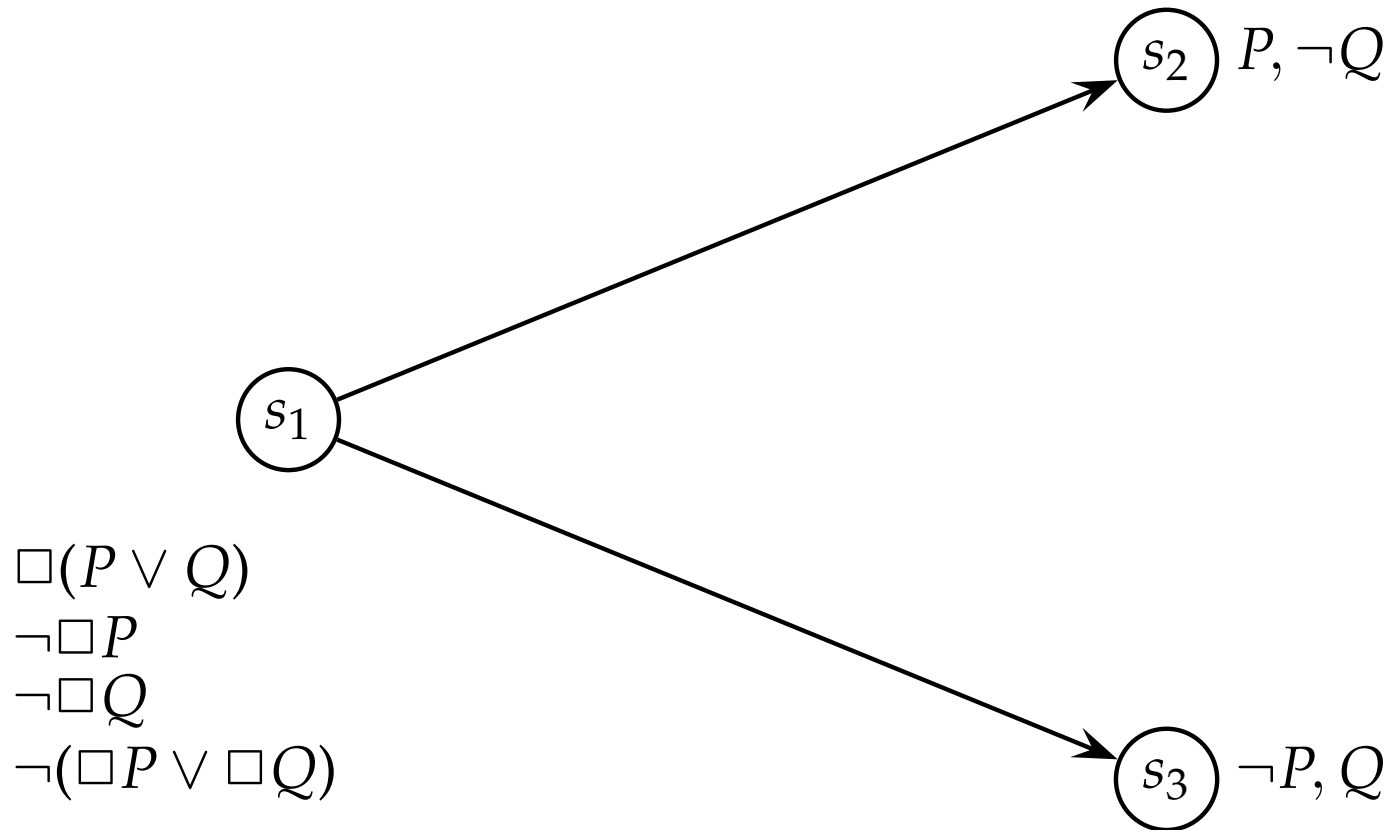
Not Valid: $\Box(P \vee Q) \rightarrow (\Box P \vee \Box Q)$



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



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



$\Box(P \vee Q) \rightarrow (\Box P \vee \Box Q)$ **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

Formulas Characterising Properties of R

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

Modal Logic: Valid Formulas

$\Box F$	$\Box F \rightarrow F$ $\Box F \rightarrow \Box \Box F$ $\Box F \rightarrow \Diamond F$ $(\Box(F \rightarrow G) \wedge \Box F) \rightarrow \Box G$ $\Diamond true$
F is necessarily true	
agent a knows F	
agent a believes F	
F holds after executing program p	

Modal Logic: Valid Formulas

	$\Box F \rightarrow F$	$\Box F \rightarrow \Box \Box F$	$\Box F \rightarrow \Diamond F$	$(\Box(F \rightarrow G) \wedge \Box F) \rightarrow \Box G$	$\Diamond true$
$\Box F$					
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